Project No. 101083594 Project start: 2022-12-01

Call: DIGITAL-2021-SKILLS-01 Project duration: 36 months

D2.2
Blended CyberSecPro technological training interactive technologies and academic practice

Document Identification	
Due date	31 October 2023
Submission date	02 January 2024
Revision	1.0

Related WP	WP 2	Dissemination Level	PU-public
Lead Participant	TalTech, ITML, Laurea	Lead Authors	Ricardo Lugo, Paresh Rathod, Paulinus Ofem Leo Johannesberg, Nikos Nikolaou, Dimitra Siaili, Kadi Kasepõld, Tiia Sõmer
Contributing Participants	All	Related Deliverables	D2.1, D2.2, D2.3

Abstract:

CyberSecPro (D2.1) undertook a market-driven investigation to identify EU cybersecurity industry knowledge and skills. This analysis (D2.2) of CSP partner courses and tools provided significant insights. Out of 81 courses assessed, 52% were undergraduate, 20% graduate, 9% summer school, and 19% professional training. Based on CSP partner offerings and market demand, these courses were divided into in-demand and high-demand knowledge domains. In addition, 64 CSP partner cybersecurity products were evaluated for applicability to different knowledge areas. To determine ENISA role alignment, CSP partner courses were compared to the European Cybersecurity Framework (ECSF). CSP classes covered certain responsibilities effectively, but others poorly. However, several ECSF courses covered numerous knowledge areas, satisfying market demand and frameworks.

Recommendations include expanding course variety, promote networking and collaboration between students and cybersecurity professionals. It is also necessary to standardize certifications for courses and tools, and align CyberSecPro program with ECSF to prepare students for ENISA-specified professional careers. Also, the integration of technical and human aspects of cybersecurity with interdisciplinary approaches, ensuring material accessibility, and providing students with easy access to textbooks, research articles, and information-sharing platforms will be needed. Another recommendation for the CyberSecPro program will be a need to update course material and resources often to reflect industry developments and developing technologies, and create a feedback loop with program participants, CSP partners, and industry experts to analyse and implement user software improvement proposals. Meeting these recommendations will make CyberSecPro a diverse and adaptable resource for cybersecurity education for the EU, and meet the everchanging industry standards.

Co-funded by the
European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union. Neither the European Union nor the granting authority can be held responsible for them.

This document is issued within the CyberSecPro project. This project has received funding from the European Union's DIGITAL-2021-SKILLS-01 Programme under grant agreement no. 101083594. This document and its content are the property of the CyberSecPro Consortium. All rights relevant to this document are determined by the applicable laws. Access to this document does not grant any right or license to the document or its contents. This document or its contents are not to be used or treated in any manner inconsistent with the rights or interests of the CyberSecPro Consortium and are not to be disclosed externally without prior written consent from the CyberSecPro Partners. Each CyberSecPro Partner may use this document in conformity with the CyberSecPro Consortium Grant Agreement provisions and the Consortium Agreement.

The information in this document is provided as is, and no warranty is given or implied that the information is fit for any particular purpose. The user thereof uses the information at its sole risk and liability.

Executive Summary

The market-driven analysis conducted by CyberSecPro (D2.1) aimed to identify the essential knowledge areas and proficiencies required within the European Union's cybersecurity industry. This analysis (D2.2) evaluated CSP partner courses and tools to provide valuable insights. CyberSecPro modules include courses, seminars, summer schools, cyber security exercises and that their syllabus and training material will be agreed among partners in order to achieve interoperability among the training offers and mobility among the trainers, trainees and cybersecurity professionals. A total of 81 courses were reviewed, with 52% being undergraduate, 20% graduate, 9% summer school, and 19% professional training courses. These courses were categorized into in-demand and high-demand knowledge domains, aligned with CSP partner offerings and market demand. Additionally, 64 cybersecurity tools offered by CSP partners were assessed, with a focus on adaptability to different knowledge areas. The analysis also compared CSP partner courses with the European Cybersecurity Framework (ECSF) to ascertain their alignment with ENISA roles. While some roles were well-covered by CSP courses, others had limited coverage. However, certain courses encompassed multiple knowledge areas under the ECSF, meeting both market demand and established frameworks.

Conclusions and recommendations:

- Harmonise and target training efforts: Harmonise the variety of training modules and modify them in addressing sector specific (maritime, energy, health) training needs in the CyberSecPro program can target these domains and accommodate sectoral stakeholders to raise their capabilities and skills in cybersecurity.
- Promote Adaptable Tools: Collaborate with Certified Security Professionals (CSP) to develop cybersecurity tools with greater adaptability and broader knowledge area coverage, ensuring their relevance in this rapidly evolving field.
- Standardize Certification: Establish clear certification standards for courses and tools, allowing students to demonstrate their expertise in specific areas, thereby advancing their careers.
- Align with ECSF: Align the CyberSecPro program with the European Cybersecurity Framework to equip students with the skills and knowledge required for professional roles specified by ENISA. This alignment can enhance the program's significance in the EU cybersecurity landscape.
- Offer Interdisciplinary Courses: Bridge technical and human aspects of cybersecurity through interdisciplinary courses that address cybersecurity's role in institutions and organizations, providing practical solutions.
- Promote Networking and Academic and Industrial Cooperation: Encourage program participants to network with industry professionals to collaborate and apply their expertise. Consider developing internship or practical placement courses to achieve learning outcomes.
- Ensure Material Accessibility: Ensure easy access to learning materials such as textbooks, research articles, and knowledge-sharing platforms to keep students updated on scientific findings and market knowledge.
- Continuous Updates: Due to industry changes and evolving technologies, the program's course content and tools should be regularly updated. Establish a feedback loop involving program participants, CSP partners, and industry experts to evaluate and integrate user suggestions for software improvements.

These recommendations aim to keep the CyberSecPro program competitive and adaptable to the dynamic EU cybersecurity industry. Embracing diversity, promoting adaptability, and aligning with industry standards are key steps in ensuring the program's success and relevance in the ever-evolving field of cybersecurity.

Document Information

Contributors

Name:	Beneficiary
Ricardo Lugo, Kadi Kasepõld, Tiia Sõmer	TALTECH
Nikos Nicolau, Dimitra Siailis	ITML
Paresh Rathod, Paulinus Ofem, Jari Savolainen, Jari Räsänen, Leo Johannesberg, Jyri Rajamäki, Rauno Pirinen	LAU
N. Polemi, T. Karvounidis, D. Koutras, A. Spatharos	UPRC
S. Borotis	MAG
K. Kioskli, K. Voliotis	trustilio
D. Boberic Krsticev	UNSPMF
Cristina Alcaraz, Javier Lopez, Ruben Ríos, Isaac Agudo, Antonio Muñoz, J. A. Onieva, J. A. Montenegro	University of Malaga (UMA)
Antonis Spatharos, Kai Rannenberg, Per Håkon Meland, Nektaria Kaloudi, Ahad Niknia, Ann-Kristin Lieberknecht, Elias Athanasopoulos, Narges Arastouei, Frederic Tronnier, Fabio Martinelli, Nuno Mateus-Coelho, Gregor Langner, Stella Markopoulou, Bruno Bender	GUF, IMT, TUBS, TUC, UCY, AIT, CNR, COFAC, SINTEF, UNI, ACEEU, APIRO, FP, SLC, FCT

Reviewers

Name	Beneficiary
Dr. Ana Isabel Cerezo Domínguez	University of Malaga (UMA)
Dr. Elias Athanasopoulos	University of Cyprus (UCY)

History

Version	Date	Contributor(s)	Comment
0.01	09.03.2023	TalTech, ITML, GUF (updated later)	1st Draft of ToC
0.02	28.04.2023	TalTech, UPRC, Lau	Comments on ToC
0.03	08.05.2023	TalTech, ITML	Consolidated ToC
.1	09.05.2023 – 06.30.2023	All Partners	Contribution
.2	06.07.2023	TalTech, ITML	Review of the structure and consolidation and early draft
.3	10.07.2023 – 18.07.2023	All Partners	Updates and contributions
.31	08.09.2023 – 18.09.2023	All Partners	Updates and contributions
.4	08.10.2023	TalTech, ITML	1st draft
.5	12.10.2023-16.10.2023	TalTech, ITML	Editorial updates, submission to reviewers preparation
.6	27.10.2023- 31.10.2023	TalTech, ITML	Editorial updates after reviewer comments
.7	31.10.2023 – 09.11.2023	TalTech, ITML	Editorial updates after reviewer comments
.8	10.11.2023 – 24.11.2023	TalTech, ITML	Editorial updates after 2nd round reviewer comments
.81	26.11.2023	TalTech, ITML, UCy, UMA	Final feedback from reviewers
.82	26.11.2023	TalTech, ITML, UPRC	Final Feedback from technical officer
.83	19.12.2023	TalTech, ITML, ACEEU	Final feedback from QM
.9	20.12.2023	GUF, TalTech, ITML	Feedback from PL
.91	22.12.2023 – 30.12.2023	TalTech, ITML, Laurea	Editorial updates after technical feedback
1.0	31.12.2023 – 02.01.2024	TalTech, ITML	Final version
1.0	02.01.2024	GUF	Final check, preparation and submission process

Table of Contents

List of Tables

List of Figures

List of Acronyms

A	ACL	Access Control List
	ACS	Australian Computer Society
	AD	Anomaly Detection
	AI	Artificial Intelligence
	ARP	Address Resolution Protocol
B	B2C	Business-to-Consumer
	BACS	Behavioural Analysis and Cognitive Security
C	CA	Certificate Authority
	CDPSE	Certified Data Privacy Solutions Engineer
	CEP	Cyber Exercise Platform
	CEPOL	EU Agency for Law Enforcement Training
	CERT	Computer Emergency Response Team
	CET	Certified in Emerging Technology
	CGEIT	Certified in the Governance of Enterprise IT
	CISA	Certified Information Systems Auditor
	CISM	Certified Information Security Manager
	CNPD	National Commission for Data Protection
	CRISC	Certified in Risk and Information Systems Control
	CRL	Certificate Revocation List
	CSDP	Common Security and Defence Policy
	CSMS	Cybersecurity Management Systems
	CSP	CyberSecPro
	CSP	Certified Security Professionals
	CSP	Cyber-Physical Systems
	CSR	Certificate Signing Request
	CTF	Capture the Flag Framework
	CSX-P –	CSX Cybersecurity Practitioner Certification
	CVD	Coordinated Vulnerability Disclosure
D	DDOS	Distributed Denial of Service
	DEP	Digital Europe Programme
	DNS	Domain Name System
	DSO	Distribution System Operator

E	ECCC	European Cybersecurity Competence Centre
	ECSF	European Cybersecurity Framework
	ECTS	European Credit Transfer and Accumulation System
	EDA	European Defence Agency
	EDIH	European Digital Innovation Hubs
	EMPL	Directorate-General for Employment, Social Affairs and Inclusion
	ENISA	European Union Agency for Cybersecurity
	ESCO	European Skills, Competence, Qualifications and Occupations
	ESDC	European Security and Defence College
	ETEE	Cyber Education, Training, Exercise and Evaluation
F	FP	Focal Point
G	Gbd	GNU debugger
	GCFA	GIAC Certified Forensic Analyst
	GCIH	GIAC Certified Incident Handler Certification
	GIAC	Global Information Assurance Certification
	GPEN	GIAC Penetration Tester Certification
	GPG	GNU Privacy Guard
	GSE	GIAC Security Expert
	GVM	Greenbone Vulnerability Management
	GX-IA	GIAC Experienced Intrusion Analyst Certification
	GX-IH	GIAC Experienced Incident Handler Certification
	GX-CS	GIAC Experienced Cybersecurity Specialist Certification
H	HEI	Higher Education Institution
	HIDS	Host-based Intrusion Detection System
I	ICMP	Internet Control Message Protocol
	ICT	Information and Communication Technology
	IDPS	Intrusion Detection and Prevention System
	IDS	Intrusion Detection
	FIP	International Federation for Information Processing
	IGMP	Internet Group Management Protocol
	IOC	Indicators of Compromise
	IPS	Intrusion Prevention System

	IRCA	International Register of Certified Auditors
	ISC2	International Information System Security Certification Consortium
	ISMS	Information Security Management System
	IT	Information Technology
	ITCA	Information Technology Certified Associate
J	JRC	Joint Research Centre
K	KA	Knowledge Area
L	LINDDUN	Linkability, Identifiability, Non-repudiation, Detectability, and Unlinkability
	LMS	Learning Management System
	LTE	Long Term Evolution
M	MISP	Malware Information Sharing Platform and Threat Sharing
N	NIDS	Network-based Intrusion Detection System
	NMAP	Network Mapper
	NPS	Naval Postgraduate School
	NSE	NMAP Scripting Engine
O	OpenVAS	Open Vulnerability Assessment System
	OSCP	Offensive Security Certified Professional
P	PGP	Pretty Good Privacy
	PWK	Penetration testing with kali Linux
R	RARP	Reverse Address Resolution Protocol
S	SANS	SysAdmin, Audit, Network, and Security
	SAST	Static Application Security Test
	SCAP	Security Content Automation Protocol
	SFIA	Skills Framework for the Information Age
	SI	Security Infusion
	SIEM	Security Information and Event Management
	SLC	Security Lab Consulting

	SMB	Server Message Block
	SOC	Security Operation Center
	SPA	Secure Personal Access
	STIX2	Structured Threat Information Expression
	STRIDE	Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, and Elevation of Privilege
	SQL	Structured Query Language
T	TCP	Transmission Control Protocol
	TGTs	Ticket-Granting Tickets
	TIP	Threat Intelligence Platform
	TORC	Training for Operational Resilience
	TSOs	Transmission System Operators
U	UDP	User Datagram Protocol
W	WLAN	Wireless Local Area Network
X	XCA	Certificate and Key Management
	XSS	Cross-site Scripting
Z	ZAP	Zed Attack Proxy

1 Comparative Education Methodology for Cybersecurity Knowledge Areas and Education in Higher Education

1.1 Background

In order to provide users with the knowledge and skills they need, it is critical to establish effective instructional offerings as the subject of cybersecurity continues to evolve quickly. Particularly in the area of cybersecurity, comparative education provides an invaluable framework for evaluating and contrasting various educational approaches. This section examines how comparative education methodology can be used to improve higher education's cybersecurity curricula, with a focus on identifying and contrasting knowledge areas derived from data collection from deliverable D2.1 and the role frameworks for cybersecurity professionals developed by the Joint Research Centre (JRC) and European Union Agency for Cybersecurity (ENISA). Institutions can improve their cybersecurity curricula, harmonize them with industry standards, and handle the changing problems of the digital ecosystem by utilizing comparative education approaches.

1.2 Scope

Cybersecurity has become a crucial concern for individuals, corporations, and countries in the linked world of today. There is a rising need to create skilled cybersecurity experts through efficient educational programs, given the frequency and sophistication of cyber threats. The purpose of this section is to examine how comparative educational approaches might be used to improve cybersecurity education in higher education, specifically by identifying and contrasting knowledge domains resulting from gathered data and recognized role frameworks like those offered by JRC and ENISA.

1.3 Methodology Comparative Education

Comparative education is the study of educational practices, policies, and systems in various contexts or nations. It offers a useful framework for assessing the benefits and drawbacks of various educational techniques, allowing for the discovery of best practices and potential areas for development.

By using comparative education methodologies in cybersecurity education, institutions can learn from various educational models and modify their curricula to meet the changing needs of the industry. This strategy enables the identification of crucial subject areas, instructional techniques, and evaluation procedures that successfully prepare students for employment in cybersecurity.

One component of comparative education methodology entails gathering information from a variety of sources, including academic offerings and publications, industry reports, and professional certifications. Educational institutions can determine the knowledge areas that should be covered in their cybersecurity curricula by studying this data. Network security, cryptography, secure coding techniques, incident response, and risk management are a few examples of knowledge domains.

Role frameworks created by the JRC and ENISA offer detailed instructions for the abilities and capabilities expected of cybersecurity experts. These frameworks list the knowledge, skills, and abilities needed for each function, including security architect, incident responder, and vulnerability analyst. Educational institutions can learn a lot about the expectations of the business by comparing these role frameworks with the data that has been gathered and then adapting their courses.

Comparative Analysis Methodologies: Educational institutions can use a variety of methodologies, including content analysis, curriculum mapping, and gap analysis, to facilitate a comparative analysis. The gap analysis was provided by D2.1 and content analysis will be provided by D2.3. Reviewing the collected data and job frameworks is part of content analysis. This is done to find similarities, overlaps, and gaps in the knowledge areas. D2.2 will be about mapping knowledge areas from CSP partner course offers to the knowledge domains found in D2.1. Course offerings include courses at the undergraduate and graduate levels from Higher Education Institutions (HEI), and from the private industry. This also includes seminars, workshops, summer schools and other offerings regardless of learning modes, such as physical, virtual, or hybrid delivery methods.

Comparative analysis also helps institutions to evaluate their cybersecurity courses in comparison to industry norms and needs as provided in D2.1 and pinpoint areas for strength or further development. This will ensure institutions that their graduates have the abilities needed to handle new cybersecurity threats by utilizing the advantages of various educational models and combining pertinent knowledge areas from training modules offered at other institutions.

Educational institutions can also use the findings from both D.2.1 and D2.2 to update and/or create cybersecurity curricula that complement the indicated knowledge areas by using the findings from the gap analysis (D2.1) and comparative analysis (D2.2). To address the multifaceted nature of cybersecurity, this may entail updating existing courses, offering new modules, collaborating with other HEI's, or using interdisciplinary approaches.

For cybersecurity education to be successful, effective pedagogical methods must be used. Trainees' practical skills and critical thinking abilities can be improved through active learning techniques, practical exercises, case studies, and simulated scenarios. Additionally, group projects, internships, and business alliances can give students real-world experience and guarantee the relevancy of the curriculum. For this, D.2.2 also provides an analysis of platforms and tools offered by the CSP consortium, as well as evaluations of the provided courses described in D2.2.

Using comparative education methods to build and enhance higher education's cybersecurity curricula has many benefits. Institutions can improve their cybersecurity curricula, align them with industry standards, and produce graduates who are equipped to handle the complex challenges of cybersecurity by identifying and comparing knowledge areas derived from gathered data and established role frameworks like JRC and ENISA. For cybersecurity education to be effective and a secure digital ecosystem to be maintained, there must be ongoing study and collaboration between academics and industry.

2 Cybersecurity Training Offerings

This section will review cybersecurity course offerings, that are both from the private sector and from European Union initiatives. This will entail a description of the offering, summarize their approaches and explain any certifications or accreditations where applicable.

2.1 Non-European Union Initiatives

2.1.1 SecureSet Academy

SecureSet Academy [1] (Denver, Colorado, USA), part of Flatiron School since 2022, is a center for cybersecurity education that provides students with intensive, bootcamp-style courses that will provide them the skills they need to work in the field. SecureSet Academy places an emphasis on practical, hands-on cybersecurity training. Their courses are created to be in-depth and engaging, emulating the difficulties that cybersecurity professionals have in the real world. Depending on the program and format, bootcamps can last anywhere from a few weeks to many months.

Programs available through SecureSet Academy include:

CORE: A comprehensive cybersecurity program that is full-time and immersive, covering everything from network security to ethical hacking and threat intelligence.

HUNT: Emphasizes cybersecurity analytics and instructs students on how to recognize, evaluate, and react to security threats.

PATH: A part-time program created for people who need a more flexible schedule or who are working professionals.

The SecureSet Academy's curriculum is intended to be experiential and useful. Learners participate in projects, simulations, and labs that reflect real-world cybersecurity difficulties. Network security, penetration testing, threat intelligence, security analytics, and other subjects are discussed. In addition to analysts, penetration testers, and consultants, many recent graduates have found work in a variety of cybersecurity areas. The academy has worked with numerous groups and businesses in the cybersecurity sector to ensure that their curriculum is up to date, and that learners have access to networking and job placement opportunities. SecureSet Academy mostly provides intense bootcamp-style modules meant to give learners real-world cybersecurity knowledge. They do not issue widely accepted industry credentials like those from (ISC)2, CompTIA, or EC-Council, despite offering thorough training and education.

2.1.2 Fullstack Academy

Fullstack Academy [2] (Brooklyn, New York, USA) is a coding bootcamp that offers immersive training programs in web development and cybersecurity. Fullstack Academy's Cyber Bootcamp is designed to transform individuals with little to no background in information technology (IT) into cybersecurity professionals. The bootcamp is typically several months long, with both full-time and part-time options available. The bootcamp offers immersive experiences, often with live instruction, collaborative projects, and interactive labs. The program covers a wide range of topics, including networking, system architecture, cryptography, ethical hacking, vulnerability discovery, and penetration testing. The program emphasizes hands-on learning with real-world scenarios, labs, and exercises.

2.1.3 The Australian Computer Society (ACS)

The ACS [3] (Sydney Australia; Australian Computer Society) is a professional association that represents Australia's Information and Communication Technology (ICT) sector. ACS offers training and certification to help professionals validate their skills and knowledge in the field. The ACS provides a certification program tailored to the cybersecurity domain and is designed to recognize the skills and expertise of professionals in the field and is aligned with the Skills Framework for the Information Age (SFIA). The ACS cybersecurity certification is recognized in Australia and provides a benchmark for employers to assess the skills and expertise of potential candidates.

2.1.4 The Offensive Security Certified Professional (OSCP)

The OSCP [4] (New York, USA; The Offensive Security Certified Professional) credential for penetration testing abilities is widely acknowledged. It is provided by Offensive Security and is renowned for its demanding and practical approach. "Penetration Testing with Kali Linux" (PWK) is the main training for the OSCP. This course presents numerous tools and methodologies while giving students the fundamental skills needed for penetration testing. Trainees can practice their abilities on a range of machines in a virtual lab environment that simulates real-world settings as part of the PWK course. Candidates for the OSCP exam have to manage a number of devices in a specific testing environment over the course of 24 hours. Candidates must successfully exploit these computers in order to obtain the OSCP certification.

2.2 Existing European Union Initiatives

There are various divergent cybersecurity training efforts and supply in EU including:

2.2.1 EU Agency for Cybersecurity (ENISA)

ENISA has been developing instruments related to role profiles or higher education, e.g. the European Cybersecurity Skills Framework (ECSF); the CYBERHEAD - Cybersecurity Higher Education Database (CyberHead); the Cyber Exercise Platform (CEP); the European Cyber Security Challenge; the European Cyber Security Month. Also, ENISA[5] provides training courses and practical materials on cybersecurity and crisis management with a focus on incident responders, operational security professionals and cybersecurity trainers. The training course offerings include, among others, malware analysis and memory forensics, mobile threats and incident management and network forensics [5].

2.2.2 European Cybersecurity Competence Centre (ECCC)

ECCC [6] is addressing cybersecurity skills in a dedicated working group. One of the main objectives of the Network and the Centre is to align the high educational programmes and certifications in all cybersecurity sectors (such as network security, cloud security, hardware security) and provide a comprehensive matrix that matches skills and workforce. It will be a continuous effort of the Network and the Centre to build comprehensive curricula and training programmes addressing industrial needs covering all cybersecurity sectors.

2.2.3 The European Security and Defence College (ESDC)

ESDC [7] is working on the cybersecurity skills of the civilian and military workforce in the context of the Common Security and Defence Policy (CSDP). ESDC has developed the cyber-Education, Training, Exercise and Evaluation [8] (ETEE; ESDC) platform providing cybersecurity defence training. ETEE addresses cyber security and defence training among the civilian and military personnel for the CSDP requirements for all CSDP training levels. The ESDC train personnel with a view to provide all EU Member States with the option of developing a cyber defence reserve capability. The training is carried out by Member States' national universities, academies, colleges and institutes certified as a ETEE platform member. The certified institutions are financed for each trainee.

2.2.4 Computer Emergency Response Team EU (CERT-EU)

CERT-EU [10] provides training to the EC institutions in several cybersecurity areas such as intrusion detection – in depth, digital forensics and incident response, continuous monitoring and security operations, among others. This is done in cooperation with the European Council in the context of a framework cyber-security contract [8].

2.2.5 European Defence Agency (EDA)

EDA [11] is active in cyber ranges federation. They have developed a powerful platform for cyber training purposes, connecting Member States' national Cyber Ranges to one another and enabling other countries, which do not have their cyber ranges, to train and improve their cyber defence skills. It comprises a European federation of cyber ranges that are mutually accessible for member states for cyber defence training and exercise ranges.

2.2.6 Digital Skills and Jobs Coalition

The Digital Skills and Jobs Coalition [12] currently counts more than 340 members – a number which is growing steadily. Members are ICT companies and ICT-using companies e.g. from the banking sector, social partners such as employees and employers federations, as well as education and training providers, civil society organisations. They all have a role to play in the dissemination and the uptake of the digital skills for the citizens, the labour force and the development of ICT specialists in Europe. Currently 90 members of the Coalition have taken their engagement a step further and pledged action - made concrete commitments - to equip all Europeans with the digital skills needed to live, work and participate in the digital society. Some of these pledges address cybersecurity. The activities of the Coalition have so far reached around 7 million citizens with over 3.7 million people trained in digital skills, over a million digital skills certifications delivered, four and half thousand events which have reached to over a million citizens, and over nine thousand job placements and around 200 internships offered.

2.2.7 National Coalitions for Digital Skills and Jobs

The National Coalitions for Digital Skills and Jobs [13] are partnerships that bring together different stakeholders from the public, private, and non-profit sectors in various countries. These coalitions aim to address the digital skills gap and to help increase the digital talent pool in their respective nations. The establishment of these coalitions was spurred by the European Commission's Grand Coalition for Digital Jobs initiative, which was launched in 2013. The initiative recognized the growing need for digital skills in the workforce due to the rapid digitization of the economy and the emerging digital skills gap.

The goals of the coalition include:

- Improving digital training and education: This includes modernizing education and training systems to make them relevant to the current job market's needs.
- Certification: Introducing certification mechanisms to validate digital skills can help employers recognize and trust the digital competencies of potential employees.
- Awareness raising: Many coalitions aim to increase awareness about the importance of digital skills and the vast career opportunities in the digital sector.
- Job placement and internships: Some coalitions play an active role in connecting trained individuals with potential employers or offering internships.

Different European countries have set up their own national coalitions tailored to their specific challenges and needs. While each coalition is unique in its approach and initiatives, they all share the common goal of boosting digital skills and promoting digital employment.

2.2.8 Directorate-General for Employment, Social Affairs and Inclusion (EMPL)

The Skills Agenda encompasses the Blueprint for sectoral cooperation on skills [14], which is an initiative by the European Commission (EC) aimed at fostering strategic collaboration among key stakeholders in a specific economic sector. These stakeholders include businesses, trade unions, research institutions, education and training institutions, and public authorities. The Blueprint operates on a bottom-up approach, empowering businesses within a sector to identify their skills requirements and establish partnerships with relevant entities capable of addressing those needs. There is a particular emphasis on skills associated with the digital advancement of various sectors, and the study conducted within these sectors may encompass the identification of cyber security skill requirements. Cybersecurity is considered a priority sector due to its transversal nature, affecting multiple sectors.

2.2.9 Digital Competence Framework (DigComp)

The EU DigComp [15] was developed by the European Commission (together with the JRC) to identify and describe the set of digital competences that are needed by all citizens today. The Framework uses a common language for competences and proficiency levels that can be understood across Europe.

DigComp is a common reference framework that sets out 21 competences, grouped in the following 5 key areas:

1. **Information and Data Literacy**: This involves browsing, searching, filtering data and information, and evaluating data, information, and digital content.
2. **Communication and Collaboration**: This area emphasizes interacting in digital environments, sharing through digital means, engaging in citizenship through the digital realm, collaborating through digital channels, and netiquette (online etiquette).
3. **Digital Content Creation**: It encompasses developing, creating, and editing digital content, integrating and re-elaborating knowledge, programming, and solving problems through digital means.
4. **Safety**: This involves personal protection, data protection, digital identity protection, safe and sustainable use of digital technologies, and protecting the environment.
5. **Problem Solving:** This key area focuses on identifying needs and technological responses, making informed decisions, identifying digital gaps, creatively using digital technologies, and troubleshooting.

The competences included under safety are: protecting devices; protecting personal data and privacy; protecting health and well-being; protecting the environment. The current version of the framework is 2.2, which incorporates more than 250 new examples of knowledge, skills and attitudes that help citizens engage confidently, critically and in a secure manner with digital technologies, and new and emerging ones such as systems driven by Artificial Intelligence (AI).

2.2.10 European Skills, Competences, Qualifications and Occupations (ESCO)

The classification of ESCO [16] includes ICT security skills under digital transversal skills, i.e. skills not assigned to specific occupations. This includes 4 concepts from DigComp and 7 additional more specific skills. In addition, there are some concepts in ESCO related to more expert skills, e.g. "cyber security", "cyber-attack counter measures", "ICT security legislation". They feature in occupational profiles of related occupations, e.g. "webmaster", "ICT security manager", "ICT disaster recovery analyst", "ICT resilience manager" or "ethical hacker".

2.2.11 DG GROW

DG GROW [17] refers to the Directorate-General for Internal Market, Industry, Entrepreneurship and SMEs of the European Commission and id responsible for EU policy on the single market, industry, entrepreneurship, and small and medium-sized enterprises (SME) Its objectives are to research, design, test and validate specific measures supporting the following:

- **Big Data**: This involves training and skills development around collecting, processing, analyzing, and interpreting large sets of data. For SMEs, understanding big data can lead to better business decision-making, more efficient operations, and improved customer experiences.
- **IoT (Internet of Things):** This pertains to the network of interconnected devices that can collect and exchange data. For SMEs, leveraging IoT can offer enhanced product features, more efficient processes, and new business models. Training covers the creation, management, and security of these devices.

- **Cybersecurity:** As cyber threats become more sophisticated, SMEs, which might not have the resources of larger corporations, need to be equipped to protect their digital assets. Specialized skills development training for SMEs is offered to safeguard their businesses from cyber threats, ensure data privacy, and respond to potential cyber incidents.

DG GROW's focus on these areas indicates the European Commission's recognition of the importance of these technologies for the future competitiveness and resilience of European businesses, especially SMEs. By ensuring that SMEs have access to the necessary skills and knowledge in these domains, the Commission aims to foster innovation, growth, and security within the European single market.

2.2.12 Joint Research Centre (JRC)

The JRC [18] of the European Commission plays a significant role in providing scientific advice and technical expertise to support EU policies. While the JRC covers a wide range of research areas, its focus on cybersecurity is particularly essential given the increasing importance of digital security in the modern age. JRC cybersecurity skills education strategies and awareness-raising campaigns include:

- **Research and Analysis**: The JRC often conducts studies on the current state of cybersecurity education, identifying gaps in skills and training across member states.
- **Curriculum Development:** Based on its research, the JRC may provide recommendations or even frameworks for cybersecurity curriculum development at various educational levels, ensuring a standardized level of competency across the EU.
- **Training Programs:** The JRC could initiate or support specialized training programs targeted at both public and private sector stakeholders, ensuring they are equipped to deal with current and emerging cyber threats.
- **Awareness Campaigns:** Recognizing that many cyber incidents stem from human error or lack of awareness, the JRC can launch campaigns to educate the public and organizations about best practices in digital security, phishing threats, password management, and more.
- **Collaborations and Partnerships:** The JRC might foster partnerships with academic institutions, industry, and other stakeholders to amplify the reach and impact of its cybersecurity initiatives.
- **Policy Recommendations:** Based on its findings, the JRC can provide policy recommendations to the European Commission and member states, advising on how best to bolster digital security and resilience.

For the most current and detailed information on JRC's strategies as they pertain to cybersecurity skills education and awareness, one would need to refer to the JRC's official publications or the European Commission's communications from after January 2022.

The Joint Research Centre (JRC) and Digital Europe have a relationship centred around advancing and supporting the European Union's digital agenda and policy framework. The JRC, as a scientific and technical arm of the European Commission, plays a crucial role in providing research, data, and technical expertise. This support is vital in shaping and informing EU policies, including those related to the digital domain.

Digital Europe, on the other hand, represents a broad program by the EU aimed at bolstering the digital transformation of Europe's society and economy. This program focuses on funding and driving digital capabilities, from high-performance computing and artificial intelligence to cybersecurity and advanced digital skills.

The relationship between JRC and Digital Europe involves the JRC contributing scientific and technical insights that guide and shape the initiatives under the Digital Europe program. This collaboration ensures that the EU's digital policies and programs are grounded in robust scientific research and state-of-the-art technological understanding. The synergy between these two entities is vital for the EU's ambition to be digitally sovereign, innovative, and competitive on a global stage.

2.2.13 Directorate-General for Mobility and Transport (DG MOVE)

DG MOVE [19] developed terms of reference for a public procurement exercise to develop a holistic and interactive cyber security toolkit usable via an Information Technology (IT) application. This is to support security managers and professionals in the transport sector to better identify, assess and mitigate against cyber security risks. The objectives of this toolkit are:

- to explain and promote recommended good practices covering both generic aspects of cyber-security and in addition more specific modules related to the needs of each transport mode;
- to create a secure closed digital platform where the transport sector's security managers and cyber professionals could interact and exchange both operational and technical advice/reporting and real time information/warnings about new cyber threats and advice for mutual benefit. It develops an integrated community of staff working in all transport modes who are either IT cyber-security experts or managers responsible for all security risks that can support each other, providing greater resilience for the sector; and
- develop a package of awareness materials that should be developed both to clearly articulate the business risks of not properly considering and addressing cyber risks, and promoting the online toolkit to ensure organisational buy-in and usage of the products.

The target group is the transport sector: aviation, maritime and rail transport sector, both service operators and infrastructure managers. In particular: (i) management and employees who are required to deal with security matters including physical, operational, information and personnel security; (ii) Senior organisational managers/executives with responsibility for business investment and operational oversight.

2.2.14 CEPOL & Europol

The EU Agency for Law Enforcement Training [21] and Europol, as of 2023, are key agencies in the European Union that offer training on various aspects of cybercrime. CEPOL specializes in law enforcement training, ensuring that officers across member states are equipped with the knowledge and skills needed to tackle evolving security threats. Their training encompasses the following areas:

<u>CEPOL:</u>

- **Cybercrime Identification and Reporting**: Training covers how to identify various forms of cybercrime, from financial fraud to cyberbullying. Law enforcement personnel are taught how to document and report these incidents correctly.
- **Digital Forensics**: Instruction on the techniques to recover, preserve, and analyse digital evidence from electronic devices.
- **Incident Handling and Response**: Training in this area focuses on how officers should react when a cyber incident occurs. This includes ensuring data integrity, collecting evidence, and coordinating with other departments or agencies.
- **Public-Private Partnerships:** Emphasizes collaborations between law enforcement and the private sector. Training covers communication channels, shared resources, and joint strategies.
- **Emerging Threats and Technologies:** Addresses upcoming threats, such as those posed by newer technologies like IoT devices, AI, or quantum computing.

<u>Europol:</u>

- **Cyber Intelligence Sharing:** Foster intelligence sharing. Training sessions discuss platforms, tools, and protocols for securely sharing information on cyber threats across borders.
- **Joint Action and Collaboration:** Trainings cover how different member state agencies can collaboratively respond to significant cross-border cyber incidents, ensuring a unified approach.
- **Specialized Cybercrime Modules**: Specialized modules are offered on areas like dark web operations, cryptocurrency fraud, ransomware, or state-sponsored cyber-attacks.

- **Operational Support:** Training offers operational support to member states during active investigations, including the provision of specialized tools, expertise, and coordination.
- **Legal and Jurisdictional Challenges:** Trainings discuss the legal complexities of cross-border cyber investigations, ensuring that officers know the limitations and protocols when handling such cases.

Both agencies continuously adapt their training programs based on emerging cyber threats, technological advancements, and the ever-evolving digital landscape, ensuring that law enforcement personnel across the EU are prepared to tackle the challenges of the digital age.

2.2.15 Cybersecurity Skills Academy

To overcome the challenge of addressing cybersecurity skills and closing the labour market gap, the European Commission is putting forward a *Cybersecurity Skills Academy* [20], as announced by the President of the European Commission and in the context of the European Year of Skills.

The Cybersecurity Skills Academy aims at creating a single point of entry and synergies for cybersecurity education and training offers, as well as for funding opportunities and specific actions for supporting the development of cybersecurity skills. It will scale up stakeholders' initiatives to reach a critical mass that will make a difference on the labour market, including for defence. Those activities would align along common goals and key performance indicators to seek greater impact.

The focus of the Academy will be the skilling of cybersecurity professionals. The activity of the Academy will feed into to EU policies on cybersecurity, but also into education and lifelong learning. It complements the two Council recommendations related to digital education and skills proposed by the Commission at the same time as this Communication.

The Academy will rely on four pillars:

(1) fostering knowledge generation through education and training by working on a common framework for cybersecurity role profiles and associated skills, enhancing the European education and training offer to meet the needs, building career pathways and providing visibility and clarity over cybersecurity trainings and certifications to enhance the supply side of the labour

(2) ensuring a better channelling and visibility over available funding opportunities for skills-related activities to maximise their impact

(3) calling stakeholders to act

(4) defining indicators to monitor the evolution of the market and be in a capacity to assess the effectiveness of their actions.

The implementation of the Academy will be supported by a EUR 10 million funding from the Digital Europe Programme (DEP). CyberSecPro will highly contribute in the development of the Academy (the project is highlighted in the relevant COM2023).

2.2.16 North Atlantic Treaty Organization (NATO)

The Cybersecurity Certificate Programme [22], in partnership with the Naval Postgraduate School (NPS) in Monterey, California, has initiated a Cyber Security Certificate Programme to enhance cybersecurity training among its members and affiliated partners. This programme aligns with NSO's Cyber Defence Policy, furthering cooperation in cyber defense. It aims to elevate the cyber protection capabilities of NATO and its partner countries, especially for vital communication and information systems. The offered courses, which cater to both security managers and technicians, are highly technical, promoting informed decision-making and fostering better communication with engineering professionals. The learning format is a blend of in-person and online sessions, spanning ten weeks. Participants attend in-person sessions at the NSO during the first and last weeks, while the other weeks involve distance learning overseen by a Senior NPS Computer Science Lecturer. The curriculum includes courses on Network Security, Network Vulnerability Assessment, Incident Handling, Disaster Recovery Planning, and Network Traffic Analysis.

Name of the certifications:

M6-108, "Network Security Course" Aim: To provide a thorough understanding of network security through a "bits-in-transit" approach to all the dominant terminology, principles and technologies. Scoping in this manner permits the delivery of a cohesive course of instruction on network security's core principals, to include the "risk equation", "defence in depth", and what types of attacks exist. Supporting topics include defining what a network is, exploring routers, routing and Access Control List basics, traffic analysis, perimeter defence and Network Intrusion Detection System weaknesses, authentication, and virtual private networks. This course involves one-week resident training at NATO School followed by 8 weeks of distance learning followed by one more week at NATO School.

M6-109, "Network Vulnerability Assessment & Risk Mitigation Course" (NU) Aim: To involve trainees directly with the methodologies and techniques used for vulnerability assessments and follow on mitigation. These methodologies will be reviewed in-depth as they are applied from the vantage point of an evil hacker. Common vulnerabilities will also be studies. Lab exercises will be used to improve the trainee's detailed knowledge of security threats and the methods used to exploit them; leading them to knowledge on the methodologies and motives used by those who will attack the networks they may someday have to defend. This course involves one-week resident training at NATO School followed by 8 weeks of distance learning followed by one more week at NATO School.

M6-110, "Cyber Incident Handling & Disaster Response Course" (NU) Aim: To prepare trainees to address the nature and scope of cyber security incident handling services, including intrusion/incident detection, damage control, service continuity, forensic analysis, service/data restoration, and incident reporting. This course involves one-week resident training at NATO School followed by 8 weeks of distance learning followed by one more week at NATO School.

M6-111, "Network Traffic Analysis" (NU) Aim: To develop students who are able to master the methods and techniques used in gaining deep insight into the operations, use, investigation, and troubleshooting of cyber systems. This course involves one-week resident training at NATO School followed by 8 weeks of distance learning followed by one more week at NATO School.

XX-148 "Principles of Software Reserve Engineering" (NU) Aim: To prepare trainees to apply methodologies and tools used for discerning software functionality and to identify vulnerabilities in that software without prior access to the overarching program design. 10-Week-Course

2.2.17 European Network for Cyber Security (ENCS)

ENCS[23] is a non-profit organisation composed of power grid providers and operators, such as Distribution System Operators (DSOs) and Transmission System Operators (TSOs), and focused on the continuous improvement of cybersecurity in the energy sector. Among its activities, we can find those related to promote specific security training programs related to policy, architecture, and operations, and for different stakeholders such as officers, experts, analysts and managers.

The European Network for Cyber Security (ENCS) plays a crucial role in enhancing cybersecurity across various sectors in Europe, while European Digital Innovation Hubs (EDIHs) focus on supporting digital transformation in businesses and the public sector. The EDIHs are integral to the EU's digital strategy, providing comprehensive support for companies and public sector organizations in their digital transformation. These hubs offer access to technical expertise, innovation services like financing advice and skills development, and guidance on using digital technologies for environmental sustainability. With both regional presence and European network coverage, EDIHs facilitate local support and pan-European knowledge exchange. They are funded jointly by the EU's DIGITAL program and Member

States, with the network enhancing cooperation and knowledge transfer among various stakeholders. ENCS's expertise in cybersecurity can be pivotal for EDIHs, ensuring that digital innovations and transformations they foster are secure and resilient against cyber threats. This collaboration aligns with the broader EU goal of a secure, robust, and digitally advanced Europe.

2.3 Private Commercial Offerings

2.3.1 Information Systems Audit and Control Association (ISACA)

ISACA is a global professional association and learning organization with 170,000 members who work in Digital Trust fields such as information security, governance, assurance, risk, privacy and quality. With a presence in 188 countries and with 225 chapters worldwide, ISACA is recognized around the world for its guidance, credentials, education, training and community. To serve its professional community across the globe, ISACA has established three offices based in North America, Europe and China.

ISACA offers certifications and certificates within the area of Digital Trust. Specifically, the following are offered by ISACA:

ISACA CERTIFICATIONS

CISA—Certified Information Systems Auditor

CISM—Certified Information Security Manager

CRISC—Certified in Risk and Information Systems Control

CGEIT—Certified in the Governance of Enterprise IT

CDPSE—Certified Data Privacy Solutions Engineer

CET—Certified in Emerging Technology

ITCA—Information Technology Certified Associate

CSX-P—CSX Cybersecurity Practitioner Certification

ISACA CERTIFICATES

IT Audit Fundamentals Certificate

IT Risk Fundamentals Certificate

Certificate of Cloud Auditing Knowledge

Cybersecurity Audit Certificate

Computing Fundamentals Certificate

Networks and Infrastructure Fundamentals Certificate

Cybersecurity Fundamentals Certificate

Software Development Fundamentals Certificate

Data Science Fundamentals Certificate

Cloud Fundamentals Certificate

Blockchain Fundamentals Certificate

IoT Fundamentals Certificate

Artificial Intelligence Fundamentals Certificate

COBIT Design and Implementation

Implementing the National Institute of Standards and Technology (NIST) Cybersecurity Framework Using COBIT 2019

COBIT Foundation

For all the areas mentioned above and in the broader subject of Digital Trust, ISACA offers training courses through various platforms (on-line, self-paced, classroom etc). Especially in the area of cybersecurity, ISACA offers courses to prepare candidates for the participation to the relevant certification exams and lab packages aiming to provide the skills of participants in relation to cybersecurity.

2.3.2 Global Information Assurance Certification (GIAC)

GIAC [24] offers a relevant set of certifications for security professionals. Through its extensive portfolio of certifications, GIAC aims to extend and enhance the most practical information security skills and knowledge, considering the following thirteen areas of application:

1. Cloud Security
2. Cyber Defense
3. Cybersecurity and IT Essentials
4. Digital Forensics and Incident Response
5. Incident Response and Threat Hunting
6. Industrial Control Systems Security
7. Offensive Operations
8. Operating System and Device In-Depth
9. Penetration Testing and Red Teaming
10. Purple Team
11. Red Team Operations
12. Security Awareness
13. Security Management, Legal, and Audit

The portfolio of certifications is quite extensive, allowing prospective candidates to select from more than 40 practitioner certifications, including GIAC Security Expert (GSE), GIAC Certified Incident Handler Certification (GCIH), GIAC Certified Forensic Analyst (GCFA) and GIAC Penetration Tester Certification (GPEN). Likewise, GIAC also provides applied knowledge certifications such as GIAC Experienced Cybersecurity Specialist Certification (GX-CS), GIAC Experienced Intrusion Analyst Certification (GX-IA), and GIAC Experienced Incident Handler Certification (GX-IH).

In addition, most of these certifications are aligned with the training programs provided by SANS, ensuring relevant mastery and specialisation in information security-related topics, as indicated in GIAC (2023). Given its relationship with SANS, SANS courses and certifications are listed below.

2.3.3 SysAdmin, Audit, Network, and Security (SANS)

SANS is a private organisation that is focused on educating and empowering cybersecurity practitioners across the globe. SANS offers several cybersecurity courses and certifications. Some of the cybersecurity courses offered by SANS are presented in Table 1. For each course, SANS' associated certification is indicated.

Table 1: Cybersecurity Courses offered by SANS

Courses	Certification
Hacker Tools, Techniques, and Incident Handling	GIAC Certified Incident Handler (GCIH)
Security Essentials - Network, Endpoint, and Cloud	GIAC Security Essentials (GSEC)
Advanced Incident Response, Threat Hunting, and Digital Forensics	GIAC Certified Forensic Analyst (GCFA)
Foundations: Computers, Technology, & Security	GIAC Foundational Cybersecurity Technologies (GFACT)
Enterprise Penetration Testing	GIAC Penetration Tester (GPEN)
Cyber Threat Intelligence	GIAC Cyber Threat Intelligence (GCTI)
Introduction to Cyber Security	GIAC Information Security Fundamentals (GISF)
Security Leadership Essentials for Managers	GIAC Security Leadership (GSLC)
Cloud Security Essentials	GIAC Cloud Security Essentials (GCLD)
Windows Forensic Analysis	GIAC Certified Forensic Examiner (GCFE)
ICS/SCADA Security Essentials	Global Industrial Cyber Security Professional (GICSP)
Enterprise Cloud Forensics and Incident Response	GIAC Cloud Forensics Responder (GCFR)
Security Strategic Planning, Policy, and Leadership	GIAC Strategic Planning, Policy, and Leadership (GSTRT)
Defensible Security Architecture and Engineering: Implementing Zero Trust for the Hybrid Enterprise	GIAC Defensible Security Architecture (GDSA)
Reverse-Engineering Malware: Malware Analysis Tools and Techniques	GIAC Reverse Engineering Malware (GREM)

Network Monitoring and Threat Detection In-Depth	GIAC Certified Intrusion Analyst (GCIA)
Web App Penetration Testing and Ethical Hacking	GIAC Web Application Penetration Tester (GWAPT)
Cloud Security and DevSecOps Automation	GIAC Cloud Security Automation (GCSA)
Cloud Penetration Testing	GIAC Cloud Penetration Tester (GCPN)
Practical Open-Source Intelligence (OSINT)	GIAC Open Source Intelligence (GOSI)
Advanced Penetration Testing, Exploit Writing, and Ethical Hacking	GIAC Exploit Researcher and Advanced Penetration Tester
SANS Training Program for the CISSP Certification	GIAC Information Security Professional (GISP)
SANS Training Program for the CISSP Certification	GIAC Information Security Professional (GISP)
Public Cloud Security: AWS, Azure, and GCP	GIAC Public Cloud Security (GPCS)
ICS Visibility, Detection, and Response	GIAC Response and Industrial Defense (GRID)
Blue Team Fundamentals: Security Operations and Analysis	GIAC Security Operations Certified (GSOC)
Automating Information Security with Python	GIAC Python Coder (GPYC)
Implementing and Auditing Security Frameworks and Controls	GIAC Critical Controls Certification (GCCC)
Defeating Advanced Adversaries - Purple Team Tactics & Kill Chain Defenses	GIAC Defending Advanced Threats (GDAT)
Advanced Network Forensics: Threat Hunting, Analysis, and Incident Response	GIAC Network Forensic Analyst (GNFA)
Building and Leading Security Operations Centers	GIAC Security Operations Manager (GSOM)

2.3.4 International Information System Security Certification Consortium (ISC^2)

The ISC^2 was founded to provide professional cybersecurity education and certification programmes. The courses provided by ISC^2 are delivered under the following certifications.

Certified in Cybersecurity (CC)

Certified Information Systems Security Professional (CISSP)

Systems Security Certified Practitioner (SSCP)

Governance, Risk and Compliance (CGRC)

The Industry’s Premier Secure Software Development Certification (CSSLP)

The HealthCare Security Certification (HCISPP)

Certified Cloud Security Professional (CCSP)

The main security areas addressed by ISC2 through its diverse certifications are as follows:

Cloud Security

Cybersecurity Leadership

Entry-Level Cybersecurity

Governance, Risk and Compliance

Software Security

2.3.5 Computing Technology Industry Association (CompTIA)

CompTIA [25] is an association that promotes business growth through the CompTIA Security+ certification. This type of certification establishes the basic knowledge, (practical) skills and competencies to properly manage networks, systems, software components, hardware components, and data security, as well as the ability to identify vulnerabilities and threats, manage risks/events, governance, response, and provide secure hybrid environments such as cloud-IoT, a response.

CompTIA's Security+ (SY0-601) focuses to prepare contents and skills related to:

1. Attacks, threats and vulnerabilities
2. Architecture and design
3. Implementation
4. Operations and incident response
5. Governance, risk and compliance

As indicated in CompTIA [25], to pass the Security+ exam, prior knowledge on CompTIA Network+ and two years of experience in IT administration with a security focus are required.

3 CSP Cybersecurity Training Course Catalogue

The following CyberSecPro modules include courses, seminars, summer schools, cyber security exercises and that their syllabus and training material will be agreed among partners in order to achieve interoperability among the training offers and mobility among the trainers, trainees and cybersecurity professionals. All HEI academic partners report their modules using the European Credit Transfer and Accumulation System (ECTS), while private CSP partners report their modules based on coursework hours.

3.1 CSP Academic Partners Cybersecurity Course Catalogue

3.1.1 Instituto De Desenvolvimento De Novas Tecnologias-Associacao (Uninova), Portugal

Cybersecurity Executive Program

Strategic Leadership and Governance: This module will focus on providing executives with a strategic understanding of cybersecurity, enabling them to lead cybersecurity initiatives, make informed decisions, and effectively communicate cybersecurity risks and investments to stakeholders.

Incident Response and Risk Management: This module will emphasize the preparedness and response aspects of cybersecurity. Executives will learn how to effectively respond to incidents, manage crises, mitigate risks associated with vendors and third parties, and integrate cybersecurity into business continuity planning.

Emerging Trends and Collaboration: This module will explore emerging trends, technologies, and collaboration in the cybersecurity landscape. Executives will gain insights into ethical and legal implications, international cooperation, cyber threat intelligence, security operations, and the impact of emerging technologies on cybersecurity.

3.1.2 Johann Wolfgang Goethe-Universitaet Frankfurt Am Main (GUF), Germany

Goethe University Frankfurt (GUF) was founded in 1914 as a unique “citizens’ university” financed by wealthy citizens in Frankfurt/Main, Germany, the 5th largest city in Germany and one of the top business and logistics hubs of Germany including critical infrastructures like the management of the .de domain, the country-code top-level domain for Germany, and Frankfurt airport (FRA). Named in 1932 after one of the city’s most famous natives, Johann Wolfgang von Goethe, today the university has over 48,000 students. GUF is the public research university in Frankfurt/Main. A special focus is on integrating cybersecurity education and training into mainstream business informatics courses for general, business, informatics, economics, and business didactic programmes. GUF members have also a significant experience in running summer schools as the IFIP Summer School on Privacy and Identity Management (since 2007 Kai Rannenberg has been active in e.g. the Programme and the Steering Committee).

The training modules offered and the tools used are as follows:

Undergraduate Courses

Wirtschaftsinformatik II (PWIN) (Business Informatics II)

Department: Economics & Business - Students also from Informatics/Computer Science programme

Semester: 3rd - 4th

Course Website: changes per term, but is reachable via https://www.m-chair.de/teaching, e.g. for summer term 2023 https://www.m-chair.de/teaching?view=article&id=259:wirtschaftsinformatik-ii-pwin-summer-2023&catid=15:lectures

ECTS: 6

Contact: Rannenberg, Kai (kai.rannenberg@m-chair.de)

Course Content

- Information Systems I - IS Basics
- Informationssysteme II - Modelle und Architekturen
- Informationssyteme III - Mobile Information Systems
- Communication Systems I - Layer-based Communication
- Communication Systems II - Wired and Wireless Communication
- Management of ICT Projects
- ICS Development I - Software Engineering
- ICS Development II - Object Orientation & UML
- ICS Development III - Markup Languages
- Database Management I - Databases & Data-oriented
- Modelling
- Database Management II - Structured Query Language
- Business Process Reengineering (BPR)

Tools Used*: Visual (graphical) simulation of movement profiles in cellular mobile networks,* https://interactive.zeit.de/opendata/widgets/vorratsdatenspeicherung/index.html

Graduate Courses

Mobile Business I - Technology, Markets, Platforms, and Business Models

Department: Economics & Business - Students also from Informatics/Computer Science and Business Informatics programmes

Semester: 1st - 4th

Course Website: changes per term, but is reachable via https://www.m-chair.de/teaching, e.g. for winter term 2022/2023 https://www.m-chair.de/teaching?view=article&id=42:mobile-business-i-technology-markets-platforms-and-business-models&catid=9:teaching

ECTS: 6

Contact: Rannenberg, Kai (kai.rannenberg@m-chair.de)

Course Content

The "Mobile Business" lecture series provides an introduction to technologies and economic principles defining these markets. Students will be qualified to identify success factors of mobile business models and to judge possible application scenarios. Starting with the basics of mobile communication services, emphasis will be put on an analysis of the interaction between individuals and mobile devices/services.

This includes a historical overview of the development of mobile communication infrastructures, services, and protocols. Based on this, students will be qualified to identify the possibilities and limitations of mobile business applications and business models in order to consider the resulting opportunities and challenges when deriving the success factors. Characteristic attributes of mobile services, especially in contrast to electronic services, will be outlined and considered in an analysis of the current market environment for mobile business applications. Furthermore, traditional as well as emerging business models will be discussed. The course concludes with a presentation and discussion of several exemplary application scenarios. Students will be able to reflect on specific attributes of mobile applications, analyse new scenarios, and draw connections to traditional and established scenarios.

The 2nd part of this lecture series (Mobile Business II) focuses on the variety of opportunities and challenges that are offered by mobile communication technologies and their specific properties and which need to be considered and addressed by companies and regulators. The overall objective of the course is to provide advanced knowledge about mobile applications and mobile services, ranging from technical to economic aspects. Students will be qualified to realise the inherent commercial potential proactively and to identify and address challenges and problems in the area of mobile business. An important facet of this is the discussion of international regulation and its implications on the development and application scenarios for mobile services.

Architectures for mobile services and their development are the focus of the first part of the course. This includes topics such as security and privacy, usability, and the role of standardisation. The presentation of exemplary application areas will allow students to understand and question how different design aspects are considered in current scenarios. The course concludes with a state-of-the-art overview of current mobile business research topics and activities, enabling students to understand the lines of research and draw connections to already existing mobile business applications and scenarios.

Sequence of lectures:

- Mobile Telecommunication Infrastructures
- Wireless Internet-oriented Infrastructures and Protocols
- Mobile Communication Services
- E-Business vs. M-Business
- Market Structure and Value Chain
- Business Models
- Smartcards and Infrastructures
- Mobile Devices
- Concepts of Mobile OS
- Mobile OS and Security Aspects - Examples
- Trusted Devices
- Acceptance and Success Factors in Mobile Business
- Current Research
- Selected and varying contributions from (industry) guest speakers, e.g.
- Privacy and Innovations: How firms can leverage privacy
- To gain competitive advantages
- Privacy in connected car scenarios
- 5G networks and security evaluation

***Tool Used**: Visual (graphical) simulation of movement profiles in cellular mobile networks,* https://interactive.zeit.de/opendata/widgets/vorratsdatenspeicherung/index.html

<u>Mobile Business II - Technology, Markets, Platforms, and Business Models</u>

Department: Economics & Business - Students also from Informatics/Computer Science and Business Informatics programmes

Semester: 1st - 4th

Course Website: changes per term, but is reachable via https://www.m-chair.de/teaching, e.g. for summer term 2023 https://www.m-chair.de/teaching?view=article&id=260:mobile-business-ii-application-design-applications-infrastructures-and-security-summer-2023&catid=2:uncategorised

ECTS: 6

Contact: Rannenberg, Kai (kai.rannenberg@m-chair.de)

Course Content

The "Mobile Business" lecture series provides an introduction to technologies and economic principles defining these markets. Students will be qualified to identify success factors of mobile business models and to judge possible application scenarios. Starting with the basics of mobile communication services, emphasis will be put on an analysis of the interaction between individuals and mobile devices/services.

This includes a historical overview of the development of mobile communication infrastructures, services, and protocols. Based on this, students will be qualified to identify the possibilities and limitations of mobile business applications and business models in order to consider the resulting opportunities and challenges when deriving the success factors. Characteristic attributes of mobile services, especially in contrast to electronic services, will be outlined and considered in an analysis of the current market environment for mobile business applications. Furthermore, traditional as well as emerging business models will be discussed. The course concludes with a presentation and discussion of several exemplary application scenarios. Students will be able to reflect on specific attributes of mobile applications, analyse new scenarios, and draw connections to traditional and established scenarios.

The 2nd part of this lecture series (Mobile Business II) focuses on the variety of opportunities and challenges that are offered by mobile communication technologies and their specific properties and which need to be considered and addressed by companies and regulators. The overall objective of the course is to provide advanced knowledge about mobile applications and mobile services, ranging from technical to economic aspects. Students will be qualified to realise the inherent commercial potential proactively and to identify and address challenges and problems in the area of mobile business. An important facet of this is the discussion of international regulation and its implications on the development and application scenarios for mobile services.

Architectures for mobile services and their development are the focus of the first part of the course. This includes topics such as security and privacy, usability, and the role of standardisation. The presentation of exemplary application areas will allow students to understand and question how different design aspects are considered in current scenarios. The course concludes with a state-of-the-art overview of current mobile business research topics and activities, enabling students to understand the lines of research and draw connections to already existing mobile business applications and scenarios.

Sequence of lectures:

- Positioning Methods for Location-based Services
- LBS Business Models
- Cryptography
- Electronic Signatures
- Data Protection / IdM
- Regulation of Mob. Telec.
- Regulation by Licensing
- LBS and Mobile Communities
- M-Payment I
- M-Payment II

- HCI Issues
- Regulation
- Design Evaluation
- Current Research
- Selected and varying contributions from (industry) guest speakers, e.g.
- § Cryptocurrency Adoption

Tool Used*: Visual (graphical) simulation of movement profiles in cellular mobile networks,* https://interactive.zeit.de/opendata/widgets/vorratsdatenspeicherung/index.html

Information & Communication Security

Department: Economics & Business - Students also from Informatics/Computer Science and Business Informatics programmes

Semester: 1st - 4th

Course Website: changes per term, but is reachable via https://www.m-chair.de/teaching, e.g. for summer term 2022 https://www.m-chair.de/teaching/courses?view=article&id=61:information-communication-security&catid=9:teaching

ECTS: 6

Contact: Rannenberg, Kai (kai.rannenberg@m-chair.de)

Course Content

- Authentication
- Access Control
- Cryptography I
- Cryptography II
- Electronic Signatures
- Identity Management
- Privacy Protection I
- Privacy Protection II
- Computer System Security
- Network Security I
- Network Security II
- Selected and varying contributions from (industry) guest speakers, e.g.
- Security Management
- Biometrics

Tool Used: *Visual (graphical) simulation of movement profiles in cellular mobile networks,* https://interactive.zeit.de/opendata/widgets/vorratsdatenspeicherung/index.html

3.1.3 Laurea University of Applied Sciences, Finland

Undergraduate Courses

The ICT Environment and Infrastructure

Department: ICT & Cybersecurity (Laurea Leppävaara, tiko)

Semester: 1st

Course Website: https://ops.laurea.fi/212701/en/69076/230740/2521/0/27154

ECTS: 5

Contact: Outi Grotenfelt/Lassi Virtanen (outi.grotenfelt@laurea.fi, lassi.virtanen@laurea.fi)

Course Content

Description of the processes of information systems development, implementation and maintenance

Description of the structure and operational environment of information systems

Identification of typical threats related to information security

Data Networks and Information Security

Department: ICT & Cybersecurity (Laurea Leppävaara, tiko)

Semester: 2nd

Course Website: https://ops.laurea.fi/212701/en/69076/230740/2521/0/27157

ECTS: 5

Contact: Seppo Koponen/Riku Salmenkylä (Seppo.Koponen@laurea.fi, Riku.Salmenkyla@laurea.fi)

Course Content

Description of the structure and operation of data networks in relation to the following terms: Local area networks, wireless networks, the Internet

Description of the functionality of IP-networks and key internet protocols

Implementation and maintenance of basic services in a local area network

Justification of the importance of information security according to the CIA (Confidentiality, Integrity and Availability) model

Identification of common information security threats faced by organisations

Implementation of basic level information security safeguards for local area network

Information Management and Databases

Department: ICT & Cybersecurity (Laurea Leppävaara, tiko)

Semester: 1st

Course Website: https://ops.laurea.fi/212701/en/69076/230740/2521/0/27156

ECTS: 5

Contact: Jukka Malinen/Outi Grotenfelt (Jukka.Malinen@laurea.fi, Outi.Grotenfelt@laurea.fi)

Course Content

Design and implementation of databases

Management and usage of databases

Query languages to search and modify data in a database

Tools Used: SQL

Internet Infrastructure and Security

Department: ICT & Cybersecurity (Laurea Leppävaara, tiko)

Semester: 3rd

Course Website: https://ops.laurea.fi/212701/en/69076/230740/2521/0/34032

ECTS: 5

Contact: Seppo Koponen/Riku Salmenkylä/Anssi Mattila (Seppo.Koponen@laurea.fi, Riku.Salmenkyla@laurea.fi, Anssi.M.Mattila@laurea.fi)

Course Content

Comprehension and description of the operations and protocols in global IP networks

Calculation of IP subnets and supernets

Comprehension and description of security vulnerabilities in IP network infrastructure

Comparison and contrasting of IPv6 to IPv4

Comprehension and description of the functional concepts and security risks in wireless networking

comprehension and description of the functional concepts and security risks in cloud computing

Tools Used: Cisco Packet Tracer

Fundamentals of Programming

Department: ICT & Cybersecurity (Laurea Leppävaara, tiko)

Semester: 2nd

Course Website: https://ops.laurea.fi/212701/en/69076/230740/2521/0/26625

ECTS: 5

Contact: Katja Henttonen (Katja.Henttonen@laurea.fi)

Course Content

Fundamental syntax and building blocks of programming languages

Planning, implementation and testing of small-scale programs in accordance with the best practices of programming

Tools Used: Python and Visual Studio Code

Foundations of Web Development

Department: ICT & Cybersecurity (Laurea Leppävaara, tiko)

Semester: 2nd

Course Website: https://ops.laurea.fi/212701/en/69076/230740/2521/0/27155

ECTS: 5

Contact: Outi Grotenfelt (Outi.Grotenfelt@laurea.fi)

Course Content

Design and implementation of web sites using fundamental web development tools and techniques

Design, create, and publish www content

Design and implement web site layouts according to customer needs

Evaluate web site development needs

Tools Used: HTML5, CSS3, JavaScript

Network Applications

Department: ICT & Cybersecurity (Laurea Leppävaara, tiko)

Semester: 3rd

Course Website: https://ops.laurea.fi/212701/en/69076/230740/2521/0/26590

ECTS: 5

Contact: Seppo Koponen/Riku Salmenkylä (Seppo.Koponen@laurea.fi, Riku.Salmenkyla@laurea.fi)

Course Content

Design and implementation of web sites using fundamental web development tools and techniques

Development and management of LAN services

Identification of common network applications for companies

Network application security threats.

Planning, designing, development and implementation of secure ICT infrastructure with needed network applications

Tools Used: Cisco Packet Tracer

Introduction to Information Security

Department: ICT & Cybersecurity (Laurea Leppävaara, tiko)

Semester: 3rd

Course Website: https://ops.laurea.fi/212701/en/69076/230740/2521/0/34034

ECTS: 5

Contact: Pasi Kämppi Paresh Rathod (Paresh.Rathod@laurea.fi, Pasi.Kamppi@laurea.fi)

Course Content

Act ethically as a member of study group and community

Recognize and comprehend the importance of confidentiality, integrity and availability model for the information and cybersecurity

Recognize and comprehend different threats, attacks and vulnerabilities

Comprehend and describe security technologies and tools

Comprehend and describe security architectures and designs

Comprehend and describe identity and access management approaches

Comprehend, describe and apply risk management principles

Comprehend and describe cryptography and PKI concepts

Differentiate cybersecurity domains and subdomains from each other

Comprehend and explain the importance of the cybersecurity in the modern society

Reflect and develop their own learning process

Tools Used: Embedded Linux Shell with iFrame (HTML based shell), PicoCTF (Catch the flag platform)

Information Security Management

Department: Business information technology (Laurea University of Applied Sciences)

Semester: 3rd

Course Website: https://ops.laurea.fi/212701/en/69076/230740/2521/0/34035

ECTS: 5

Contact: Pasi Kämppi (pasi.kamppi@laurea.fi), Paresh Rathod (paresh.rathod@laurea.fi)

Course Content

Information security program, development and management principles

Risk management, incident management and compliance principles

Risk assessment process

Typical information security management related problems and draw solutions to them

Tools Used: Risk assessment sheet with Word or Excel, OSINT framework

Enterprise Security and Practitioners

Department: Business information technology (Laurea University of Applied Sciences)

Semester: 4th / 5th

Course Website: https://ops.laurea.fi/212701/en/69076/230740/2521/0/34036

ECTS: 5

Contact: Paresh Rathod (paresh.rathod@laurea.fi), Pasi Kämppi (pasi.kamppi@laurea.fi)

Course Content

Identification of threats, vulnerability and risks associated with web applications and web servers

Common attack tactics, techniques used when hacking web servers, applications and wireless networks

Security controls for information systems against common threats

Hacking exercises in virtualized training environment

Tools Used: Virtual Practice Labs Environment for CASP KAs (proprietary third-party environment)

Cybersecurity Analyst

Department: Business information technology (Laurea University of Applied Sciences)

Semester: 4th / 5th

Course Website: https://ops.laurea.fi/212701/en/69076/230740/2521/0/34037

ECTS: 5

Contact: Paresh Rathod (paresh.rathod@laurea.fi), Pasi Kämppi (pasi.kamppi@laurea.fi)

Course Content

Network discovery, reconnaissance, harvesting and vulnerability analysis techniques

Tools for network discovery reconnaissance, harvesting and vulnerability analysis

Network vulnerabilities with network discovery, reconnaissance, harvesting and analysing tools

Reducing the attack surface of a network host

Presenting the results of network reconnaissance and vulnerability analysis in professional format

Tools Used: Virtual Practice Labs Environment for CySA+ KAs (proprietary third-party environment)

Network and Applications Security

Department: Business information technology (Laurea University of Applied Sciences)

Semester: 4th / 5th

Course Website: https://ops.laurea.fi/212701/en/69076/230740/2521/0/34039

ECTS: 5

Contact: Paresh Rathod (paresh.rathod@laurea.fi), Pasi Kämppi (pasi.kamppi@laurea.fi)

Course Content

The role of ethical hacking in the offensive and defensive network and applications security

Penetration testing processes including footprinting, reconnaissance, scanning networks, enumeration, vulnerability analysis and system hacking

Tools and techniques used in penetration testing process

Security controls to network security based on vulnerability analysis

Common penetration testing tools in virtualized training environment

Tools Used: Virtual Practice Labs Environment for CEH KAs (proprietary third-party environment)

Systems Security

Department: Business information technology (Laurea University of Applied Sciences)

Semester: 4th / 5th

Course Website: https://ops.laurea.fi/212701/en/69076/230740/2521/0/34040

ECTS: 5

Contact: Paresh Rathod (paresh.rathod@laurea.fi), Pasi Kämppi (pasi.kamppi@laurea.fi)

Course Content

Threats, vulnerabilities and risks associated with organisation’s systems

Confidentiality, integrity and availability model for the information and cybersecurity in practice

Differences regarding different cryptographic methods, its applications and techniques

Risk assessment, risk analysis and risk management

Security controls for workstation and server environments

Authentication and authorization mechanisms

Tools Used: Virtual Practice Labs Environment for CISSP KAs (proprietary third-party environment)

Cybersecurity Project

Department: Business information technology (Laurea University of Applied Sciences)

Semester: 4th / 5th

Course Website: https://ops.laurea.fi/212701/en/69076/230740/2521/0/34078

ECTS: 5

Contact: Jyri Rajamäki (jyri.rajamaki@laurea.fi)

Course Content

Working as a member cybersecurity analyst team (project target varies including research, innovation, business, cyber ranges, cyber drill or cyber defense projects)

Ethical actions as a member of team, community and working-life partners

Planning, implementation and documentation of a cybersecurity research project

Frameworks and methods for cybersecurity research project

Presenting research results in the academic and business format

Cybersecurity professional practices and applying practitioners' skills in the community

Cybersecurity Hackathon Project

Department: Business information technology (Laurea University of Applied Sciences)

Semester: 4th / 5th

Course Website: https://ops.laurea.fi/212701/en/69076/230740/2521/0/34042

ECTS: 3

Contact: Pasi Kämppi (pasi.kamppi@laurea.fi), Paresh Rathod (paresh.rathod@laurea.fi)

Course Content

Working as a member cybersecurity analyst team (project target varies including research, innovation, business, cyber ranges, cyber drill or cyber defence projects)

Participating and acting ethically as a member of team, community and working-life partners

Selecting appropriate tools and strategies for network reconnaissance and vulnerability analysis project in real exercise or company environment

Presentation of the results of network reconnaissance and vulnerability analysis in a professional format

Critical analysis of the project outcomes

Tools Used: Kali Linux, Nessus, Burpsuite, Nmap, Sqlmap, OWASP ZAP, OWASP Websccarab, Hydra, Drupageddon2, Metasploits, Social engineering tookit, Curl, Nikto, Gobuster, WP Zoom, Hascat, Wireshark, Dirb, John the Ripper, Dirbuster, Ncrack, Metagoofil, Wappalyzer, Wfuzz, XSStrike, XSS Hunter, WhatWeb

Cybersecurity Working Life Practices

Department: Business information technology (Laurea University of Applied Sciences)

Semester: 4th / 5th

Course Website: https://ops.laurea.fi/212701/en/69076/230740/2521/0/34043

ECTS: 2

Contact: Pasi Kämppi (pasi.kamppi@laurea.fi), Paresh Rathod (paresh.rathod@laurea.fi)

Course Content

Cybersecurity professional working life events including industrial visits, seminars, workshops, hands-on, cyber ranges, cyber drill and cyber defense activities

Ethical actions as a member of team, community and working-life partners

Networking with other cybersecurity professionals

Cybersecurity professional practices and applying practitioners' skills in the community

Tools Used: Splunk, BOTSv3, Google dork sheets, Google dork sheets, Shodan, DNS Dumbster, OpintelLinks, Exploit Database, Dorksearch, Investigator, Similarweb, Builtwith, Virustotal, Reallygoodemails

Information and Cyber Security

Department: Safety, Security and Risk Management (Laurea University of Applied Sciences)

Semester: 1st

Course Website: https://ops.laurea.fi/212701/fi/68153/206649/2497

ECTS: 5

Contact: Seija Tiainen (seija.tiainen@laurea.fi), Rauno Hammarberg (rauno.hammarberg@laurea.fi), Veli Sulkava (veli.sulkava@laurea.fi)

Course Content

The key principles of information and cyber security

The basis of requirements set for information and cyber security and best practices

Information and cyber security risks management

Procedures and instructions related to information and cyber security

Information and Cyber Security Management

Department: Safety, Security and Risk Management (Laurea University of Applied Sciences)

Semester:

Course Website: https://ops.laurea.fi/212701/fi/68153/206649/2497

ECTS: 10

Contact: Anja Aatsinki (anja.aatsinki@laurea.fi), Kaci Bourdache (kaci.bourdache@laurea.fi), Veli Sulkava (veli.sulkava@laurea.fi)

Course Content

Requirements and best practices for information and cyber security

Information and cyber security risks management

Administrative, operational, technical and structural procedures

Information and cyber security planning, evaluation and development

Post-graduate Courses

Cyber Security Management

Department: Security Management (Laurea University of Applied Sciences)

Semester:

Course Website: https://ops.laurea.fi/68096/fi/68153/69176/2536

ECTS: 5

Contact: Anssi Mattila (anssi.m.mattila@laurea.fi)

Course Content

The importance of cyber security and impact on the operations of companies and organisations

Critical threats and risks from information networks to companies and organisations

Organisation's information security, risk management and continuity management

Professional courses / Training / Executive education

Risk Manager

Department: Advanced Training in Security and Risk Management (Laurea University of Applied Sciences)

Semester:

Course Website: https://www.laurea.fi/koulutus/taydennyskoulutukset/risk-manager--koulutus/

ECTS: 5

Contact (responsible teacher first): Soili Martikainen (soili.martikainen@laurea.fi), Veli Sulkava (veli.sulkava@laurea.fi), Katja Suonperä (katja.suonpera@laurea.fi)

Course Content

- Threat identification
- Security of information systems
- Standards

3.1.4 Polytechneio Kritis (Technical University of Crete), Greece

UnderGraduate Courses

Computer Organization

Department: School of Electrical and Computer Engineering (TUC)

Semester: 6st Semester
Course Website: https://www.eclass.tuc.gr/modules/contact/index.php?course_id=1219

ECTS: 5

Contact: Ioannidis Sotirios (sioannidis@tuc.gr)

Course Content

The course covers the principles of computer organization, including the design of computer hardware, software, and firmware. It also covers topics such as: Digital logic circuits, Boolean algebra, logic gates, combinational and sequential circuits, and flip-flops. Computer arithmetic: Number systems, arithmetic operations, floating-point arithmetic, and error analysis. Processor organization: Instruction set architecture, pipelining, instruction-level parallelism, and memory hierarchy. Memory organization: Memory technology, cache memory, virtual memory, and memory management. Input/output organization: I/O devices, interrupts, DMA, and bus architecture. Multiprocessing: Symmetric multiprocessing, cache coherence, and memory consistency. Computer system performance: Metrics, benchmarks, and evaluation techniques.

Security of Systems and Services

Department: School of Electrical and Computer Engineering (TUC)

Course Website: https://www.eclass.tuc.gr/courses/HMMY270/

ECTS: 5

Contact: Ioannidis Sotirios (sioannidis@tuc.gr)

Course Content

The course focuses on the concepts of confidentiality, integrity, and availability of data and the different security measures to ensure these properties. There is also an overview of basic security concepts, including threat models, risk analysis, and attack vectors. It then covers various security mechanisms, such as authentication, access control, encryption, and firewalls. The course also covers some common attacks and countermeasures, such as denial-of-service (DoS) attacks, buffer overflows, and malware. Some topic that there is an introduction of them are: network security, web security, mobile security, cloud security, and cryptography. Students will also learn about different security policies and standards.

Master Courses

Advantage Computer Architecture

Department: School of Electrical and Computer Engineering (TUC)

Semester: Spring Semester

Course Website: https://www.eclass.tuc.gr/courses/HMMY174/

ECTS: 5

Contact: Ioannidis Sotirios (sioannidis@tuc.gr)

Course Content

In this course the main purpose is to learn about the state-of-the-art technologies in the Computer Architecture field. In order to do that there is an analysis in the literature of the field. Reading recent papers, as well as tools that are state-of-the-art nowadays.

3.1.5 Tallinn University of Technology, Estonia

Introduction to Cybersecurity

Estonian Maritime Academy

Semester: Spring

Course Website: https://ois2.ttu.ee/uusois/subject/VLL1480

ECTS: 6

Language: Estonian (Some English guest lecturing)

Contact: Dan Heering (Dan.Heering@taltech.ee)

Course Content

The aim of the course is to give an overview of cyber security in general and related threats to ships, organizations and individuals.

The student:

- understands the concept of the security;
- understands the terminology of cyber security;
- understands the main cyber risks and threats to ships and organisations;
- is familiar with the cyber security guidelines developed for maritime sector;
- understands the main threats to information society, the main courses and outcomes of the problems in information security;
- is able to employ best practices of cyber hygiene and can also explain them to others;
- understands the ethical aspects of cyber security.

Tools Used: Moodle

Strategic Communications and Cybersecurity

IT – Department of Software Science

Semester: Spring

Course website: https://ois2.ttu.ee/uusois/subject/ITC8320

ECTS: 6

Language: English

Contact: Adrian Nicholas Venables (adrian.venables@taltech.ee)

Course Content:

In July 2016, NATO recognised cyberspace as a domain of operations in which the alliance must defend itself as effectively as it does in the air, on land and at sea. Within the cyber domain, information is used as the weapon to achieve objectives at the strategic, operational and tactical levels and this course focuses on how can be used in offensive and defensive contexts. A reoccurring theme throughout the course is the nature of power projection and how the behaviour of target audiences can be influenced through operations in cyberspace. This is achieved through several means, including Strategic

Communications, Information Operations, Influence Activities and related disciplines, each of which is the theme of an individual lecture. Each subject is discussed in terms of its wider context and how cyber operations can contribute to their success. The role of cybersecurity is emphasized throughout as either facilitating the success of a friendly force activity or in preventing an adversary from being successful in their operations. The leadership and management of cyber capabilities is discussed with dedicated time devoted to the development and implementation of cybersecurity strategy and policy. This will equip the students with the information they need to utilise the material that they have studied in a range of scenarios in their future employment in cyber security. This course aims to provide students with a wider contextualisation of the role of cybersecurity in the information environment and how it contributes to a nation's Strategic Communications strategy. The general objective of the course is to provide a broader understanding of how students' technical knowledge and skills can contribute to the production of cyber security strategy and policy.

By the end of the course the student will:

- understand and explain the nature of cyberspace beyond that of a purely technical description;
- understand the concept on Strategic Communication and Information Operation, is familiar with different Influence Activities and is able to discuss in their related disciplines;
- is able to analyse and explain the role of strategy, policy, processes and procedures in achieving national objectives in the information environment;
- understand and describe the nature of hybrid warfare and asymmetric operations in the "grey zone" of conflict;
- understand how the behaviour of target audiences are influenced through the use of strategic communication and understand the role of cyber security in facilitating or denying those activities.

Tools Used: Moodle

Cyber Incidence handling

IT – Department of Software Science

Semester: Autumn

Course website: https://ois2.ttu.ee/uusois/subject/ITC8270

ECTS: 6

Language: English

Contact: Rain Ottis (Rain.Ottis@taltech.ee)

Course Content:

The aim of this course is to give the student foundational knowledge required to work in a Security Operation Center (SOC) and participate in cyber incident response.

On completion of the course the student:

- Triage and basic incident handling
- Creating incident handling procedures and testing
- Large scale incident handling
- Cooperation with Law Enforcement agencies
- Identifying and handling cyber-crime traces
- Incident handling and cooperation during phishing campaign
- Law enforcement view of computer security incidents
- Law enforcement needs for evidence analysis

- Role of (tabletop) exercises in developing incident handling capability
- After completing this course, the student:
- is able to establish incident handling team and typical team designs;
- manages cyber incidents, preserving needed evidence and chain of evidence;
- builds incident management system and manages cooperation between law enforcement and incident handlers;
- establishes procedures for evidence and incident management.

Tools Used: Platform: Moodle

CyberDefense Monitoring Solutions

IT – Department of Software Science

Semester: Autumn

Course website: http://ois2.ttu.ee/uusois/subject/ITX8071

ECTS: 6

Language: English (only 5 extra students allowed)

Contact: Risto Vaarandi (Risto.Vaarandi@taltech.ee)

Course Content:

Main monitoring solutions and techniques in cyber defense. Log and event generation for firewalls, IDS/IPS sensors, services, and applications. Collecting and monitoring logs and events. Intrusion detection and prevention.

On completion of the course the student:

- has an overview of the principles and standards of log collecting (BSD and IETF syslog)
- can tune the UNIX logging software syslogd, rsyslog ja syslog-ng
- is able to filter the network packets and generate log messages using netfilter firewall
- knows different dialects of the regular expression languages (ERE, Perl) and is able to use these in the log monitoring
- has an overview of the event correlation principles
- is able to correlate events using Simple Event Correlator and use it for discovering and responding to attacks using different correlation techniques
- has an overview of the network-based intrusion detection and prevention systems (network IDS/IPS)
- is able to use Snort for intrusion detection and prevention

Tools Used: Platform: Moodle, UNIX logging software syslogd, rsyslog ja syslog-ng

3.1.6 University of Malaga (UMA), Spain

The University of Malaga (UMA) was founded in 1972 with the Decree 2566/1972 ([BOE-A-1972-1400). The university began its activity in the Campus of El Ejido, and continued its expansion in the Campus of Teatinos where it continues to grow, not only in infrastructure and degrees offered, but also in national and international prestige, collaborating with various entities.

The educational offer of UMA is developed in five branches of knowledge: Arts and Humanities, Social and Legal Sciences, Health Sciences, Sciences and Engineering and Architecture. On the Engineering side, UMA offers a MSc. program in “Computer Science” with specialisation in cybersecurity, a recent specific BSc. program in "*Cybersecurity and Artificial Intelligence*", and several courses in Computer Science BSc. programs in cybersecurity. All these programs are under the control of the Computer Science Department of UMA, which also offers cybersecurity courses in other degrees of other faculties to complement and prepare experts in their respective disciplines.

More particularly, these courses (along with their respective tools) are as follows:

Graduate Courses

Design and Configuration of Secure Networked Systems

Department: Computer Science, Master's Degree in Computer Engineering with specialisation in Cybersecurity

Semester: 1st

Course Website: https://www.uma.es/centers/subject/5296/102673/

ECTS: 6,0

Contact: Javier Lopez (javierlopez@uma.es)

Course Content

This course aims to lay the foundations for understanding the structure and motivation of the problem of security in computer networks and the fundamental principles on which to support and develop their learning. This knowledge will help to address the following blocks of content. These blocks focus on acquiring a thorough understanding of attacks at different levels of the network, the security requirements necessary to mitigate these attacks, as well as an overview of the countermeasures to be taken in order to harden the network system.

In particular, this course focuses the following aspects:

Foundations: Introduction to cyber-security (sources and motives of cybersecurity threats, sources of vulnerabilities, and types of threats in network security), and network perimeter basics (network elements, protocols, and attacks landscape).

Network hardening: Switches and routers hardening (attacks to switches and countermeasures, attacks to routers and countermeasures, and wireless hardening), firewalls hardening (firewall features, type of network firewalls and checklists, and firewalls configuration and location), and intrusion detection and prevention systems (fundamentals, categories and deployment architectures, honeypots, and tools for testing).

Hardening infrastructure systems: Harden the operating system (Linux security, Windows security, and vulnerability analysis), and Security Information and Event Management (SIEM) systems (characteristics and purpose of a SIEM, basic steps and requirements to configure a SIEM, and Security Operations Center (SOC)).

Tools Used: GNS3, GNS3 VM, Virtualbox / VMWare, Mikrotik, Containers, SCP, Putty, Etherape, Nmap, Hping3 / nping, Legion, Etthercap / ARPSpoof, Yersinia, Scpay, Netstat, OPenVPN, OpenSSL, XCA, Metasploitable 2, Snort, Snorpy, IPTables, OpenVAS / Nessus, Kali Linux / Parrot.

Security and Privacy in Application Environments

Department: Computer Science, Master's Degree in Computer Engineering with specialisation in Cybersecurity

Semester:2nd

Course Website: https://www.uma.es/departments/subjects/titulation/102674/5296/

ECTS: 4,5

Contact: Ruben Rios (ruben.rdp@uma.es)

This course aims to provide a high-level overview of the security and privacy challenges in IoT and Cloud scenarios and the security techniques used in each; analyse different security issues in web environments and associated best practices; and iii) discuss different security techniques that have emerged in recent years to address security and privacy issues in complex scenarios.

In particular, this course focuses the following aspects:

Course Content

- End-to-end Encryption in IoT
- Cloud data security
- Data Anonymization
- Online tracking and fingerprinting
- HTTP Security headers / Certificate transparency
- SSL/TLS vulnerabilities
- Web Input Validation
- Cryptographic primitives for PETS

Tools Used: Python cryptography library, Google Cloud KMS, Amazon KMS, ARX, OWASP OWASP Secure Headers Project, OWASP Vulnerable Web Applications, OWASP Zap, Github repositories.

Security in Industrial and Cyber-Physical systems

Department: Computer Science, Master's Degree in Computer Engineering with specialization in Cybersecurity

Semester: 3rd

Course Website: https://www.uma.es/departments/subjects/titulation/102688/5296/

ECTS: 4,5

Contact: Cristina Alcaraz (alcaraz@uma.es)

Course Content

This course is focused on the security and privacy issues related to the deployment of Cyber-Physical Systems (CPSs), including their secure interactions with related technologies, such as the (Industrial) Internet of Things and Cloud Computing, and their secure integration with Smart Infrastructures, including smart industries, smart cities, smart homes, and smart healthcare. The main goal of this course is to provide students with the necessary knowledge and tools to analyse, select, develop, deploy, and evaluate security solutions in these heterogeneous and complex ecosystems.

In particular, this course focuses the following aspects:

Connecting cyber-physical systems to smart environments: Fundamentals of CPS, CPS-related technologies, smart ecosystems, integration of CPS and related technologies, and communication protocols in an interconnected world.

Security issues in a smart world: Security and privacy problems and requirements, and threat taxonomy and practical cases.

Secure interconnection of smart devices: Secure primitives, secure communication channels, and authentication and access control.

Advanced cyber-physical systems security in smart environments: Trust and privacy, attack prevention and detection, and advanced protection services.

Tools Used: GNS3, GNS3 VM, Virtualbox / VMWare, Mikrotik, ESP32 (Arduino), Raspberry Pi, Nmap, Hping3 / nping, Etthercap / ARPSpoof, Scapy, Wireshark (for ModbusTCP, OPC-UA), Python (pycryptodome), XCA, Anomaly-based IDS (Machine-Learning models), Snort / Suricata.

Malware Analysis

Department: Computer Science, Master's Degree in Computer Engineering with specialization in Cybersecurity

Semester: 3rd

Course Website: https://www.uma.es/centers/subject/5296/102684/

ECTS: 4,5

Contact: José A. Onieva (onieva@uma.es)

Course Content

This course aims to introduce the students to malware analysis techniques through interactive readings and analysis of malware samples. In particular, this course focuses the following aspects:

Malware analysis introduction: Malware analysis techniques, types of malware, and malware analysis in controlled environments (sandboxes, Virtual Machines, network configuration and tools for malware analysis).

File static analysis: Hashing: a fingerprint for malware, strings, packed and obfuscated malware, PEF, DLLs and functions.

Basic dynamic analysis: Monitoring and registry snapshots, diffing, API tracing, and other related issues.

Advanced static analysis: Windows internals, reverse program blocks, and reverse engineering.

Advanced Dynamic Analysis: debugging.

Tools Used: REMNUX toolset**,** VirtualBox, IDA Pro Educational, Wireshark, Regshot, PEStudio, CFF Explorer, Process Explorer, Autoruns, ProcMon.

Computer Forensics

Department: Computer Science, Master's Degree in Computer Engineering with specialization in Cybersecurity

Semester: 3rd

Course Website: https://www.uma.es/departments/subjects/titulation/102683/5296/

ECTS: 4,5

Contact: Rodrigo Román (rroman@uma.es)

Course Content

During this course, the student will acquire the technical skills to carry out computer forensic analysis and those methodologies that are fundamental for the successful training of a forensic computer practitioner. In particular, the course covers in a horizontal manner the different phases of identifying, obtaining, analysing and presenting electronic evidence. These skills will be consolidated through a complete use case.

This course includes the following sections:

- Computer forensics fundamentals: Past, present and future of digital forensics, International standards and practices, and anti-Forensics

- Gathering Digital Evidence: Sources of digital evidence, and tools and procedures for gathering digital evidence
- Analysing digital evidence: Tools and procedures for analysing Digital Evidence.

Tools Used: FTK Imager, Autopsy, Volatility, John the Ripper, THC-Hydra, ExifTool, OpenPuff, Veracrypt.

Secure Coding

Department: Computer Science, Master's Degree in Computer Engineering with specialization in Cybersecurity

Semester: 3rd

Course Website: https://www.uma.es/centers/subject/5296/102686/

ECTS: 4,5

Contact: José A. Montenegro Montes (jmmontes@uma.es)

Course Content

This course covers the principles and practices of secure programming. More specifically, it shows security models, threats, design principles and secure coding practices. A developer with the proper knowledge of these techniques will minimize vulnerabilities in the software, avoiding that the developed software can be vulnerable and exposed to possible attacks. For the development of the subject from the theoretical and practical point of view, the course contemplates the role of the most representative platforms, from traditional platforms to mobile devices, including web platforms.

In particular, this course focuses the following aspects:

- Introduction to Secure Coding
- Application Security - Linux and Windows Platforms
- Statics Analysis
- Web Security
- Mobile Security
- Machine Learning Security

Tools Used: Gdb, Immunity Debugger, Visual C, Cppcheck, Sonarqube, OWASP ZAP, Drozer y Sieve, Python, Jupiter.

Undergraduate Courses

Foundations of Cybersecurity

Department: Computer Science, Bachelor's Degree in "Cybersecurity and Artificial Intelligence".

Semester: 1st

Course Website: Not yet available (Course 2023-2024)

ECTS: 6

Contact: Javier Lopez (javierlopez@uma.es)

Course Content

This course provides the core concepts and competences related to cybersecurity. As such, its goal is to allow students to assess the main security threats and their impact on networks and information systems, and to distinguish the different security protocols and services applicable to protection against the most common threats. For this purpose, the course not only introduces the main challenges and risks, but also introduces the most important security services in terms of primitives, algorithms, and protocols.

For this reason, this course includes the following sections:

Introduction to Cybersecurity: Basic Security Concepts and Principles, Security threats and risks, Security services, Organisations, regulations and security standards, cybersecurity specialization.

Cryptographic Algorithms and Protocols: Classical cryptography, Symmetric cryptography, Asymmetric Cryptography, Authentication and Key Exchange Protocols, Advanced Protocols.

Network Security Fundamentals: TCP/IP Security Protocols, Internet Security Mechanisms.

Tools Used: Cryptii, Cryptool, Cyberchef, WinSCP, OpenSSH, Wireshark.

Digital Identity and Privacy

Department: Computer Science, Bachelor's Degree in "Cybersecurity and Artificial Intelligence".

Semester: 2nd

Course Website: Not yet available (Course 2023-2024)

ECTS: 6

Contact: Isaac Agudo (isaac@uma.es)

Course Content

The objectives of this course are to provide students the necessary competences and knowledge to i) distinguish the different mechanisms for authentication and access control used in modern systems, and in particular those applicable to the web, and ii) implement different privacy and anonymity protocols and mechanisms.

For this reason, this course includes the following sections:

- Authentication and access control: Authentication Mechanisms, Access control policies, Access monitoring
- Digital Identity: Public Key Infrastructures, Self-sovereign Identity, Identity Protocols for the web
- Privacy and Anonymity Systems: Privacy-enhancing technologies, Data privacy, Anonymisation mechanisms

Tools Used: OpenLDAP, XCA, OpenSSL, Tor, ARX, Hyperledger Indy, mimikatz.

Information Security

Department: Computer Science, Bachelor's Degree in Computer Science / Bachelor's Double Degree in Computer Science and Mathematics (shared course).

Semester: 5th Bachelor's Degree in Computer Science / 7th Bachelor's Double Degree in Computer Science and Mathematics.

Course Website:

https://sara.uma.es/ht/2022/ProgramasAsignaturas_Titulacion_5102_AsigUMA_51011.pdf - Bachelor's Degree in Computer Science.

https://sara.uma.es/ht/2022/ProgramasAsignaturas_Titulacion_5310_AsigUMA_51011.pdf - Bachelor's Double Degree in Computer Science and Mathematics.

ECTS: 6,0

Contact: Cristina Alcaraz (alcaraz@uma.es)

Course Content

This course focuses on contents related to security and privacy in computer and communications environments. The syllabus is designed to provide students with a broad knowledge of the techniques, mechanisms, protocols and tools that allow the protection of different levels of these environments, from the lowest level (networks) to the highest (applications and services). In particular, this course focuses the following aspects:

- Introduction: Basic security concepts and principles, security services and mechanisms, basic cryptographic techniques.
- Introduction to cryptography: Symmetric and asymmetric algorithms, and other cryptographic primitives such as hash and MAC functions.
- Schemes, protocols and support mechanisms: Key management, access control mechanisms, and advanced cryptographic protocols and mechanisms.
- Security and privacy in telematic applications: security in applications: e-mail and electronic payments, and privacy of users in applications.
- TCP/IP network security: Security at the transport layer, security at the Internet layer, and security in wireless networks.

Tools Used: Pycryptodome (for Python), XCA, Thunderbird for OpenPGP and S/MIME, IPTables, nmap.

Security in Services and Applications

Department: Languages and Computer Science (University of Málaga)

Semester: 2st

Course Website: https://www.uma.es/departments/subjects/titulation/51174/5103/

ECTS: 6

Contact: Antonio Muñoz (anto@uma.es)

Course Content

The subject of Security in Services and Applications focuses on those aspects of security that must be considered during software development and in the secure deployment of applications on the Internet. Regarding the first point, the identification of threats and vulnerabilities is studied, as well as risk management. This information will be used as input to the secure software development process, which begins with the elicitation of security requirements and concludes by ensuring that the implemented software meets those requirements. As for the security of Internet applications, the course addresses it on two fronts: first by covering the high-level security services that are necessary for the successful deployment of these applications, and second by studying the mechanisms that are currently used to provide security to these applications, both at the transport level (SSL/TLS) and in the programming of these applications.

For this reason, this course includes the following sections:

- Basic cryptographic techniques and associated security services. Access control mechanisms).
- Schemes, Protocols and Support Mechanisms (key management, Security Tools (Secure e-mail, Secure remote session, Data encryption and Web application security).
- TLS, Web access control and identity management, Web vulnerabilities and attacks.
- OS security.

Tools Used: Python, Wireshark, OpenSSL, XCA, Wireshark, Cisco Packet Tracer, and Kleopatra.

Information Security and Computer Forensics

Department: Computer Science, Bachelor's Degree in Criminology

Semester: 7th

Course Website: https://www.uma.es/departments/subjects/titulation/52524/5112/

ECTS: 6

Contact: Rodrigo Román (rroman@uma.es), Ana Isabel Cerezo Domiguez

Course Content

This course is aimed at criminology students who need to understand the context of an investigation involving electronic devices. The primary goal is to cultivate a new generation of professionals who can address cybersecurity challenges through the lens of criminology. Consequently, this course combines the fundamental principles of computer security with key aspects of computer forensics, all tailored to suit the needs of a criminologist and foster effective collaboration with other experts.

For this reason, this course includes the following sections:

- Introduction: Cybercrimes, Information security fundamentals, Computer forensics fundamentals.
- Information security: Applied cryptography, Security services, End user security.
- Computer forensics: Forensic investigation, Anti-forensic mechanisms, Operative system forensic analysis.

Tools Used: FTK Imager, Autopsy, John the Ripper, ExifTool, OpenPuff, Veracrypt.

3.1.7 University Of Cyprus (UCY), Cyprus

System Security. *Mandatory undergraduate course (7.5 ECTS)*. Introduction to systems security aiming for covering a wide range of security concepts. Primarily, the course helps students to become familiar with different fields and to render a global view of modern systems security. The course covers several topics, such as applied cryptography, software vulnerabilities and memory errors, attacks and defences, mobile security, web security, network security, privacy, and anonymity.

Software Analysis. *Optional undergraduate course (7.5 ECTS).* The course explores fundamental concepts in analysing software of multiple forms and for different purposes. Many times, we need to analyse software for (a) locating bugs (debugging), (b) measuring performance bottlenecks (profiling), (c) adding instrumentation that enhances a program’s behaviour (e.g., adding a security defence). The course exposes several techniques for working directly with the binary form of software (binary analysis and re-writing), as well as exploring and augmenting the source of C/C++ programs through the extension of modern compiler toolchains (LLVM).

Data Security. *Graduate course (8 ECTS).* Processing data is often realised through systems that can operate under hostile conditions, where adversaries try to monetize access to sensitive data. In this course we provide a short introduction of data security, and we review the basic arsenal we have for protection. We cover a large portion of applied cryptographic primitives and protocols that facilitate secure transmission of data. We then proceed and review how systems that process data can be attacked and protected. Finally, we discuss advanced attacks, and potential defences, for systems that are based on Machine Learning.

3.1.8 University Of Novi Sad (UNSPMF), Serbia

The University of Novi Sad, with almost 50,000 students and 5,000 employees, is one of the largest educational and research centres in Central Europe. It belongs to the group of comprehensive universities, which are characterised by providing nearly all fields of science and higher education. The University of Novi Sad offers around 320 accredited study programs at the level of Bachelor, Master, Specialist and Doctoral studies, carried out at its faculties and within the University Center for Interdisciplinary and Multidisciplinary Studies and Research. The study programs are modern and up-to-date with the latest developments in science and research.

The Faculty of Sciences is one of the members of the University and it offers courses in mathematics, informatics, ecology, biology, geography, physics, chemistry and related disciplines. The Faculty of Sciences consist of 5 departments and the courses that are conducted at the Department of Mathematics and Informatics and may be of interest for cyber security education are given below.

Undergraduate Courses

Development of information systems

Department: Department of Mathematics and Informatics

Semester: 5th

ECTS: 7

Contact: Danijela Boberic Krsticev (dboberic@uns.ac.rs)

Course Content

Course related to development of multi-layer web application using Spring boot framework. Course covers Spring MVC, Spring Data and Spring Security modules, Authentification, Authorisation, JWT

Computer networks

Department: Department of Mathematics and Informatics

Semester: 6th

ECTS: 6

Contact: Danijela Tesendic (tesendic@uns.ac.rs)

Course Content

Undergraduate introductory course about Computer Networks, OSI reference model. Detailed walkthrough over TCP/IP stack, Linux & Windows network management tools

Graduate Courses

Deep Learning

Department: Department of Mathematics and Informatics

Semester: 1st

ECTS: 6

Contact: Nemanja Milosevic (nmilosev@dmi.uns.ac.rs)

Course Content

Introductory Deep Learning course focusing on Deep Neural Networks, Gradient Descent, Backpropagation, Convolutional and Recurrent Models, Autoencoders, Data preprocessing

Distributed Deep Learning

Department: Department of Mathematics and Informatics

Semester: 2nd

ECTS: 5

Contact: Nemanja Milosevic (nmilosev@dmi.uns.ac.rs)

Course Content

Advanced Deep Learning Course focusing on HPC aspects of Deep Learning such as Distributed Training and Optimizations, TinyML, SLURM, Linux and HPC management Tools

Distributed optimization with applications

Department: Department of Mathematics and Informatics

Semester: 2nd

ECTS: 6

Contact: Dusan Jakovetic (dusan.jakovetic@dmi.uns.ac.rs)

Course Content

Algorithm design and convergence analysis for convex distributed optimization and learning, including gradient based and alternating direction-based methods

3.1.9 Universidade Nova De Lisboa (FCT), Portugal

Undergraduate Courses

Networks and Computer Systems Security

Department: Informatics (NOVA FCT)

Semester: 1 and 2

Course Website: https://guia.unl.pt/en/2023/fct/program/1059/course/11619

ECTS: 6

Contact: Henrique João Lopes Domingos (hj@fct.unl.pt)

Course Content:

Networks and Computer Systems Security Fundamentals

Applied Computational Cryptography and Cryptographic Tools

Authentication and Access Control

TCP/IP Stack Security

Systems Security

Software Security

Department: Informatics (NOVA FCT)

Semester: Specialisation Unit

Course Website: https://guia.unl.pt/en/2023/fct/program/1059/course/11619

ECTS: 6

Contact: Luís Manuel Marques da Costa Caires (lcaires@fct.unl.pt)

Course Content:

Software Security Concepts. Security Properties. Threat and Attacker Modelling. How to express security properties and policies. Security Properties as System Invariants.

Principles of Secure Software Design. Basic principles (Least Privilege; Fail-Safe Defaults; Economy of Mechanism; Complete Mediation; Separation of Duties; Least Common Mechanism), and how they map into programming / architectural concepts. Preserving security across modules and trust maintenance: some basic techniques.

Authorization. Authorization and Access control models. Access control policies and rules. General languages and frameworks for expressing and enforcing authorization. Signatures and certificates. Language-Based authorization security: Authorization in runtime support systems, Stack inspection, Proof carrying code, signed code (Java). Permissions and object-capability models (Google Caja).

Information Flow. Security Lattices. Non-interference. Declassification. Covert Channels and indirect flows. (Sand)boxing and Tainting. Reference Monitors. Language-based information flow security: Data Flow analysis. Type-based analysis. Tainting. Paragon - Java, JSFlow - JavaScript.

Domain Specific Security Threats. Two sample scenarios: Web Applications (code injection, cross-site scripting, cross-site request forgery, and session hijacking). Unsafe Languages (exploiting unsafety to violate integrity – buffer overruns, stack smashing). Countermeasures to sample threats using general principles and techniques (information flow, capabilities, tanting, monitors).

Data Security and Provenance. Schema oriented security and row oriented security. Access Control in Data Models. Database inference. Balancing privacy and utility; statistical database security; k-anonymity; differential privacy, privacy languages. Provenance models and languages.

Graduate Courses

Cybersecurity and Governance

Department: MsC in Law and Security (NOVA School of Law)

Semester: 1

Course Website: https://guia.unl.pt/en/2022/fd/program/9279/course/36121

ECTS: 6

Contact: Laura Íñigo Álvarez (laura.inigo@novalaw.unl.pt)

Course Content:

Information, Information Security and Cybersecurity

Hackers, Crackers e other outlaws in Cyberspace

Cyberspace Regulation

Fight against Cybercrime

Incident response and Cybersecurity crisis management

Algorithms and future technologies

Data Protection and Management Law

Department: MsC in Law and Security (NOVA School of Law)

Semester: 1

Course Website: https://guia.unl.pt/pt/2020/fd/program/M364/course/37035

ECTS: 6

Contact: Laura Íñigo Álvarez (laura.inigo@novalaw.unl.pt)

Course Content:

The rights to privacy and data protection: Contextualization of these rights in European law

The GDPR: legal background and practical application

Critical assessment of the GDPR

Cybercrime

Department: MsC in Law and Security (NOVA School of Law)

Semester: 1

Course Website: https://guia.unl.pt/en/2022/fd/program/M364/course/33241

ECTS: 6

Contact: Laura Íñigo Álvarez (laura.inigo@novalaw.unl.pt)

Course Content:

Threats in the online environment

Cybercrime typologies

Cyber-criminology: Why cybercrime occurs; why people are victimized by criminals in the cyberspace

Financial crime in online settings (e.g., cyber extortion; online fraud; money laundering by means of cryptocurrency)

Cyber-terrorism (with an emphasis of terrorist financing)

Attacks against information systems

The transition from electronic to AI-generated evidence

Automation in law enforcement settings

Algorithmic criminal justice

Cyber-security: technical solutions

Cyber-security: EU policies and plans

Seminars/Summer Schools

Cybersecurity

Department: Post-Grad in Information Management and Security (NOVA Information Management Schools)

Semester: 2

Course Website: https://guia.unl.pt/en/2022/novaims/program/4964/course/400149

ECTS: 7.5

Contact: João Barbas (jbarbas@novaims.unl.pt)

Course Content:

Information Security in the context of organizations.

Legal and normative framework for Information Security and Cybersecurity.

Cyberspace Actors and Threats

Risk Assessment and Management

Information Security Technologies

Information Security Policies

Information Security Organization

Management and Governance

Compliance and Reporting

Globalisation and Security Risks

Department: Post-Grad in Information Management and Security (NOVA Information Management Schools)

Semester: 2

Course Website: https://guia.unl.pt/en/2022/novaims/program/4964/course/400031

ECTS: 7.5

Contact: Teresa Rodrigues (trodrigues@novaims.unl.pt)

Course Content:

Develop capacities to understand, analyze and investigate themes and problems arising from the globalization process(s), inserted in a logic of security and securitization;

Based on case studies, acquire in-depth theoretical knowledge about the concept of Security, with emphasis on the terms of human security and cooperative security;

Gain knowledge about the response tools to be used in an increasingly global world, characteristic of the emergence of new risks, threats and inter- and infra-state conflicts (diplomacy, development, cooperation, democracy....);

Develop capacities to perceive and analyze Portugal's position, from a perspective of alliances and international cooperation;

Gather information on the current and future reality, enabling participation in strategic analysis processes and support for decision-making, in particular in the sphere of public policies;

Intelligence Services and Political Regimes

Department: Post-Grad in Information Management and Security (NOVA Information Management Schools)

Semester: 2

Course Website: https://guia.unl.pt/en/2022/novaims/program/4964/course/400030

ECTS: 7.5

Contact: Vasco Rato (vrato@novaims.unl.pt)

Course Content:

Concepts of Democratization in the world and in Portugal.

Contributions of the Information Services to the establishment of Democracy.

Social Network Intelligence

Department: Post-Grad in Information Management and Security (NOVA Information Management Schools)

Semester: 1

Course Website: https://guia.unl.pt/en/2022/novaims/program/4964/course/400036

ECTS: 7.5

Contact: Guilherme Vitorino (gmvictorino@novaims.unl.pt)

Course Content:

The course aims to introduce students to the importance of managing data, information, and knowledge effectively in a contemporary knowledge-based society, where social networks, geographic information, and technology play fundamental roles in the successful evolution of intelligence and information management.

Regional Dynamics of Security and Defense

Department: Post-Grad in Information Management and Security (NOVA Information Management Schools)

Semester: 1

Course Website: https://guia.unl.pt/en/2022/novaims/program/4964/course/400035

ECTS: 7.5

Contact: Luis Cunha (lcunha@novaims.unl.pt)

Course Content:

Develop an in-depth knowledge of the security and defense dynamics in different regions of the World.

Obtain analytical and critical skills on these regional dynamics.

Obtain qualified tools to study security and defense and its specific dynamics at a regional level.

Economic and Competitive Intelligence

Department: Post-Grad in Information Management and Security (NOVA Information Management Schools)

Semester: 1

Course Website: https://guia.unl.pt/en/2022/novaims/program/4964/course/400033

ECTS: 7.5

Contact: Luis Madureira (lmadureira@novaims.unl.pt)

Course Content:

The aim of this course is to understand what is Competitive Intelligence, its relation to Strategy and Marketing, and its use for greater overall efficiency. Students should be able to integrate tools, techniques, and methodologies to understand the key behavior of a given competitor in the market. This integration will provide a deduction of the performance of a given competitor based on the Competitive Landscape, or in the opposite direction, as their Marketing Communications can be used to infer the competitor's strategy. It will be shared with students a global perspective of the What, When, How, and Why of using these tools, per se, or in an integrated fashion. The ultimate goal is to create conditions for students positive impact in strategic decision making in organizations to which they belong or will belong.

Methodology and Techniques for Analysis and Prospection

Department: Post-Grad in Information Management and Security (NOVA Information Management Schools)

Semester: 1

Course Website: https://guia.unl.pt/en/2022/novaims/program/4964/course/400037

ECTS: 7.5

Contact: João Ribeiro (jribeiro@novaims.unl.pt)

Course Content:

Familiarize participants with basic concepts, tools and uses of Foresight and present examples of Foresight exercises carried out on international relations topics.

Introduce participants to scenario building methodologies, a relevant tool in foresight.

Contribute to the understanding of the dynamics of the international system by intervening at the geoeconomic, geopolitical and planned levels in the evaluation of possible alternative scenarios of Evolution.

Structured Analytical Techniques for Information Analysis

Department: Post-Grad in Information Management and Security (NOVA Information Management Schools)

Semester: 2

Course Website: https://guia.unl.pt/en/2022/novaims/program/4964/course/400032

ECTS: 7.5

Contact: Paula Esperança (pesperanca@novaims.unl.pt)

Course Content:

The objective of this course is to provide the student with the specificity of the intelligence analysis and the different structured analytic techniques regarding the intelligence matters, being able to choose the appropriate technique in each concrete situation.

Digital Transformation in a Cybersecurity context

Department: Executives Seminar: Cybersecurity and Data Privacy in Information Management (NOVA Information Management Schools)

Course Website: https://nova-ims.stage.fever.pt/en/education/programs/executive-education/cybersecurity-and-data-privacy-in-information-management/

Contact: Jorge Carrola Rodrigues (jcarrola@novaims.unl.pt)

Course Content:

Cybersecurity is one of the areas of technological leadership in the implementation of digital transformation of organizations. It is, therefore, essential to understand which are the various factors and technologies that facilitate this transformation and how organizations are (or can be) prepared for it. In this introduction module to the executive program, transformation and risk management methodologies will also be addressed.

Cybersecurity, IT Asset Management, and Governance

Department: Executives Seminar: Cybersecurity and Data Privacy in Information Management (NOVA Information Management Schools)

Course Website: https://nova-ims.stage.fever.pt/en/education/programs/executive-education/cybersecurity-and-data-privacy-in-information-management/

Contact: Jorge Carrola Rodrigues (jcarrola@novaims.unl.pt)

Course Content:

This module focuses on the definition of management policies, mapping, and governance of IT assets in order to identify potential risks and establish mitigation and prevention policies for information management and data protection. In a context where more and more devices are connected to the internet (IoT), the respective vulnerabilities and how to minimize the risks will also be addressed.

GDPR: Governance, Implementation, Maintenance and Control: Governance, Implementation, Maintenance and Control

Department: Executives Seminar: Cybersecurity and Data Privacy in Information Management (NOVA Information Management Schools)

Course Website: https://nova-ims.stage.fever.pt/en/education/programs/executive-education/cybersecurity-and-data-privacy-in-information-management/

Contact: Jorge Carrola Rodrigues (jcarrola@novaims.unl.pt)

Course Content:

This module will cover governance and privacy policies for compliance with GDPR.

Among other things, methods for monitoring and auditing compliance will be identified, and procedures and mechanisms for responding to requests to exercise the rights of data subjects and for incident management response will be addressed.

The Legal Framework of the Digital Ecosystem - Telecommunications, Media and Information Technology (TMT)

Department: Executives Seminar: Cybersecurity and Data Privacy in Information Management (NOVA Information Management Schools)

Course Website: https://nova-ims.stage.fever.pt/en/education/programs/executive-education/cybersecurity-and-data-privacy-in-information-management/

Contact: Jorge Carrola Rodrigues (jcarrola@novaims.unl.pt)

Course Content:

A module defining the constitutional and criminal limits and criminal liability in a digital context, as well as the definition of computer crime and cybercrime. The general data protection regulation, the supervisory authority - CNPD, the system of sanctions, and the regulation of legal protection of software will also be addressed. All are illustrated with numerous practical examples.

How to implement an Information Security Management System with ISO/IEC 27001

Department: Executives Seminar: Cybersecurity and Data Privacy in Information Management (NOVA Information Management Schools)

Course Website: https://nova-ims.stage.fever.pt/en/education/programs/executive-education/cybersecurity-and-data-privacy-in-information-management/

Contact: Jorge Carrola Rodrigues (jcarrola@novaims.unl.pt)

Course Content:

How to define a security policy to support the implementation of an ISMS according to the ISO standard. How to define an information system security architecture, assess, control, and manage risks and their control mechanisms.

Cybercrime - Prevention and Forensic Techniques

Department: Executives Seminar: Cybersecurity and Data Privacy in Information Management (NOVA Information Management Schools)

Course Website: https://nova-ims.stage.fever.pt/en/education/programs/executive-education/cybersecurity-and-data-privacy-in-information-management/

Contact: Jorge Carrola Rodrigues (jcarrola@novaims.unl.pt)

Course Content:

A module where some of the best practices in safeguarding digital information for evidence purposes are addressed, with practical examples, along with the interconnection with crisis management and Criminal Law.

Competitive and Counter Intelligence

Department: Executives Seminar: Cybersecurity and Data Privacy in Information Management (NOVA Information Management Schools)

Course Website: https://nova-ims.stage.fever.pt/en/education/programs/executive-education/cybersecurity-and-data-privacy-in-information-management/

Contact: Jorge Carrola Rodrigues (jcarrola@novaims.unl.pt)

Course Content:

"Data is the new Oil" is the new mantra of business. However, too much Data and Information, as well as Fake News and misinformation, make navigating the Competitive Environment an absolute nightmare. This module shares how actionable insights (Competitive Intelligence) enable organizations to find their way to success and protect themselves from competitors' onslaughts, for example, through Social Engineering, to gain access to organizations' main assets, their knowledge.

3.1.10 University Of Piraeus Research Center (UPRC), Greece

Undergraduate Courses

Web Technologies

Department: Informatics (University of Piraeus)

Semester: 1st

Course Website: https://gunet2.cs.unipi.gr/courses/TMA110/

ECTS: 5

Contact: Douligeris Christos (cdoulig@unipi.gr)

Course Content

This course describes in an introductory, but complete, way the technologies and protocols on which the Internet and the World Wide Web are based and analyses in more detail the development of applications using specific tools/languages, which are performed on the client side and/or on the server side

Some of the concepts that are addressed are: TCP/IP protocol stack, transport and internet level, HTML5, CSS3, Javascript, jQuery, AJAX call, PHP nodejs, XML and JSON

Cryptography

Department: Informatics (University of Piraeus)

Semester:5th

Course Website: https://gunet2.cs.unipi.gr/courses/TMC106/

ECTS: 5

Contact: Patsakis Constantinos (kpatsak@unipi.gr)

Course Content

- Basic Algorithms (Monoalphabetic substitution, One-Time-Pad, Ceasar Vigener, Hill)
- Symmetric Algorithms (Cipher Modes: ECB, CBC, OFB etc.) DES, AES
- Stream Ciphers: PRNG vs TRNG, LFSR, RC4
- Public key Algorithms (RSA Algorithm, Elliptic Curves)
- Homomorphic Encryption
- Hash Functions
- Digital Signatures
- Cryptographic Applications and Protocols
- Cryptanalysis (Linear, Differential, Integer Factorisation)
- Development Problems

Security Governance

Department: Informatics

Semester: 6th

Course Website: https://gunet2.cs.unipi.gr/courses/TMD116/

ECTS: 5

Contact: Polemi Despoina (dpolemi@unipi.gr)

Course Content

The main objective of this course is to assess the security that is offered by an information system as well as the quality of the security that is offered from the application of processes of an organisation.

- Common vulnerabilities of systems and applications
- Methods and tools to discover vulnerabilities of apps and systems
- Exploitation & persistence
- Digital forensics
- Information risk analysis
- Security plans, policies and processes
- Regulatory framework and security standards
- Continuity and recovery plans

Information Systems Security

Department: Informatics

Semester: 7th

Course Website: https://gunet2.cs.unipi.gr/courses/TMD108/

ECTS: 5

Contact: Kotzanikolaou Panagiotis (pkotzani@unipi.gr)

Course Content

The security of information, systems and applications is a basic requirement in the development and operation of information systems. The course covers basic issues of information systems security and includes the following sections:

- Introduction to information system security concepts
- Security Management Systems
- Cryptographic systems
- Public Key Infrastructure
- Access control and Privacy
- Security in Technologies
- Secure electronic and mobile services
- Introduction to network security

Tools Used: CrypTool, John the Ripper (password security), nmap, OpenVas, OWASP ZAP

Network Security

Department: Informatics

Semester: 8th

Course Website: https://gunet2.cs.unipi.gr/courses/TMA102/

ECTS: 5

Contact: Kotzanikolaou Panagiotis (pkotzani@unipi.gr)

Course Content

The aim of the course is the theoretical and practical study of security issues at all levels of networks.

The following sections will be analyzed in the course:

- Introduction to network security
- Routing Security
- Design of Firewall systems
- Virtual Private Networks (VPNs)
- Network layer security (IPSec)
- Session Layer Security (SSL / TLS)

Tools Used: Wireshark, iptables, snort, nmap, OWASP ZAP

Security Policies and Security Management

Department: Digital Systems

Semester: 5th

Course Website: https://aristarchus.ds.unipi.gr/courses/DS-COURSES-SEM124/ (username and password required)

ECTS: 5

Contact: Gritzalis Stefanos (sgritz@unipi.gr)

Course Content

Introductory issues: The issue of information security, the need to protect information, information protection framework, standards and standardization, basic concepts of information security.

Information security management systems: Information security as a management problem, basic concepts and necessity of information security management systems, ISO 27k series of standards, ISO / IEC 27001: 2013.

Risk analysis, assessment and management: The concept of risk, risk management as a methodology, ISO / IEC 27005: 2011.

Organizational framework for information security: Security policies, policy hierarchy, feasibility of existence, information security policy, thematic policies, other elements of the organizational framework, desirable policy characteristics, policy cycle, policy development competence.

Management of security incidents: Basic concepts – Incident life cycle – Concerns, purpose and objectives of the incident handling process, case types, incident handling group, case management process phases.

Business Continuity and Disaster Recovery: Basic concepts, necessity of business continuity planning, types of projects and relationships between them, the disaster recovery planning process, investment level.

Security Assurance: Basic concepts, types of security metrics, the security measurement process.

Tools Used: Nmap - Zenmap GUI, Wireshark

Maritime ICT Systems

Department: Informatics

Semester: 7th

ECTS: 5

Contact: Polemi Despoina (dpolemi@unipi.gr)

Course Content

- Database Systems, Maritime Information Systems
- Maritime monitoring systems
- Threats in the maritime operation
- Attacks in the maritime technologies
- Standards and Regulatory Frameworks for the security of maritime operations
- Risk management of Ports ICT

Network Security

Department: Digital Systems

Semester: 5th

Course Website: https://aristarchus.ds.unipi.gr/courses/DS-COURSES-SEM135/ (username and password required)

ECTS: 5

Contact: Xenakis Christos (xenakis@unipi.gr)

Course Content

- Security at lower layers.
- Network layer security solutions.
- Application layer security solutions.
- Key management protocols; identity management protocols.
- Firewalls.
- Trust management.
- Distributed authentication systems and intrusion detection systems.

Tools Used: Nmap, Cisco packet tracer (use of Python, use of Blockly), Wireshark

Information Systems Security

Department: Digital Systems

Semester: 6th

Course Website: https://aristarchus.ds.unipi.gr/courses/DS-COURSES-SEM139/ (username and password required)

ECTS: 5

Contact: Gritzalis Stefanos (sgritz@unipi.gr)

Course Content

- Identification and Authentication: Authentication Categories, Authentication Data, Authentication Systems, Biometric Systems.
- Identity management: examples, technologies, data protection.
- Access control: Access operations, access matrix, access control mechanisms.
- Security of Operating Systems: Operating System Security Parameters, Operating Systems Security Mechanisms, development of secure OS, case studies (Unix, Windows NT).

- Database Systems Security: Security requirements, data integrity and system availability, security for sensitive data, multi-level databases, Oracle security.
- Malware: Classification, types, methods, case studies.
- System and product security and assurance: Purpose, issues and methods of assurance, assurance criteria, evaluation systems.

Tools Used: Cain & Abel passwork recovery/cracking tool, VMWare Workstation Player, Kali Linux, Nessus, Metasploit Framework, Damn Vulnerable Web Application

Internet Protocols

Department: Digital Systems

Semester: 6th

Course Website: https://aristarchus.ds.unipi.gr/courses/DS-COURSES-SEM137/ (username and password required)

ECTS: 5

Contact: Rouskas Angelos (arouskas@unipi.gr)

Course Content

- Introduction to Internet main concepts.
- OSI and TCP/IP models.
- Application layer protocols Dynamic Host Configuration Protocol (DHCP). HyperText Transfer Protocol (HTTP). File Transfer Protocol (FTP). Simple Mail Transfer Protocol (SMTP), POP, IMAP. Domain Name Service (DNS). Peer-2-Peer protocols.
- Client-Server Architecture and programming. Sockets and Socket Programming.
- Transport layer protocols. Transmission Control Protocol (TCP). User Datagram Protocol (UDP).
- Internet layer protocols. IP Addressing. Internet Protocol (IPv4, IPv6). Internet Group Management Protocol (IGMP). Internet Control Message Protocol (ICMP). Routing Protocols, Autonomous Systems, Interior and Exterior protocols (RIP, OSPF, eBGP, iBGP)
- Link layer protocols. Address Resolution Protocol (ARP). Reverse Address Resolution Protocol (RARP).
- Multimedia networking. Multimedia applications, VoIP and Video over IP.

Tools Used: Wireshark, packet sniffer, protocol analyzer

Privacy Enhancing Technologies

Department: Digital Systems

Semester: 6th

Course Website: https://aristarchus.ds.unipi.gr/courses/DS-COURSES-SEM150/ (username and password required)

ECTS: 5

Contact: Lambrinoudakis Konstantinos (clam@unipi.gr)

Course Content

- Definition of Privacy.
- Legal Framework for the Protection of Personal Data.

- Attacks on Privacy and Subjectivity of Impact in case of Privacy violation incidents.
- Requirements for anonymity, unlinkability, undetectability and unobservability.
- Pseudo-anonymity.
- Identity Management.
- Privacy Enhancing Technologies (Anonymizer, LPWA, Onion Routing, Crowds, MixNets, etc.).
- Privacy protection in Ubiquitous Computing (RFIDs, Positioning Services), Internet Telephony, Health Information Systems, etc.
- The Greek Framework for Digital Authentication and the Unique Citizen Identification Number for Electronic Services Offered by Government Bodies.
- Privacy Economics

Cryptography

Department: Digital Systems

Semester: 7th

Course Website: https://aristarchus.ds.unipi.gr/courses/DS-COURSES-SEM172/ (username and password required)

ECTS: 5

Contact: Xenakis Christos (xenakis@unipi.gr)

Course Content

- Basic definitions and concepts; information security
- Symmetric cryptography
- Digital signatures
- Authentication
- Public key cryptography
- Hash functions
- Integrity checking
- Key management and random number generators

Mobile and Wireless Communications Security

Department: Digital Systems

Semester: 8th

Course Website: https://aristarchus.ds.unipi.gr/courses/DS-COURSES-SEM192/ (username and password required)

ECTS: 5

Contact: Xenakis Christos (xenakis@unipi.gr)

Course Content

- Wireless security
- WLAN, IEEE 802.11
- Authentication check on IEEE 802.11
- RADIUS & EAP methods
- IEEE 802.1x
- WEP
- IEEE 802.11i, WPA, WPA2 (TKIP, CCMP)

Tools Used: Wireshark, Kali Linux

Privacy on the Internet

Department: Digital Systems

Semester: 8th

Course Website: https://aristarchus.ds.unipi.gr/courses/DS-COURSES-SEM193/ (username and password required)

ECTS: 5

Contact: Gritzalis Stefanos (sgritz@unipi.gr)

Course Content

- Privacy protection: Technical, legal, regulation, and ethical issues
- Privacy framework according to ISO/IEC 29100:2011 and ISO/IEC 29101:2018
- Privacy by Design critical issues
- Privacy Impact Assessment according to ISO/IEC 29134:2017
- Privacy protection countermeasures according to ISO/IEC 27701:2019
- Cloud computing and related Privacy protection issues according to ISO 27018:2014
- GDPR and ISO 27001 synergies of activities towards organization's compliance
- Case study: Privacy in social media

Information Systems

Department: Industrial Management & Technology

Semester: 5th

Course Website:

ECTS: 5.5

Contact: Chondrokoukis Gregory (gregory@unipi.gr)

Course Content

- Introduction to information systems
- Information systems and strategy
- Information and telecommunication technologies
- Data bases and file management systems
- Business information systems
- eCommerce and Internet
- Decision Support Systems
- Collaboration technologies
- ELearning
- Information security and privacy

E-Business and Innovation

Department: Informatics

Semester: 8th

Course Website: https://gunet2.cs.unipi.gr/courses/TMD128/ (username and password required)

ECTS: 5

Contact: Polemi Despoina (dpolemi@unipi.gr)

Course Content

- Introduction to e-Business and e-Commerce.
- e-Commerce fundamentals.
- Trustworthy e-Business Infrastructure.
- Analysis and understanding of the e-Environment.
- e-Business Strategy.
- Supply Chain Management.
- Digital Marketing.
- Customer Relationship Management.
- Change Management.
- Analysis and trustworthy Design.
- Implementation and optimization of secure e-Business services.

Operational Research

Department: Business Administration

Semester: 4th

Course Website: https://eclass.unipi.gr/courses/ODE175/ (username and password required)

ECTS: 6

Contact: Kopanaki Evangelia (evik@unipi.gr)

Course Content

- Management decision-making process
- Linear programming (modelling – simplex method – problem solving using computers – applications)
- Sensitivity analysis – duality theory
- Transportation and assignment problems
- Network analysis
- Dynamic programming
- Case studies

Management Information Systems

Department: Business Administration

Semester: 7th

Course Website: https://eclass.unipi.gr/courses/ODE196/ (username and password required)

ECTS: 7

Contact: Kopanaki Evangelia (evik@unipi.gr)

Course Content

The course is designed to help students understand and analyse Information Systems (IS) from a business viewpoint. Understanding IS from this viewpoint is important because business professionals inevitably encounter IS in today's business world. Today's IS leaders have become more visible and strategically important, as both technological and business forces have continued to increase information technology (IT) management responsibilities and roles within their organizations. There is a growing need for those interested in business to understand the nature of IT and the way it can best be harnessed to provide information for business functions.

E-Commerce

Department: Business Administration

Semester: Elective on 5th or 7th

Course Website: https://eclass.unipi.gr/courses/ODE197/ (username and password required)

ECTS: 3

Contact: Kopanaki Evangelia (evik@unipi.gr)

Course Content

- Introduction to e-business
- Categories of e-commerce
- Difference between e-commerce and e-business
- Stages of e-business adoption
- Business-to-consumer (B2C) e-commerce business models
- Strategic e-business planning
- ERP and CRM information systems
- Business-to-business information systems
- Traditional and modern information systems
- Technological, business and business-to-business issues
- Supply chain information systems

Undergraduate Courses of Hellenic Air Force Academy in collaboration with UPRC and department of Informatics

Network Security

Department: Aeronautical Sciences, Division of Computer Engineering and Information Science

Semester: 8th

ECTS: 2

Contact: Antonios Andreatos (antonios.andreatos@hafa.haf.gr)

Course Content

- Principles of Cryptography
- Message Integrity
- Digital Signatures
- Hash Function
- Digital Signatures
- Key Management
- End-Point Authentication
- Secure E-Mail
- SSL

- Securing Wireless LANs
- Operational Security
- Firewalls and Intrusion Detection Systems
- Malware

Computer Networks & Network Security (Introduction)

Department: Aeronautical Sciences, Division of Computer Engineering and Information Science

Semester: 6th

ECTS: 2

Contact: Antonios Andreatos (antonios.andreatos@hafa.haf.gr)

Course Content

- Application layer, Principles of network applications, Web and HTTP, SSH, Electronic Mail (SMTP, POP3, IMAP, MIME),DNS
- Transport Layer, Transport-layer services, Connectionless transport: UDP, Connection-oriented transport: TCP (segment structure, reliable data transfer, flow control, connection management), TCP congestion control
- Network Layer, IP: Internet Protocol (Datagram format, IPv4 addressing, ICMP, IPv6), Routing algorithms (Link state, Distance Vector, Hierarchical routing, AS), Routing in the Internet (RIP, OSPF, BGP), Broadcast and multicast routing
- Data Link Layer, Error detection and correction, Multiple access protocols, Link-layer Addressing, Ethernet, WiFi
- Network Security.

Tools Used: Wireshark, Nmap, Virtual Box, VMWare, Metaspoit, openssl.

Graduate Courses

Information Security of Public Services and Systems and Blockchain Technologies

Department: Informatics, MSc in Digital Culture, Smart Cities, IoT and Advanced Technologies

Semester: 2nd

ECTS: 6

Contact: Patsakis Constantinos (kpatsak@unipi.gr)

Course Content

- Frequent application security vulnerabilities
- Discover security vulnerabilities in Web applications
- Secure password storage
- Fragmentation & encryption functions
- Basic building blocks of Blockchains
- Proof of Work, Proof of Stake
- Applications of blockchains in various fields
- Tokenization
- Writing Smart Contra
- Distributed Storage & Blockchains
- IPFS.

Cryptography

Department: Informatics, MSc in Informatics

Semester: 3rd

ECTS: 5

Contact: Patsakis Constantinos (kpatsak@unipi.gr)

Course Content

- Private Key Algorithms
- Public Key Algorithms
- Hash functions
- Digital signatures
- Applications of cryptography (IPSec, SSL, SSH, electronic voting)
- Cryptanalysis

Information Security

Department: Informatics, MSc in Informatics

Semester: 4th

ECTS: 5

Contact: Patsakis Constantinos (kpatsak@unipi.gr)

Course Content

The course covers the main aspects of information security, covering both the theoretical and practical study of methodologies and tools. The main areas of study are:

- Introduction to information system security methodologies
- Cryptographic tools and techniques
- Access Control
- Security technologies for the web

Tools Used: cryptool, openssl, openldap

Maritime Informatics

Department: Informatics, MSc in Informatics

Semester: 4th

ECTS: 5

Contact: Polemi Despoina (dpolemi@unipi.gr)

Course Content

- Protection of Port s' Critical Information Infrastructures
- Trustworthy e-port services and e-maritime services
- Surveillance and monitoring maritime technologies
- Autonomous Vessels and AI attacks
- Routing Algorithms

Network and Communications Security

Department: Informatics, MSc in Cybersecurity and Data Science

Semester: 1st

ECTS: 6

Contact: Kotzanikolaou Panagiotis (pkotzani@unipi.gr)

Course Content

Network and communication security includes security methods, techniques and tools utilized in the design, implementation and audit of a network security policy. The theoretical part of the course includes the analysis of security vulnerabilities in communication protocols for all the layers of the TCP/IP network stack and the definition of a network security policy. The practical part of the course includes the implementation of network security controls such as firewalls, intrusion detection/prevention (IDS/IPS) systems and virtual private networks. The main topics covered include:

- Introduction to Network Security
- Data-link layer security (Ethernet, ARP, WiFi)
- Network layer security (IP, IPSec)
- Transport layer security (SSL/TLS)
- Designing Network Security Policies
- Cross-layer network security mechanisms (firewalls, Intrusion Detection Systems)
- Application-layer firewalls and IDS

Tools Used: iptables, snort, ossec, wireshark, nmap, openssl

Information Security Governance

Department: Informatics, MSc in Cybersecurity and Data Science

Semester: 1st

ECTS: 6

Contact: Polemi Despoina (dpolemi@unipi.gr)

Course Content

- Basic concepts and terminology
- Risk Assessment Standards
- Methodologies and Risk Management Tools
- Security Policies and Procedures
- Security Auditing and Certification
- Implementing Legal and Policy Requirements
- Business Continuity
- Incident Handling
- Supply Chain Security
- Tools for Supply Chain Risk Assessment

Scope of the course: The aims of the course are to become familiar with the:

- security management standards and tools
- risk assessment methodologies and tools
- standards and procedures for business continuity and disaster recovery
- audit and security certification

Tools Used: CRAMM, eBIOS, MITIGATE

Applied Cryptography

Department: Informatics, MSc in Cybersecurity and Data Science

Semester: 1st

ECTS: 3

Contact: Patsakis Constantinos (kpatsak@unipi.gr)

Course Content

- Symmetric and asymmetric encryption
- Hash functions
- Digital signatures
- Key generation and exchange
- Homomorphic encryption
- Cryptographic protocols
- Secure computations

Penetration Testing

Department: Informatics, MSc in Cybersecurity and Data Science

Semester: 2nd

ECTS: 6

Contact: Kotzanikolaou Panagiotis (pkotzani@unipi.gr)

Course Content

- Introduction to Penetration Test Methodology
- Reconnaissance Techniques
- Scanning Techniques
- Gaining Initial Access Techniques (Exploitation, Brute forcing, Client side attack)
- Maintain access (Trojans, rootkits, back doors)
- AV, EDR bypass Techniques
- Post exploitation Techniques
- Lateral Movement
- Network pivoting
- Covering tracks

Tools Used: Kali Linux, Hack-the-Box platform, OWASP ZAP, John the ripper, metasploit

Digital Forensics

Department: Informatics, MSc in Cybersecurity and Data Science

Semester: 2nd

ECTS: 3

Contact: Patsakis Constantinos (kpatsak@unipi.gr)

Course Content

The Digital Forensics course focuses on building incident handling and digital forensics capabilities covering Windows and Linux operating systems. The course covers all the essential information you need to properly detect, response, mitigate and recover from cyber security incidents. It is a full technical course with hands on labs. The aim of this course is, after understanding the attacking process, to learn how to deal with cyber attacks on windows and linux operating systems. You will learn the

Incident Response / handling Process and also the digital forensics process. We will focus on windows, linux and network digital forensics. More specifically this course covers the following topics:

- Incident Handling process
- Windows forensics (memory forensics, registry forensics, fle system analysis, application forensics)
- Log file analysis
- Linux forensics
- Network forensics

Tools Used: SIFT forensics workstation, volatility, autopsy

Malware Analysis

Department: Informatics, MSc in Cybersecurity and Data Science

Semester: 2nd

ECTS: 3

Contact: Patsakis Constantinos (kpatsak@unipi.gr)

Course Content

- Malware
- C&C servers (protocols and methods)
- Obfuscation
- Static Malware analysis
- Dynamic Malware analysis
- Machine learning for malware detection

Tools Used: gdb, ollyDbg, IDA pro

Software Security

Department: Informatics, MSc in Cybersecurity and Data Science

Semester: 2nd

ECTS: 6

Contact: Kotzanikolaou Panagiotis (pkotzani@unipi.gr)

Course Content

The primary goal of this course is the development of the following skills: the application of security best practices to software under development, the identification of security issues in open-source and closed source software, the demonstration of a vulnerability, the rating of a vulnerability and the management of vulnerabilities throughout the design, implementation and maintenance phases of software projects. Students will also be introduced to state-of-the-art methods for the identification of vulnerabilities and recent techniques for the proactive mitigation of risks.

Tools Used: gdb, Cuckoo sandbox, angr framewwork

Advance Cryptographic and Security Technologies (Blockchain Technologies)

Department: Informatics, MSc in Cybersecurity and Data Science

Semester: 2nd

ECTS: 3

Contact: Patsakis Constantinos (kpatsak@unipi.gr)

Course Content

This course focuses on introducing the students to the blockchain technology. After introducing the core concepts behind blockchain, we present the various consensus algorithms and the functionality that is provided. After exploring traceability in public blockchains, we shift to smart contract development to develop practical applications in real-world blockchains. More specifically this course covers the following topics:

- Introduction to blockchain
- Concensus algorithms (Proof of work, Proof of stake, Byzantine fault tolerance)
- Traceability in blockchain (tracing transactions in the blockchain)
- Smart contract development in Ethereum/Hyperledger (will depend on the year)

Network Security

Department: Digital Systems, MSc in Digital Systems Security

Semester: 1st

ECTS: 7.5

Contact: Xenakis Christos (xenakis@unipi.gr)

Course Content

- Introduction to network security considering the security requirements as well as the attacks that aim at preventing the provided services. Description of the basic security services and mechanisms.
- Fundamental network security tools. Confidentiality and conventional cryptography.
- Asymmetric cryptography and the required public key infrastructure. Providing trust in networks and services.
- Authentication services. Trust and reputation management for organizations and services.
- Security mechanisms at the application level. Analysis of the Pretty Good Privacy.
- Security mechanisms at the network level. Analysis of the IPsec.
- Security mechanisms on the web. Analysis of the protocols SSL, SSH, SET, etc.
- Protection against network attacks. Analysis, implementation and evaluation of security firewalls.
- Presentation and analysis of malware (malicious software) that is found on the Internet.
- Intrusion attacks and intrusion detection systems.
- Denial of service attacks and countermeasures.
- Attacks on Domain Name System (DNS) and Address Resolution Protocol (ARP)

Tools Used: NodeJS, Docker, Damn Vulnerable Web Application, Burpsuite, Wireshark

Applied Cryptography

Department: Digital Systems, MSc in Digital Systems Security

Semester: 1st

ECTS: 7.5

Contact: Sgouros Nikitas (sgouros@unipi.gr)

Course Content

- History and overview of cryptography
- Mathematical background
- Cryptographic foundations (Pseudorandom number generators, Pseudorandom functions and permutations, One-way functions)
- Data confidentiality protection protocols and primitives (stream ciphers, block ciphers, El Gamal, RSA, elliptic curves)
- Data integrity protection protocols (hash functions, HMAC, CBC-MAC, digital signatures, DSS)
- Key distribution and key agreement protocols (Diffie-Helman, secret key sharing, PKI, Kerberos)
- Key size selection and key generation
- Advanced topics (E-voting, E-payments, Outsourcing data and computation, Multiparty Computation)

Mobile Internet Security

Department: Digital Systems, MSc in Digital Systems Security

Semester: 2nd

ECTS: 7.5

Contact: Xenakis Christos (xenakis@unipi.gr)

Course Content

- Introduction to mobile/wireless security, mobile Internet security, security requirements and challenges.
- Wireless local area networks (WLANs) security, substantial weaknesses and possible attacks.
- The security standard IEEE 802.11i; basic mechanisms and security services.
- Security in wireless infrastructureless networks (ad hoc networks, Internet of things).
- GSM and GPRS security.
- UMTS security.
- Wireless metropolitan area networks (WiMAX) security.
- Security in wireless community network.
- Security in Long Term Evolution (LTE).
- Android and iOS operating systems security.

Cross-Institutional Graduate Courses of Department of Informatics with the University of Western Macedonia at Kastoria

Distributed Systems and Cloud Computing

Semester: 1st

ECTS: 5

Contact: Christos Douligeris (cdoulig@unipi.gr)

Course Content

- Study of the design and implementation of modern distributed systems and cloud computing.

- Concepts related to the hardware and software on which a computer system is built will be studied.
- Communication between the various parts of the system as well as process management, entity naming, and security.

In addition, the architecture of cloud computing and the emerging models that expand its capabilities will be studied (Network Function Virtualization – NFV, Software Defined Networking – SDN, Edge Cloud and Fog/Edge Computing), as well as corresponding composition models, heterogeneity, scaling, the visualization techniques of dynamic workflows, quality assurance in cloud computing, categories of parameters and requirements, but also fault tolerance techniques.

Tools Used: AWS Security components

Security of Information and Network Systems – GDPR

Semester: 1st

ECTS: 5

Contact: Christos Douligeris (cdoulig@unipi.gr)

Course Content

- Identification and authentication
- Identity management technologies
- Access control
- Operating system security
- Database system security
- Malware
- System and product security assurance and assessment
- GDPR

Tools Used: OpenSSL, Snort, CrypTool-Online, AES encryption,
RSA Encryptor/Decryptor/Key Generator/Cracker.

Open University of Cyprus and Hellenic Air Force Academy Graduate Courses

Cybersecurity

Department: Aeronautical Sciences, Division of Computer Engineering and Information Science

Contact: Antonios Andreatos (antonios.andreatos@hafa.haf.gr)

Course Content

- Introduction to Cybersecurity
- Network security essentials
- Cryptography
- User Authentication
- Database & Cloud Security
- Malicious Software (Malware
- Denial-of-Service Attacks
- Intrusion Detection
- Prevention and Firewalls
- Buffer Overflow Attacks and Software Security
- Operating System Security and IT Security Management

- IT Security Controls
- Plans and Procedures
- Internet Security Protocols and Standards
- Wireless Network Security

Tools Used: Wireshark, Nmap, Metaspoit, openssl, mimikatz, Bash shell

Seminars – Summer Schools

CCNA Security V1.0 (Summer Course, *Department of Digital Systems, MSc in Digital Systems Security)*

Contact: Xenakis Christos (xenakis@unipi.gr)

Course Content

- Introduction to CISCO security technologies and solutions.
- Modern Network Security Threats
- Securing Network Devices
- Authentication, Authorization and Accounting
- Access Control Lists
- Intrusion Prevention Systems
- Securing the LAN
- Cryptographic Systems & Services
- Implementing VPNs
- Adaptive Security Appliance Introduction & Implementation
- Introduction to ASDM
- Managing a Secure Network

CyberHot (Summer School – 29th of September 2023)

Website: CyberHOT

Contact: Polemi Despoina (dpolemi@unipi.gr)

Course Content

- Threat and attack monitoring
- Evaluate strategies, tools & procedures
- Apply system administration
- Monitoring of networks
- Detecting & responding to attacks

Cybersecurity Policies and Practices in the EU – for non-IT experts

Website: Cybersecurity Policies and Practices in the EU – for non-IT Experts (Full course) - Eipa

Contact: Polemi Despoina (dpolemi@unipi.gr)

Course Content

- Legal and policy aspects of cybersecurity in the EU
- Assessing cybersecurity risks
- Cybersecurity management and governance
- Crisis communication, business continuity and disaster recovery planning

AIS / GNSS spoofing

Contact: Bruno Bender

Course Content

- Risks and threats on GNSS
- Risks and threats on AIS
- Use cases
- Securisation of AIS
- Securisation of GNSS

Tools Used: Secure AIS transponders

3.2 CSP Commercial Partner Cybersecurity Course Catalogue

3.2.1 Focal Point (FP), Belgium

Professional Training (No ECTS)

Course Name: Tabletop Exercise

Department: Focal Point

Contact: plaras@focalpoint-sprl.be

Language: English

Course Content

The tabletop exercise is designed and delivered as an interactive, gamified experience with the purpose of providing a high-level understanding of business impacts caused by cyber-attacks. Participants will be introduced to foundational concepts of cyber hygiene and its practices and, consecutively, be given the chance to experiment with these concepts through the interactive element of the tabletop exercise. The exercise is designed for students and low to mid-level employees in various sectors. Participants of the exercise require no previous knowledge of concepts or specific terms, and neither will require any degree of mastery over applying these concepts.

This exercise is designed to raise the overall level of cyber awareness for participants and increase their receptiveness to discussing, interacting with, and thinking about cyber hygiene concepts. As such, it is best utilised as an early part of single or multi-day seminars or educational workshops as participants finishing this exercise will feel more inclined to further engage with any following exercises, seminars, and other educational opportunities within the training events, multiplying their educational outcomes. Additionally, the group element of the exercise is selected to lend the interactive scenarios opportunities for team building within the exercise setting and promoting this spirit broadly to the educational event.

Course Name: FP_CDX

Department: Focal Point

Contact: cgrigor@focalpoint-sprl.be

Language: English

Course Content

Leveraging the power of Sentinel, students are assigned their own instances of the SIEM, empowering them to utilize advanced qtl queries to actively monitor the FP_CDX network and machines and unearth logs generated by a diverse range of simulated attacks. The cyber defense exercise encompasses a rich repertoire of attack scenarios, carefully crafted to emulate the tactics employed by cyber adversaries. A few examples of the attacks that students can expect to encounter:

Enumeration Attacks (Domain & User): Students gain hands-on experience in identifying weaknesses within the active directory by conducting targeted enumeration attacks. These attacks allow them to map out the network's structure, discover hidden resources, and gather crucial information about the domain and its users.

User Spraying: This attack technique involves attempting to gain unauthorized access by systematically trying common passwords or a set of pre-determined passwords against a large number of user accounts. By simulating such attacks, students learn to recognize and mitigate the risks associated with weak or easily guessable passwords.

SMB Share Anonymous: The platform provides an opportunity for students to explore the vulnerabilities associated with Server Message Block (SMB) shares. Through this exercise, they understand the potential risks of improperly configured SMB shares, such as unauthorized access to sensitive information.

Zerologon: This simulated attack mirrors the infamous Zerologon vulnerability, enabling students to understand the impact of exploiting this critical weakness in the Windows Server environment. By studying this attack, students gain insights into the significance of timely patching and proactive vulnerability management.

ASREPRoast: Students delve into the intricacies of ASREPRoast attacks, which target weak Kerberos authentication protocols. By attempting to crack password hashes offline, students gain a deep understanding of the vulnerabilities present in authentication mechanisms and the importance of robust password policies.

Kerberoasting: This exercise challenges students to exploit vulnerabilities in service accounts and Kerberos ticket-granting tickets (TGTs). By attempting to extract sensitive information from compromised service accounts, students develop vital skills in detecting and mitigating Kerberoasting attacks.

AD ACL Abuse: The platform provides a simulated environment to explore the consequences of Access Control List (ACL) misconfigurations. Through this exercise, students comprehend the potential impact of improperly assigned permissions and learn to implement secure and well-defined access control measures.

Through the cyber defense exercise, students not only learn about these attack techniques but also develop a comprehensive understanding of defensive strategies, incident response, and mitigation techniques. The immersive nature of the platform ensures that students cultivate essential skills in analyzing logs, identifying threats, and effectively responding to cyber incidents.

As students navigate through the platform's engaging interface, they are presented with rich visual elements, including interactive diagrams and real-time graphical representations of network traffic and system logs. These visual aids enhance the learning experience, allowing for better comprehension and retention of critical cybersecurity concepts.

In summary, Focal Point's cyber defense exercise provides a complete view of the vulnerable surface applicable to active directory environments and an approach to log analytics that is hand in hand with cutting edge approaches.

Course Name: FP_Training Lab

Department: Focal Point

Contact: cgrigor@focalpoint-sprl.be

Language: English

Course Content

The FP Training Lab offers a comprehensive course focused on red teaming, where students are not only taught but also actively engage in performing a variety of realistic attacks. The purpose of this course is to provide hands-on experience and in-depth knowledge of red teaming methodologies and techniques, empowering students to simulate real-world cyber attacks and evaluate an organization's defensive capabilities.

Under the guidance of experienced instructors, students learn the intricacies of red teaming, starting with the fundamentals and gradually progressing to more advanced techniques. The curriculum covers a wide range of offensive security topics, including reconnaissance, network enumeration, privilege escalation, and lateral movement.

Throughout the course, students actively perform simulated attacks, leveraging the tools and methodologies used by real-world red teamers. They learn to exploit vulnerabilities within the FP_Training_Lab employing techniques such as injections, buffer overflows, brute-forcing, as well as exploiting misconfigurations. Through hands-on exercises and practical simulations, students gain a deep understanding of the attacker's mindset and the techniques employed to infiltrate systems.

Course Name: HtB_Enterprise_Labs: Introduction To Penetration Testing

Department: Focal Point

Contact: cgrigor@focalpoint-sprl.be

Language: English

Course Content

Throughout our introduction to penetration testing course, the wide range of virtual machines and challenges included in the HtB enterprise labs are utilized to introduce the students to a series of different attack scenarios and tools. The course covers a vast variety of introductory penetration testing scenarios so that the participants will be able to develop the proper vocabulary and understanding concerning existing attacks. The attacks taught include:

- Injections
- LFI/RFI
- IDOR
- CSRF
- XSS
- Command Injection
- SUID
- Priviledge escalation

3.2.2 Maggioli SPA (MAG),Italy

Professional Training (No ECTS)

Course Name: The Application Consultant

Department: Maggioli Academy

Contact: spiros.borotis@maggioli.gr

Language: Italian

Course Content

The aim of the training is to a general understanding of the public administration world and related services. It represents our delivery training ground. Duration: 160 hours. This course is designed for recent graduates.

Course Name: Junior Full Stack Developer

Department: Maggioli Academy

Language: Italian

Course Content

With the aim of training a group of graduates in three-year scientific subjects on the topics of CLOUD development. It represents our developers' training ground. Duration: 160 hours.

Course Name: Data Science basic and advance

Department: Maggioli Academy

Contact: spiros.borotis@maggioli.gr

Language: Italian

Course Content

The Data Science training program, now in its 5th edition, has been designed for those who want to invest in the key skills of tomorrow. Data analysis and the ability to navigate through records, numbers, information, and data are increasingly in demand in the job market.

Course Name: Project Management

Department: Maggioli Academy

Contact: spiros.borotis@maggioli.gr

Language: Italian

Course Content

As a market leader, we believe that companies should become places of higher education, fostering advanced skills that are directly applicable in the world of work. In this regard, one characteristic of Maggioli Academy's course instructors is that they are, first and foremost, business professionals with teaching experience.

Course Name: Cyber Security Specialist

Department: Maggioli Academy

Contact: spiros.borotis@maggioli.gr

Language

Italian

Course Content

The (1st Edition) arises from the need to train professional profiles for both the public administration sector and the private sector, with specialized technical skills and a cross-functional vision across different areas of expertise: technology, organizational, procedural, legal, and legislative.

Seminars (No ECTS)

Seminar’s Name: Bootcamp Maggioli Academy

Department: Maggioli Academy

Contact: spiros.borotis@maggioli.gr

Language: Italian

Seminar’s Content

It is an intensive training initiative, now in its second edition. It is a three-day immersive experience that involves two final year classes of the "Business Information Systems" course from Rino Molari Technical Institute in Santarcangelo di Romagna, in an innovative artificial intelligence project

Seminar’s Name: H-Greenovation

Department: Maggioli Academy

Contact: spiros.borotis@maggioli.gr

Language: Italian

Seminar’s Content

It is an original and engaging team-based project marathon that stems from the strong collaboration and co-design of innovative training programs between the Higher Institutes and the Maggioli Group. The 2022 initiative involved a total of 48 students from the "Einaudi - Molari" high schools in 2 challenges dedicated to #GreenMobility and #GreenPackaging.

Seminar’s Name: Girls Code it Better

Department: Maggioli Academy

Contact: spiros.borotis@maggioli.gr

Language: Italian

Seminar’s Content

It is an all-female initiative promoted by Officina Futuro Fondazione W-Group, aimed at encouraging girls to pursue studies in the STEM field (Science, Technology, Engineering, and Mathematics). Our Maggioli Academy has set a national record by hosting 44 students from Franchini Institute in Santarcangelo di Romagna, divided into two clubs.

3.2.3 SINTEF, Norway

Postgraduate courses

Introduction to Cyber Security

Department: SINTEF Digital together with Norwegian University of Science and Technology (NTNU)

Semester: Spring

ECTS: 2.5

Contact: Karin Bernsmed

Course content: This course/topic will focus on digital systems, where digital security is a very important feature. The course will provide a basic introduction to how a digital system is constructed. The criticality, complexity and diversity of digital systems will then be discussed (human, technological, organizational and interaction between actors). The emphasis is on showing dependencies between digital systems, how digital solutions are incorporated into systems that are necessary to maintain society's basic needs (critical infrastructure) and to discuss what can happen in the event of attacks and errors in such systems.

Introduction to Cyber Security: Risk Management

Department: SINTEF Digital together with Norwegian University of Science and Technology (NTNU)

Semester: Spring

ECTS: 2.5

Contact: Karin Bernsmed

Course content:

Risk-based approach to digital security

Risk assessment-based identification ISO/IEC 27005

Threat profiling

Consequence and vulnerability assessment

Risk management

Seminars

Thinking like an attacker

Department: SINTEF Digital

Semester: By demand

Course content: Cybersecurity failure is seen as a critical threat to the world in 2022, and now more than ever, it needs to be taken seriously. Every company is vulnerable and working in security today is more about making the life of an attacker as difficult as possible and being ready to respond in case of a breach. In this introduction course, we look at how “thinking like an attacker” can help secure a company. We first cover the security testing methodology before moving on to a set of hands-on exercises covering common flaws in web applications. Recommendations: While this course does not assume any security knowledge, having some programming background and a basic understanding of the inner working of the web is important.

Digital Torc training

Department: SINTEF Digital

Semester: By demand

Course content: Training for Operational Resilience (TORC) is a training-by-gaming approach based on a board-game setup. TORC is designed to facilitate organizations and teams that seek to reveal, understand, articulate, demonstrate and/or develop their inherent repertoire of resilient performance in face of unexpected deviations, disturbances and shocks. The training outcomes and experiences are captured in a way that prepares them to be used as raw material of technological, human, organizational and managerial priorities and resources that are needed to transform the experience from the training exercise into effective resilience capabilities under a more formal managerial supervision.

Tool used: https://torc.no/

3.2.4 trustilio, Netherlands

Professional Training (No ECTS)

ISO 27001

Department: N/A

Contact: Kitty Kioskli (kitty.kioskli@trustilio.com)

Course Content

The course content for ISO 27001 covers a comprehensive range of topics related to information security management systems. Participants will gain a deep understanding of the ISO 27001 standard, its framework, and requirements. The course delves into risk assessment and management, emphasizing the identification and mitigation of potential threats to information security. Participants will learn about security controls, policies, and procedures to protect sensitive data and maintain the confidentiality, integrity, and availability of information assets. Additionally, the course covers incident response and business continuity planning, ensuring organizations are prepared to handle security incidents and maintain operations during disruptions. Overall, the course equips participants with the knowledge and skills to establish, implement, and continually improve information security management systems based on ISO 27001 standards.

Some of the concepts that are addressed are:

- Information Security Management System (ISMS): Understanding the purpose, benefits, and requirements of implementing an ISMS based on ISO 27001.
- Risk Assessment and Management: Identifying and assessing information security risks, developing risk treatment plans, and implementing controls to mitigate those risks.
- Security Controls: Exploring various security controls and measures to protect information assets, including physical security, access controls, encryption, and network security.
- Policies and Procedures: Developing and implementing information security policies, procedures, and guidelines to ensure consistent practices throughout the organization.
- Incident Response and Business Continuity: Preparing for and responding to security incidents, including incident handling, investigation, and recovery procedures. Additionally, understanding the importance of business continuity planning to maintain operations during disruptions.
- Compliance and Audit: Comprehending the compliance requirements of ISO 27001 and conducting internal audits to assess the effectiveness of the ISMS.

- Continual Improvement: Establishing processes for monitoring, measuring, and continually improving the effectiveness of the ISMS, including regular reviews and updates to address changing security risks and requirements.

Lean Business Canvas Model

Department: N/A

Contact: Kitty Kioskli (kitty.kioskli@trustilio.com)

Course Content

The course content for the Lean Business Canvas Model revolves around providing participants with a practical framework for designing and refining business models. The course covers key elements of the Lean Business Canvas, including customer segments, value propositions, channels, customer relationships, revenue streams, key resources, key activities, key partnerships, and cost structure. Participants learn how to identify and understand customer needs, create unique value propositions, and design effective channels to reach target customers. The course also emphasizes the importance of continuous learning and adaptation, encouraging participants to validate assumptions, test hypotheses, and iterate their business models based on customer feedback and market insights. By the end of the course, participants will have a solid understanding of how to use the Lean Business Canvas Model as a tool for strategic decision-making and business innovation.

Some of the concepts that are addressed are:

- Customer Segments: Identifying and understanding the different groups of customers or target market segments that a business aims to serve.
- Value Propositions: Defining the unique value that a business offers to its customers and how it solves their problems or satisfies their needs.
- Channels: Determining the most effective channels or distribution methods to reach and engage with customers, considering both online and offline options.
- Customer Relationships: Understanding the types of relationships and interactions that need to be established with customers to create and maintain loyalty.
- Revenue Streams: Identifying the different sources of revenue for the business, such as product sales, subscriptions, licensing, or advertising.
- Key Resources: Identifying the essential resources, assets, or capabilities required to deliver the value proposition and run the business successfully.
- Key Activities: Defining the crucial activities or actions that need to be performed to create, deliver, and maintain the value proposition.
- Key Partnerships: Recognizing the strategic alliances or partnerships that can provide essential resources, expertise, or access to new markets.
- Cost Structure: Understanding the cost drivers and determining the cost structure of the business, including fixed costs, variable costs, and economies of scale.
- Validation and Iteration: Emphasizing the importance of validating assumptions, testing hypotheses, and continuously iterating and improving the business model based on customer feedback and market insights.

3) Code Auditing

Department: N/A

Contact: Costas Voliotis (costas.voliotis@codewetrust.com)

Tool: C2M

Website: https://www.codewetrust.com/download

Course Content

The course content for Code Auditing focuses on the essential skills and techniques required to assess and evaluate the security, efficiency, and quality of software code. Participants will learn how to conduct thorough code reviews to identify vulnerabilities, bugs, and potential security risks. The course covers various programming languages, code analysis tools, and best practices for code auditing. Participants will gain an understanding of common coding errors, such as input validation issues, injection vulnerabilities, and insecure coding practices. They will also learn how to analyze code for performance bottlenecks and identify areas for optimization. Additionally, the course emphasizes the importance of compliance with coding standards, code documentation, and code maintainability. By the end of the course, participants will be equipped with the knowledge and skills to perform comprehensive code audits, enhance the security and quality of software systems, and contribute to the development of secure and efficient code.

Some of the concepts that are addressed are:

- Code Review Process: Understanding the systematic approach to reviewing and analyzing code, including planning, execution, and documentation of the code audit process.
- Security Vulnerabilities: Identifying common security vulnerabilities in code, such as input validation flaws, cross-site scripting (XSS), SQL injection, and insecure authentication and authorization mechanisms.
- Code Quality and Best Practices: Evaluating code for adherence to coding standards, readability, maintainability, and scalability. Understanding best practices for writing secure, efficient, and maintainable code.
- Code Analysis Tools: Familiarizing with code analysis tools and techniques used for static code analysis, vulnerability scanning, and identifying code smells and performance issues.
- Secure Coding Practices: Learning and promoting secure coding practices, including input validation, output encoding, proper error handling, secure session management, and data protection.
- Performance Optimization: Identifying performance bottlenecks in code, such as inefficient algorithms, memory leaks, or excessive database queries, and suggesting optimization strategies.
- Compliance and Standards: Understanding the importance of complying with industry standards, regulations, and guidelines related to code security, privacy, and data protection.
- Reporting and Documentation: Documenting findings, vulnerabilities, recommendations, and suggested remediation measures in a clear and concise manner for stakeholders and developers.
- Continuous Improvement: Emphasizing the need for ongoing code auditing, security testing, and continuous improvement to ensure the long-term security and quality of software code.

Seminars (No ECTS)

CyberHOT
Department: N/A

Contact: Kitty Kioskli (kitty.kioskli@trustilio.com)

Website: https://www.cyberhot.eu/

Seminar Content

The CyberHOT training program, based upon NATO Red Teaming knowledge and expertise, will enable the participants to implement various red-teaming methodologies and tools. Utilizing the dedicated labs by HacktheBox, a wide range of penetration testing scenarios will be showcased. The aim is to raise the skills of the workforce to meet current and future cyber incidents and challenges. An introductory session will cover popular red-teaming/penetration testing tools, along with basic steps followed in penetration testing methodologies. Having introduced a general methodology to penetration testing along with the tools to apply it, the participants will be introduced to the Dedicated labs of the Hack the Box platform where each participant will boot their own instances of attacker and target machines and pawn them along with the lecturers.

3.2.5 Zelus, Greece

Department: N/A

Contact: Stella Markopoulou (s.markopoulou@zelus.gr)

Tool: SmartViz

Website: https://www.zelus.gr/smartviz/

Language: English

Course Content

This training course, we will explore various aspects of cybersecurity while leveraging the functionalities of SmartViz. It aims to provide a detailed understanding of key cybersecurity concepts and their practical application. The key topics covered in this course:

Incident Response and Decision-Making:

Incident response plays a pivotal role in effective cybersecurity management. This training equips participants with the skills to make prompt and accurate decisions when faced with alerts and events in the environment. By assessing the severity of potential threats, participants will determine when to initiate incident response procedures, ensuring efficient incident management and mitigation.

Threat Intelligence Analysis:

Effective threat intelligence analysis is crucial in today's dynamic cybersecurity landscape. Participants will acquire the skills to analyse logs, network traffic, and system behaviour, enabling them to identify potential indicators of compromise. By leveraging various threat intelligence sources, participants will learn to interpret and analyse these indicators to detect and respond to threats promptly.

Defensive Analysis:

A robust defence is vital in mitigating cyber attacks. This course covers defensive analysis techniques that employ both automated tools and manual methods to simulate real-world attacks. Participants will gain practical insights into testing defensive measures, security controls, and monitoring capabilities. Additionally, they will learn to document and present detailed reports containing findings, recommended remediation strategies, and security best practices.

Penetration Testing or Ethical Hacking:

The course begins by delving into the field of penetration testing or ethical hacking. Participants will learn the techniques involved in identifying and exploiting vulnerabilities in computer systems, networks, and applications. Through simulated attacks imitating malicious actors, participants will gain hands-on experience in assessing and strengthening the security posture of organisations.

Throughout the course, the SmartViz tool will be utilised to visualise and analyse cybersecurity data, enriching the learning experience. Participants can expect to gain comprehensive knowledge and practical skills to tackle cybersecurity challenges effectively.

3.2.6 APIROPLUS Solutions, Cyprus

Seminar’s Name : ISO 27001 Auditor / Lead Auditor Course IRCA Approved

Department: APIROPLUS Solutions & LRQA Hellas

Contact: ac@apiroplus.solutions

Language: English or Greek

Duration: 40 hours

Seminar’s Content:

This course is an ideal course for those wishing to pursue a qualification in information security management systems auditing, or to develop advanced skills in auditing information security management systems.

The course covers

- the importance and benefits of information security for the organisation and its customers
- the basic structure and requirements of ISO/IEC 27001:2022
- the correlation of the PDCA cycle to the requirements of ISO/IEC 27001:2022
- the principles and methods prescribed related to information security risk management and the connection to Annex A
- the mandatory minimum documentation related to an ISO/IEC 27001:2022 implementation
- the terms, definitions, principles, methods and techniques for the implementation of a third
- party audit
- the process and activities implemented related to audit and certification according to ISO 19011 and ISO 17021
- the differentiation between ISO/IEC 27001:2022 audit for the core requirements (4-10) and the assessment of the controls of Annex A
- how to control and work with an audit team with practical examples related to an ISMS audit
- the skills to audit processes and their interaction with other processes
- the reporting of findings and audit conclusions.

Other information: With the successful completion of the course, the participants have the ability to participate in the relevant ISO 27001:2022 exams administered by the International Register of Certified Auditors (IRCA).

Seminar’s Name: Introduction to the new ISO/IEC 27001 version

Department: APIROPLUS Solutions

Contact: ac@apiroplus.solutions

Language: English or Greek

Duration: 8 hours

Seminar’s Content:

The course has been created to introduce to the greater audience the requirements and operations of ISO/IEC 27001. Since the course has been created near the publication of the new ISO/IEC 27001 standard, the course also focuses on the changes between version 2013 and version 2022.

The course covers

- the importance and benefits of information security for the organisation and its customers;
- the basic structure and requirements of ISO/IEC 27001:2022;
- the principles and methods prescribed related to information security risk management and the connection to Annex A;
- the mandatory minimum documentation related to an ISO/IEC 27001:2022 implementation;
- the transition period for certified ISO/IEC 27001:2013 systems based on the IAF Mandatory Document;
- the changes between version 2013 and version 2022 for the core requirements (4-10); and
- the changes between version 2013 and version 2022 for the controls of Annex A and the way that ISO/IEC 27002:2022 is used.

Seminar's Name: Cybersecurity Maturity Models Requirements / Auditing practices

Department: APIROPLUS Solutions

Contact: ac@apiroplus.solutions

Language: English or Greek

Duration: 8 hours

Seminar's content:

The last years, maturity models have been introduced also in the cybersecurity domain. Although the cybersecurity maturity models developed are still in their early stages and vary in type, scope and range, the market has already identified them as a valuable asset for organisations.

The course covers

- the concept of maturity models in general and in specific in cybersecurity,
- the different types of maturity models and their scales,
- well known examples of cybersecurity maturity models
- processes and methods utilised in order to assess the compliance of an organisation against the requirements of the levels of specific cybersecurity maturity models.

4 CSP Cybersecurity Tool and Platform Catalogue

4.1 Assessment methodology for Training Tools and Platforms

This section delineates the formalized assessment methodology employed to evaluate the training tools and platforms employed within the CyberSecPro. The comprehensive assessment process encompassed the distribution of questionnaires and the execution of workshops, involving genuine participants partaking in both physical and online training sessions. An integral facet of the assessment procedure involved the generation of evaluation reports for each training tool, centering on crucial aspects such as session summaries, learning outcomes, and demonstrative efficacy.

A pivotal aspect of the assessment methodology involved the distribution of questionnaires to participants, focused on each training tool's suitability across various training contexts. These questionnaires inquired about the utilization of the tool in scenarios like commercial seminars, courses, academic labs, cybersecurity exercises, hackathons, serious games, specific topics, network security, penetration testing, incident response, cloud security, risk management, forensics, and other settings. The questionnaire template is provided in Annex G.

Furthermore, a Training Workshop was convened in Chania, Greece, on the 25-26th of September 2023 (Training Schedule & Reports are detailed in Annex C and E). The primary aim of the workshop was to meticulously evaluate the effectiveness and appropriateness of a selection of tools and platforms through live training sessions with real participants. The primary objective was to ascertain the impact of these tools on participants' comprehension and competency in the field of cybersecurity, considering the diverse knowledge areas outlined in Section 5.1.

Each evaluation report (a template is provided in Annex D**)** for the training tools and platforms adhered to a structured framework comprising the following key components: a summary of the training session, an overview of the specific training tool, learning outcomes assessment, and descriptions of any practical demonstrations that were part of the training sessions.

The learning outcomes assessment focused on participants' ability to achieve specific outcomes aligned with the knowledge areas defined in Section 5.1. These outcomes covered various aspects of cybersecurity, including malware detection, forensics, incident response, and more. A brief presentation of any practical demonstrations conducted during the training sessions, elucidating their pertinence to the specified learning objectives.

The evaluation also considered user-friendliness, trainee and trainer privacy, and compliance with academic culture, principles, and values.

The assessment was based on the appropriateness of the training tools integrated into the CyberSecPro training processes to achieve its learning objectives. The tools were also assessed with holistic assessment criteria, against a myriad of facets: user-friendliness, trainee and trainer privacy, and compliance with academic culture, principles, and values.

The assessment methodology employed for training tools and platforms in the CyberSecPro adhered to a rigorous and comprehensive approach, encompassing questionnaires, hands-on training sessions, and expert evaluations. The insights and recommendations garnered from the evaluation reports will serve as invaluable guidance for optimizing the selection and utilization of training tools and platforms, with a commitment to nurturing learning excellence within the multifaceted realm of cybersecurity. The following graphs illustrate the results of the assessment conducted.

4.1.1 Tools Level of Difficulty

The CSP consortia offering for tools was measured on difficulty levels. The tool offerings show various levels of tool difficulty (Figure 1) and the tool offerings is adaptable delivery, courses and to levels of expertise (Figure 2).

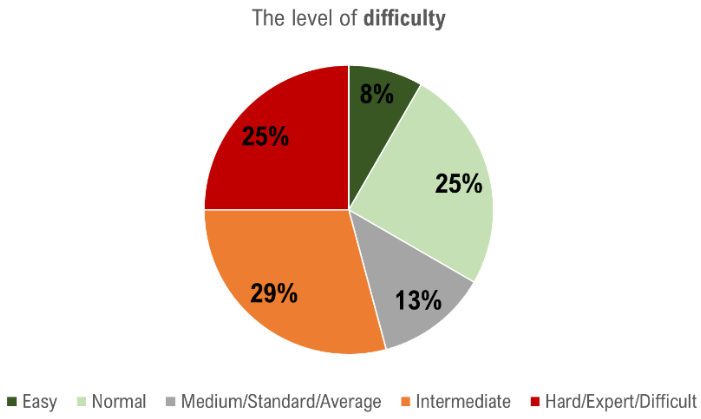


Figure 1:Tool Level of Difficulty

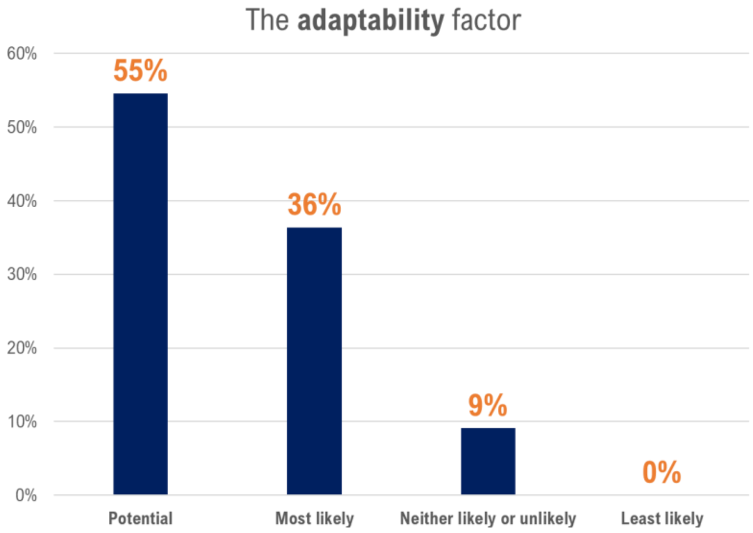


Figure 2: Adaptability

The tools were also evaluated for implementation to different knowledge areas, sectors and expertise. Most tools were evaluated to be easily implemented (50%) or implementable with some minor aspects to consider (45%) while only 5% of the tools were deemed implementable but having major issues due to specificity of the tool, previous knowledge or other requirements making it difficult to implement in training. The tools were also considered to be easily (41%) scalable for short trainings (hours-days) and longer training approaches (more than one week) or having some minor issues for scalability (59%) due to trial versions of software, application aspects of tools specifications, or other tool requirements.

4.1.2 Tool Knowledge Areas, Deliveries, and Requirements

The tools were evaluated on background knowledge (both knowledge areas and previous needed knowledge) and deliveries of the tool trainings. The CSP tool offerings do have some previous knowledge requirements (see Figure 3 for knowledge requirement levels) and would reference the course descriptions in sections 4.2 (CSP Academic Tools Offerings) and 4.3 (CSP Commercial Tool Offerings) for specific tool requirements.

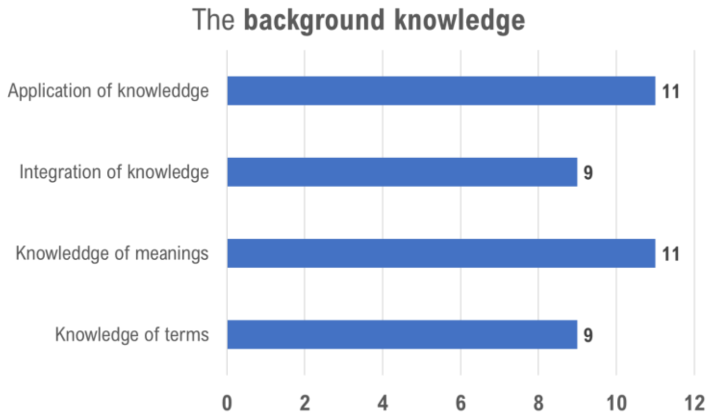


Figure 3: Background Knowledge Requirements

Forty-eight percent (48%) of the tools were offered as academic labs courses, while 18% of the courses were commercial seminars lasting up to two days. The remaining tools (34%) were classified as cybersecurity exercises and/or cyber ranges, network security control tools, or penetration testing tools that had no specific timeframe of delivery as these tools can be adapted to any course length. The tools were also evaluated for use in different course offerings and structures. Twenty-nine percent (29%) of the tools are evaluated to be appropriate for teaching cybersecurity exercises and cyber ranges, 23% of the tools can be used for cybersecurity hackathons, 20% of the tools are relevant for cybersecurity games and certification courses, and 11% of the tools are relevant for network security control learning modules. While the tools are scalable and adaptable to different knowledge areas, deliveries and sill development, the tools were also evaluated on what areas they would not be appropriate for use. Twenty-eight percent (28%) of the tools offered by CSP partners are not appropriate for courses lasting several months, 16% of the courses are not suitable for certification, and 14% of the tools are appropriate for short seminars (up to two days) or for cyber security games. As for knowledge areas, some tools were not appropriate to use for instructing n risk management (16%) or incident response (14%).

4.2 CSP Academic Cybersecurity Training Tools and Platforms (All HEIs)

4.2.1 Wireshark

Filled by	Leo Johannesburg-Paresh Rathod
Organization	Laurea University of Applied Sciences
Date	24-05-2023
Contact	leo.johannesberg@laurea.fi - paresh.rathod@laurea.fi
License	O
Cost of license	O
Available link to download tool	https://www.wireshark.org/#download
Online manual(s)	https://www.wireshark.org/docs/
Online tutorial(s)	https://www.youtube.com/watch?v=zOYohNOnWp4

Description

Summary
Guidelines:Wireshark is a freely available open-source network protocol analyzer tool. Users can observe what is happening on their network at a granular level. The primary function of Wireshark is to capture and interactively browse the traffic running on a computer network. It offers a perspective into the data traversing a network, when diagnosing network problems, tracking down cyber threats, or learning more about network protocols. *Wireshark simplifies network troubleshooting and analysis by presenting captured packet data in a human-readable form. It allows users to identify unusual network behaviour. As a learning tool, it can be used to enhance understanding of network protocols and their interactions, network troubleshooting, and network security concepts.* *Wireshark can assist in gaining knowledge in areas such as network analysis, intrusion detection, and traffic analysis. It helps develop skills such as packet analysis, traffic interpretation, and identifying malicious network activities. Competencies include network security and network diagnostics.* *Wireshark can perform a wide array of operations, including real-time network traffic analysis, offline analysis of captured files, filtering of network traffic, and more. Wireshark addresses problems related to network performance, security vulnerabilities, and network troubleshooting.*

Assessment

The training tool has been used for

Commercial seminar (up to 2 days)	x
Commercial course (up to 2 months)	
Academic Lab (accompanying cybersecurity course) / Academic course	x
Cybersecurity exercise /cyber range	
Cybersecurity hackathon	
Cybersecurity game	x
Certification cybersecurity course	x
Specific Cybersecurity Topic(s)	x
Network security control	x
Penetration testing	x
Incident response	
Cloud security	
Risk management	x
Forensics	
Other – write which one	
Demonstration /training to Customer	x
Pilot training operation	

Other (explain in free text):	

*If “**Other**”, then respond in free text.*

Is this training tool suitable for training purposes (reach the learning objectives and knowledge areas)

Yes	**x**
No	

Are there any needed compute resources (CPUs, GPU, RAM, Disk space)?

Yes	**x**
No	

*If “**Yes**”, then respond in free text.*

For Microsoft Windows:3

Any modern 64-bit AMD64/x86-64 or 32-bit x86 processor.

500 MB available RAM. Larger capture files require more RAM.

500 MB available disk space. Capture files require additional disk space.

For macOS:

macOS 10.14 and later

What is the level of difficulty to use the training tool?

Easy	
Normal	**x**
Medium/Standard/Average	
Intermediate	
Hard/Expert/difficult	

Is this training tool easily adaptable to a specific training program?

Potential	
Most likely	**x**
Neither likely or unlikely	
Least likely	

Is this training tool easily implementable for a specific training program?

Not implementable	
Implementable with minor issues (inconsistencies)	
Implementable with major issues (inconsistencies)	
Implementable	**x**

Is this training tool easily scalable for a specific training program?

Not scalable	
Scalable with minor issues (inconsistencies)	
Scalable with major issues (inconsistencies)	
Scalable	**x**

Does this training tool cover interoperability aspects of a specific training program?

Not interoperable	
Interoperable with minor issues (inconsistencies)	**x**
Interoperable with major issues (inconsistencies)	
Interoperable	

Is this training tool stable while used in a specific training program?

Not stable	
Stable with minor issues (inconsistencies)	
Stable with major issues (inconsistencies)	
Stable	x

Does this training tool support the user's (trainer, trainee) privacy and security aspects?

Yes.	x
No	
Other	

*If "**Other**", then respond in free text*

What is the level of prior knowledge needed to use the training tool?

Knowledge of terms	x
Knowledge of meanings	
Integration of knowledge	
Application of knowledge	

Do the trainers/trainees find the training tool easy to use?

Yes	**x**
No	

Does this training tool support the trainers/trainees' native language and/or multiple languages?

Yes	
No	**x**

Appropriateness of the training tool. Tool can be used for:

VG: very good, **G**: good, **NA**: not appropriate	**VG**	**G**	**NA**
Commercial seminar (up to 2 days)	**x**		
Commercial course (up to 2 months)	**x**		
Academic Lab (accompanying cybersecurity course) / Academic course	**x**		
Cybersecurity exercise /cyber range	**x**		
Cybersecurity hackathon	**x**		
Cybersecurity game	**x**		
Certification cybersecurity course		**x**	
Specific Cybersecurity Topic(s)		**x**	
Network security control		**x**	

Penetration testing			x
Incident response		x	
Cloud security			x
Risk management			x
Forensics	x		
Other – write which one			

4.2.2 Nmap

Filled by	Panayiotis Kotzanikolaou - Dimitris Koutras
Organization	UPRC
Date	20-05-2023
Contact	pkotzani@unipi.gr – dkoutras@unipi.gr
License	O
Cost of license	-
Available link to download tool	https://nmap.org/download.html
Online manual(s)	https://nmap.org/docs.html
Online tutorial(s)	https://www.youtube.com/watch?v=5MTZdN9TEO4 https://www.youtube.com/watch?v=VFJLMOk6daQ&list=PLBf0hzazHTGM8V_3OEKhvCM9Xah3qDdIx&index=2 https://www.youtube.com/watch?v=OUQkCAHdX_g&list=PLBf0hzazHTGM8V_3OEKhvCM9Xah3qDdIx&index=3

Description

Summary
NMAP is a versatile network scanning and mapping tool that provides comprehensive network security insight. With its extensive capabilities, NMAP allows users to identify open ports, discover hosts and services, and perform vulnerability scans. Its flexibility and is allowed for scripting and automation, making it valuable to both network administrators and security professionals. *NMAP supports advanced scanning techniques like TCP SYN scan, UDP scan, and OS detection.* *It can perform version detection to identify running services and their versions.* *NMAP provides flexible output options, including machine-readable formats like XML and JSON.* *It supports scripting with NSE (Nmap Scripting Engine) for automation and custom vulnerability checks.*

Assessment

The training tool has been used for

Commercial seminar (up to 2 days)	
Commercial course (up to 2 months)	
Academic Lab (accompanying cybersecurity course) / Academic course	X
Cybersecurity exercise /cyber range	X
Cybersecurity hackathon	
Cybersecurity game	
Certification cybersecurity course	
Specific Cybersecurity Topic(s)	
Network security control	X
Penetration testing	X
Incident response	
Cloud security	
Risk management	
Forensics	
Other – write which one	
Demonstration /training to Customer	
Pilot training operation	

Other (explain in free text):	

*If “**Other**”, then respond in free text.*

Is this training tool suitable for training purposes (reach the learning objectives and knowledge areas)

Yes	**X**
No	

Are there any needed compute resources (CPUs, GPU, RAM, Disk space)?

Yes	
No	**X**

*If “**Yes**”, then respond in free text.*

What is the level of difficulty to use the training tool?

Easy	
Normal	**X**
Medium/Standard/Average	
Intermediate	
Hard/Expert/difficult	

Is this training tool easily adaptable to a specific training program?

Potential	**X**
Most likely	
Neither likely or unlikely	
Least likely	

Is this training tool easily implementable for a specific training program?

Not implementable	
Implementable with minor issues (inconsistencies)	
Implementable with major issues (inconsistencies)	
Implementable	**X**

Is this training tool easily scalable for a specific training program?

Not scalable	
Scalable with minor issues (inconsistencies)	
Scalable with major issues (inconsistencies)	
Scalable	**X**

Does this training tool cover interoperability aspects of a specific training program?

Not interoperable	
Interoperable with minor issues (inconsistencies)	
Interoperable with major issues (inconsistencies)	
Interoperable	**X**

Is this training tool stable while used in a specific training program?

Not stable	
Stable with minor issues (inconsistencies)	
Stable with major issues (inconsistencies)	
Stable	**X**

Does this training tool support the user's (trainer, trainee) privacy and security aspects?

Yes.	**X**
No	
Other	

*If "**Other**", then respond in free text*

What is the level of prior knowledge needed to use the training tool?

Knowledge of terms	
Knowledge of meanings	
Integration of knowledge	**X**
Application of knowledge	

Do the trainers/trainees find the training tool easy to use?

Yes	**X**
No	

Does this training tool support the trainers/trainees’ native language and/or multiple languages?

Yes	
No	**X**

Appropriateness of the training tool. Tool can be used for:

VG: very good, **G**: good, **NA**: not appropriate	**VG**	**G**	**NA**
Commercial seminar (up to 2 days)		**X**	
Commercial course (up to 2 months)			**X**
Academic Lab (accompanying cybersecurity course) / Academic course	**X**		
Cybersecurity exercise /cyber range		**X**	
Cybersecurity hackathon		**X**	
Cybersecurity game		**X**	
Certification cybersecurity course		**X**	
Specific Cybersecurity Topic(s)			
Network security control		**X**	
Penetration testing		**X**	
Incident response		**X**	
Cloud security			
Risk management			
Forensics			
Other – write which one			

4.2.3 Nessus

Filled by	Leo Johannesberg-Paresh Rathod
Organization	Laurea University of Applied Sciences
Date	05.24.2023
Contact	leo.johannesberg@laurea.fi - paresh.rathod@laurea.fi
License	C
Cost of license	Varies (free trial available)
Available link to download tool	https://www.tenable.com/products/nessus/nessus-professional
Online manual(s)	https://docs.tenable.com/nessus/Content/Nessus.htm
Online tutorial(s)	https://www.udemy.com/course/nessus-scanner-network-scanning-from-beginner-to-advanced/

Description

Summary
Guidelines: Nessus is a vulnerability scanner with a focus on detecting potential vulnerabilities within the network infrastructure. Its central role is to examine networks for potential security risks or known vulnerabilities that malicious actors could exploit. It delivers an overview of potential network vulnerabilities, assisting in identifying and remediating them. *Nessus serves to analyse networks, providing a full vulnerability management lifecycle, from identifying weaknesses to proposing solutions. Users learn to manage vulnerabilities, understand threats, and implement strategies to mitigate risks.* *Nessus can perform a variety of tasks, including vulnerability scanning, configuration auditing, and malware detection, among others. It tackles issues of network security, vulnerability management, and compliance.*

Assessment

The training tool has been used for

Commercial seminar (up to 2 days)	
Commercial course (up to 2 months)	
Academic Lab (accompanying cybersecurity course) / Academic course	x
Cybersecurity exercise /cyber range	
Cybersecurity hackathon	x
Cybersecurity game	
Certification cybersecurity course	x
Specific Cybersecurity Topic(s)	x
Network security control	x
Penetration testing	x
Incident response	
Cloud security	
Risk management	x
Forensics	
Other – write which one	
Demonstration /training to Customer	
Pilot training operation	

Other (explain in free text):	

*If "**Other**", then respond in free text.*

Is this training tool suitable for training purposes (reach the learning objectives and knowledge areas)

Yes	**x**
No	

Are there any needed compute resources (CPUs, GPU, RAM, Disk space)?

Yes	**x**
No	

*If "**Yes**", then respond in free text.*

Nessus Scanner (Scanning up to 50.000 hosts per scan) minimum hardware requirements:
CPU: 4 2GHz cores

Memory: 4 GB RAM (8 GB RAM recommended)

Disk space: 30 GB, not including space used by the host operating system

Note: Usage (e.g., scan results, plugin updates, and logs) increases the amount of disk space needed over time.
Nessus Agent minimum hardware requirements:
Processor: 1 Dual-core CPU

Processor Speed: > 1 GHz

RAM: > 1 GB

Disk Space: Agents 10.0.x and later: > 2 GB, not including space used by the host operating system

The agent may require more space during some processes.

Disk Speed: 15-50 IOPS

What is the level of difficulty to use the training tool?

Easy	
Normal	
Medium/Standard/Average	
Intermediate	**x**
Hard/Expert/difficult	

Is this training tool easily adaptable to a specific training program?

Potential	
Most likely	**x**
Neither likely or unlikely	
Least likely	

Is this training tool easily implementable for a specific training program?

Not implementable	
Implementable with minor issues (inconsistencies)	
Implementable with major issues (inconsistencies)	
Implementable	**x**

Is this training tool easily scalable for a specific training program?

Not scalable	
Scalable with minor issues (inconsistencies)	
Scalable with major issues (inconsistencies)	
Scalable	x

Does this training tool cover interoperability aspects of a specific training program?

Not interoperable	
Interoperable with minor issues (inconsistencies)	
Interoperable with major issues (inconsistencies)	
Interoperable	x

Is this training tool stable while used in a specific training program?

Not stable	
Stable with minor issues (inconsistencies)	
Stable with major issues (inconsistencies)	
Stable	x

Does this training tool support the user’s (trainer, trainee) privacy and security aspects?

Yes.	**x**
No	
Other	

*If "**Other**", then respond in free text*

Nessus will collect and/or process users' Personal Data. In order to provide you with access to the Site, they may process users' Personal Data.

If users create a profile or register with them, users will be asked to agree to provide certain information in order to access their services or view their content.

If users change their mind and wish to withdraw their consent to them processing your Personal Data, they may withdraw their consent at any time.

What is the level of prior knowledge needed to use the training tool?

Knowledge of terms	
Knowledge of meanings	**x**
Integration of knowledge	
Application of knowledge	

Do the trainers/trainees find the training tool easy to use?

Yes	**x**
No	

Does this training tool support the trainers/trainees' native language and/or multiple languages?

Yes	
No	**x**

Appropriateness of the training tool. Tool can be used for:

VG: very good, **G**: good, **NA**: not appropriate	**VG**	**G**	**NA**
Commercial seminar (up to 2 days)			
Commercial course (up to 2 months)			
Academic Lab (accompanying cybersecurity course) / Academic course	**x**		
Cybersecurity exercise /cyber range	**x**		
Cybersecurity hackathon	**x**		
Cybersecurity game			
Certification cybersecurity course	**x**		
Specific Cybersecurity Topic(s)	**x**		
Network security control	**x**		
Penetration testing	**x**		
Incident response			
Cloud security			
Risk management	**x**		

Forensics			
Other – write which one			

4.2.4 Snort

Filled by	Cristina Alcaraz
Organization	University of Malaga
Date	18-05-2023
Contact	alcaraz@uma.es
License	O: open
Cost of license	Not applicable
Available link to download tool	https://www.snort.org/downloads
Online manual(s)	https://www.snort.org/documents
Online tutorial(s)	https://www.snort.org/resources

Description

Summary

Guidelines:

Snort is an open-source sniffer and an intrusion detection/prevention system (IDS/IPS) composed of predefined. The tool uses a rule-based language combining attack signatures and inspection methods to detect malicious activities such a denial of service, buffer overflow, scanning or infection. Its operation is simple: (i) it receives network traffic; (ii) analyzes it according to a set of rules (acting as a filter); and (iii) and generates intuitive alerts so that IT/OT administrators or other related monitoring service can be able to interpret the situation and act accordingly. Any analyzed and produced data is logged in binary format with the possibility to export the information to other formats.

Its deployment can be in either a host-based IDS (HIDS - installed on a host) or a network-based IDS (NIDS - installed somewhere on the network). Depending on their use, the monitoring measures vary, e.g. NIDSs observe traffic (for TCP, UDP, ICMP) and its data (IP, MAC, etc.), while HIDSs analyze the incoming and outgoing data of a system. All this information is processed by a set of predefined and updated rules capable of deriving, recording and/or alerting of a situation.

All these functions are thanks to three operation modes: (i) Sniffer mode to capture network traffic using the library libpcap (for UNIX/Linux) or winpcap (for Windows); (ii) Packet Logger mode to log any activity or event in binary format with the possibility to export such an information to other formats; and (iii) NIDS mode in itself to apply the Snort rules. These rules must be configured in command in-line and under a configuration file – normally they are saved in specific locations, e.g., in Linux is at */etc/snort/snort.conf*. This file includes information about: Specific network variables such as the network from which Snort must analyze the packets ($HOME_NET / $EXTERNAL_NET); the location of the rules to be applied; the display mode, either via tcpdump, log files and their locations, terminal; and the execution and listening mode.

The structure of a rule is composed of a rule header (adding the compulsory parameters) and a rule option (containing optional parameters of alert), such that:

Rule header:

Action: alert, log, …

Protocol: tcp, icmp, udp.

Source IP/netmask and port.

Destination IP/netmask and port.

Direction: , or <>.

Rule option:

Alert message.

ID of the rule.

Content match.

Size of the payload.

Flags: F (FIN), S (SYN), R (RST), A (ACK)…

Etc.

For example:

```
alert udp any any -> 10.0.1.0/24 any (msg: "hello, it is an alert."; sid:3000231;) #alert about the situation
```

```
log tcp any any -> any 6000:6010 (msg: “hello, it is a new log.”; sid: 3000232;) #alert and log about the situation
```

Therefore, the main learning objective of this tool is to understand: (i) how monitoring systems can detect irregular actions in a particular network by “observing” its traffic, and (i) how such systems are able to alert and/or log for further action. In terms of KAs, Snort could thus cover those areas that require a constant monitoring of a network, involving detection and security of distributed systems, but also those where it is possible to establish secure communication among nodes, such as cloud or cyber-physical systems.

Assessment

The training tool has been used for

Commercial seminar (up to 2 days)	
Commercial course (up to 2 months)	
Academic Lab (accompanying cybersecurity course) / Academic course	**X**
Cybersecurity exercise /cyber range	
Cybersecurity hackathon	
Cybersecurity game	
Certification cybersecurity course	
Specific Cybersecurity Topic(s)	
Network security control	**X**
Penetration testing	
Incident response	
Cloud security	
Risk management	
Forensics	
Other – write which one	
Demonstration /training to Customer	
Pilot training operation	

Other (explain in free text):	

*If “**Other**”, then respond in free text.*

Not specified

Is this training tool suitable for training purposes (reach the learning objectives and knowledge areas)

Yes	**X**
No	

Are there any needed compute resources (CPUs, GPU, RAM, Disk space)?

Yes	
No	**X**

*If “**Yes**”, then respond in free text.*

What is the level of difficulty to use the training tool?

Easy	
Normal	
Medium/Standard/Average	
Intermediate	**X**
Hard/Expert/difficult	

Is this training tool easily adaptable to a specific training program?

Potential	
Most likely	X
Neither likely or unlikely	
Least likely	

Is this training tool easily implementable for a specific training program?

Not implementable	
Implementable with minor issues (inconsistencies)	X
Implementable with major issues (inconsistencies)	
Implementable	

Is this training tool easily scalable for a specific training program?

Not scalable	
Scalable with minor issues (inconsistencies)	
Scalable with major issues (inconsistencies)	
Scalable	X

Does this training tool cover interoperability aspects of a specific training program?

Not interoperable	
Interoperable with minor issues (inconsistencies)	**X**
Interoperable with major issues (inconsistencies)	
Interoperable	

Is this training tool stable while used in a specific training program?

Not stable	
Stable with minor issues (inconsistencies)	X
Stable with major issues (inconsistencies)	
Stable	

Does this training tool support the user's (trainer, trainee) privacy and security aspects?

Yes.	
No	**X**
Other	

*If "**Other**", then respond in free text*

What is the level of prior knowledge needed to use the training tool?

Knowledge of terms	
Knowledge of meanings	**X**
Integration of knowledge	**X**
Application of knowledge	**X**

Do the trainers/trainees find the training tool easy to use?

Yes	**X**
No	

Does this training tool support the trainers/trainees’ native language and/or multiple languages?

Yes	
No	**X**

Appropriateness of the training tool. Tool can be used for:

VG: very good, **G**: good, **NA**: not appropriate	**VG**	**G**	**NA**
Commercial seminar (up to 2 days)			**X**
Commercial course (up to 2 months)			**X**
Academic Lab (accompanying cybersecurity course) / Academic course	**X**		
Cybersecurity exercise /cyber range		**X**	
Cybersecurity hackathon			**X**
Cybersecurity game			**X**
Certification cybersecurity course		**X**	
Specific Cybersecurity Topic(s)			
Network security control	**X**		
Penetration testing			**X**
Incident response		**X**	
Cloud security		**X**	
Risk management			**X**
Forensics		**X**	
Other – write which one			

4.2.5 XCA

Filled by	Cristina Alcaraz
Organization	University of Malaga
Date	17-05-2023
Contact	alcaraz@uma.es
License	O: open
Cost of license	Not applicable
Available link to download tool	https://hohnstaedt.de/xca/index.php/download
Online manual(s)	https://hohnstaedt.de/xca/index.php/documentation/manual
Online tutorial(s)	https://hohnstaedt.de/xca/

Description

Summary

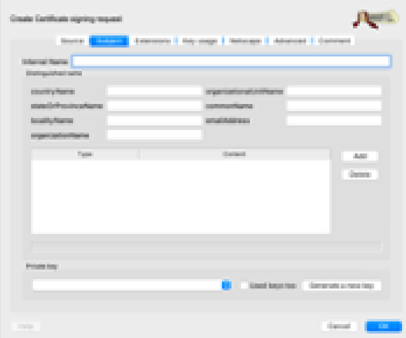
Guidelines:

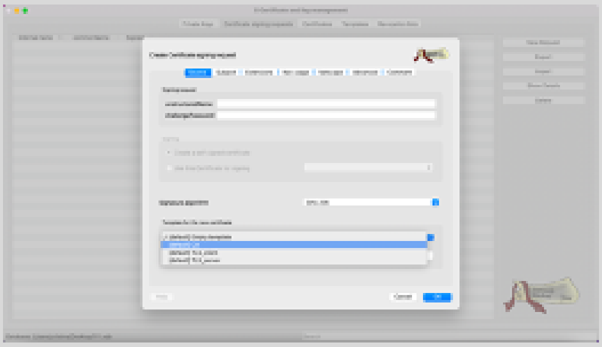
XCA / X, Certificate and Key management, is an open-source tool capable of creating and managing X.509 certificates, allowing students to understand the role of Certificate Authority (CA) entities and their operations, as well as the role of end users requesting digital certificates.

Basically, the tool has a simple graphical interface to manage the user's private keys (with an integrated database protected with a username and password) and the data corresponding to an X.509 type certificate. In this process, students must understand how to generate X.509 certificates and their associated parameters (e.g., subject information such as private key, country, organization name, common name, email address, etc. - represented in the first figure), and how to request the CA to certify it by means of a digital signature.

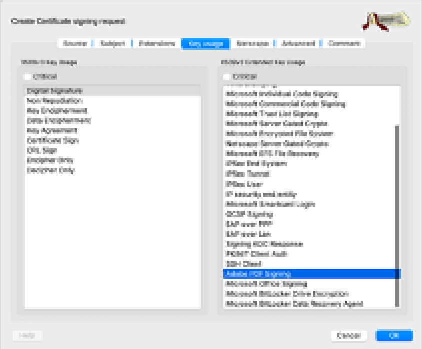
For this purpose, XCA has seven tabs (represented in the second figure), of which we highlight:

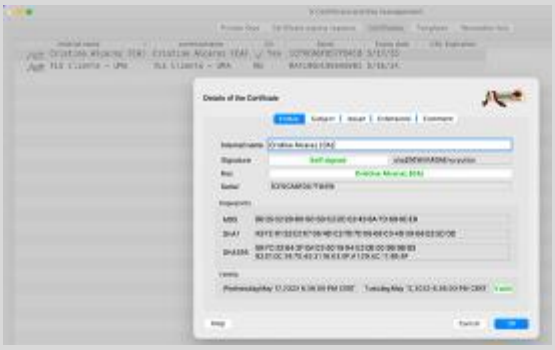
Source to generate the template, either for a CA or a TLS client or server; Subject with information related to the certificate; Extensions to indicate the type of entity (CA or end user), the validity of the certificate and the activation of the OCSP protocol; Key Usage to indicate the operations of the certificate, e.g. for signing PDF documents, as also illustrated in the third figure; Netscape to highlight its final use in the browser; and Advanced to give an overview of the final information of the certificate, as also illustrated in the fourth figure.

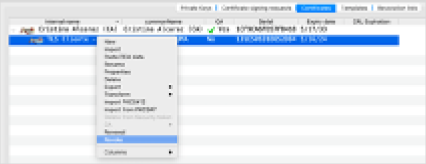


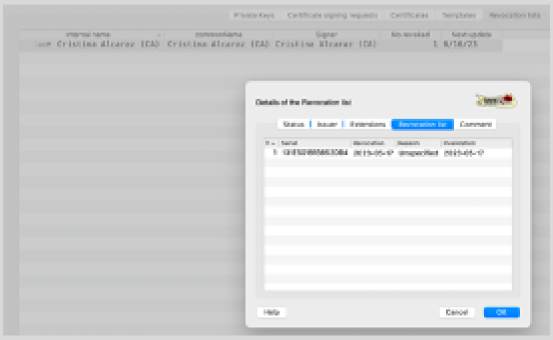


On the CA side, the CA can manage Certificate Signing Requests (CSR), sign a user's certificate or revoke it due to a specific compromised reason. This can be seen in the fifth and sixth figure. Likewise, the tool offers various certificate formats (DER, PEM) and standards (PKCS#1,7,8,10,11,12), offering several templates for common subjects (CA, TLS server and TLS client) and extensions.









Thus, the learning objectives of this tool aim to clarify the main functions of a CA, how to create and use X.509 certificates, and to understand their main parameters, operations and formats. As, in addition, its application promotes the creation of certificates for distributed communication scenarios -following the traditional client-server model-, XCA covers some KAs such as those related to distributed systems security and assess network security (e.g., in cloud or cyber-physical systems). However, its application can also be extended to promote the understanding of those distributed cryptographic protocols where authentication is required.

Trainees do need to have prior knowledge of public key cryptography, and it involves knowing how to apply private and public keys, and their main operations depending on the type of key. Finally, trainees will enhance their network management skills, as well as their soft skills (social, communication and interaction skills) if activities are scheduled to be carried out in groups, where some act as CA and others as end users.

Assessment

The training tool has been used for

Commercial seminar (up to 2 days)	
Commercial course (up to 2 months)	
Academic Lab (accompanying cybersecurity course) / Academic course	**X**
Cybersecurity exercise /cyber range	
Cybersecurity hackathon	
Cybersecurity game	
Certification cybersecurity course	
Specific Cybersecurity Topic(s)	
Network security control	**X**
Penetration testing	
Incident response	
Cloud security	

Risk management	
Forensics	
Other – write which one	
Demonstration /training to Customer	
Pilot training operation	
Other – Cryptography (advanced distributed protocols) and authentication	**X**

*If "**Other**", then respond in free text.*

Cryptography (advanced distributed protocols) and authentication

Is this training tool suitable for training purposes (reach the learning objectives and knowledge areas)

Yes	**X**
No	

Are there any needed compute resources (CPUs, GPU, RAM, Disk space)?

Yes	
No	**X**

*If "**Yes**", then respond in free text.*

What is the level of difficulty to use the training tool?

Easy	**X**

Normal	
Medium/Standard/Average	
Intermediate	
Hard/Expert/difficult	

Is this training tool easily adaptable to a specific training program?

Potential	X
Most likely	
Neither likely or unlikely	
Least likely	

Is this training tool easily implementable for a specific training program?

Not implementable	
Implementable with minor issues (inconsistencies)	
Implementable with major issues (inconsistencies)	
Implementable	X

Is this training tool easily scalable for a specific training program?

Not scalable	

Scalable with minor issues (inconsistencies)	
Scalable with major issues (inconsistencies)	
Scalable	**X**

Does this training tool cover interoperability aspects of a specific training program?

Not interoperable	
Interoperable with minor issues (inconsistencies)	**X**
Interoperable with major issues (inconsistencies)	
Interoperable	

Is this training tool stable while used in a specific training program?

Not stable	
Stable with minor issues (inconsistencies)	X
Stable with major issues (inconsistencies)	
Stable	

Does this training tool support the user's (trainer, trainee) privacy and security aspects?

Yes.	**X**
No	
Other	

*If "**Other**", then respond in free text*

What is the level of prior knowledge needed to use the training tool?

Knowledge of terms	**X**
Knowledge of meanings	**X**
Integration of knowledge	**X**
Application of knowledge	

Do the trainers/trainees find the training tool easy to use?

Yes	**X**
No	

Does this training tool support the trainers/trainees' native language and/or multiple languages?

Yes	**X**
No	

Appropriateness of the training tool. Tool can be used for:

VG: very good, **G**: good, **NA**: not appropriate	**VG**	**G**	**NA**
Commercial seminar (up to 2 days)			**X**
Commercial course (up to 2 months)			**X**
Academic Lab (accompanying cybersecurity course) / Academic course	**X**		
Cybersecurity exercise /cyber range			**X**
Cybersecurity hackathon			**X**
Cybersecurity game			**X**
Certification cybersecurity course		**X**	
Specific Cybersecurity Topic(s)			
Network security control	**X**		
Penetration testing			**X**
Incident response			**X**
Cloud security		**X**	
Risk management			**X**
Forensics			**X**
Other – Cryptography (advanced distributed protocols) and authentication	**X**		

4.2.6 OpenVAS

Filled by	Javier Lopez
Organization	University of Malaga
Date	19-05-2023
Contact	javierlopez@uma.es
License	O: open
Cost of license	Not applicable
Available link to download tool	https://github.com/greenbone/openvas-scanner
Online manual(s)	https://www.greenbone.net/en/documents/
Online tutorial(s)	--

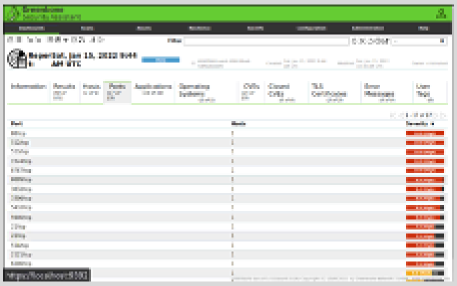
Description

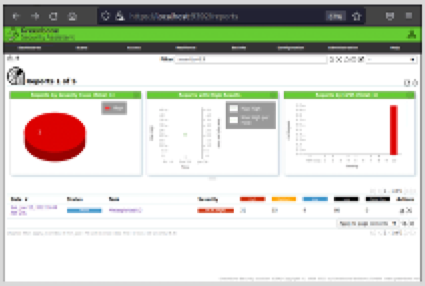
Summary

Guidelines:

Greenbone OpenVAS (Open Vulnerability Assessment System) or Greenbone Vulnerability Management (GVM), is a server-based network security scanner with a set of network vulnerability tests to detect security breaches in remote systems, and more specifically in operating system ports/services and protocols such as TLS. In fact, these tests can be launched after a client-server communication, where the client machine tracks the possible vulnerabilities presented by a given server node. Note that each vulnerability shown is labelled according to the common CVE-XXX-AAAA format, corresponding to common vulnerabilities and exposures.

Although its installation can be cumbersome, as it requires working at the command line, its graphical interface is quite intuitive. End users can verify for each test performed which services or applications present a certain level of severity, representing this information by means of color-coded indicators and various statistical graphs, as shown in the following two figures. Likewise, each reported vulnerability has linked mitigation guidelines to reduce the severity level on the node, and is associated with the ports or the services tested.





Its application allows students to understand: (i) the main functions of a pentester; (ii) how to perform multiple tests (authenticated and unauthenticated), connecting to various types of network elements, such as PC devices or routers; and (i) how to interpret potential risks by identifying vulnerabilities and severity levels. In terms of KAs, OpenVAS could cover, for example, auditing of the security and performance of the software, security of distributed systems, such as cloud systems or cyber-physical systems.

Assessment

The training tool has been used for

Commercial seminar (up to 2 days)	
Commercial course (up to 2 months)	
Academic Lab (accompanying cybersecurity course) / Academic course	**X**
Cybersecurity exercise /cyber range	
Cybersecurity hackathon	
Cybersecurity game	
Certification cybersecurity course	
Specific Cybersecurity Topic(s)	
Network security control	
Penetration testing	**X**

Incident response	
Cloud security	
Risk management	
Forensics	
Other – write which one	
Demonstration /training to Customer	
Pilot training operation	
Other (explain in free text):	

*If "**Other**", then respond in free text.*

Is this training tool suitable for training purposes (reach the learning objectives and knowledge areas)

Yes	**X**
No	

Are there any needed compute resources (CPUs, GPU, RAM, Disk space)?

Yes	**X (*)**
No	

*If "**Yes**" then respond in free text.*

(*) consumption depends on where OpenVAS is installed. For example, if it is installed in an emulated environment such as GNS3, the consumption is high.

What is the level of difficulty to use the training tool?

Easy	
Normal	
Medium/Standard/Average	
Intermediate	
Hard/Expert/difficult	**X**

Is this training tool easily adaptable to a specific training program?

Potential	
Most likely	
Neither likely or unlikely	**X**
Least likely	

Is this training tool easily implementable for a specific training program?

Not implementable	
Implementable with minor issues (inconsistencies)	
Implementable with major issues (inconsistencies)	**X**
Implementable	

Is this training tool easily scalable for a specific training program?

Not scalable	
Scalable with minor issues (inconsistencies)	**X**
Scalable with major issues (inconsistencies)	
Scalable	

Does this training tool cover interoperability aspects of a specific training program?

Not interoperable	
Interoperable with minor issues (inconsistencies)	
Interoperable with major issues (inconsistencies)	**X**
Interoperable	

Is this training tool stable while used in a specific training program?

Not stable	
Stable with minor issues (inconsistencies)	
Stable with major issues (inconsistencies)	X
Stable	

Does this training tool support the user's (trainer, trainee) privacy and security aspects?

Yes (the tools includes a access control panel based on a username and password)	**X**
No	
Other	

*If "**Other**", then respond in free text*

What is the level of prior knowledge needed to use the training tool?

Knowledge of terms	
Knowledge of meanings	
Integration of knowledge	**X**
Application of knowledge	**X**

Do the trainers/trainees find the training tool easy to use?

Yes	
No	**X**

Does this training tool support the trainers/trainees’ native language and/or multiple languages?

Yes	
No (mainly English)	**X**

Appropriateness of the training tool. Tool can be used for:

VG: very good, **G**: good, **NA**: not appropriate	**VG**	**G**	**NA**
Commercial seminar (up to 2 days)			**X**
Commercial course (up to 2 months)			**X**
Academic Lab (accompanying cybersecurity course) / Academic course	**X**		
Cybersecurity exercise /cyber range		**X**	
Cybersecurity hackathon			**X**
Cybersecurity game			**X**
Certification cybersecurity course	**X**		
Specific Cybersecurity Topic(s)			
Network security control		**X**	
Penetration testing	**X**		
Incident response			**X**
Cloud security		**X**	
Risk management		**X**	
Forensics			**X**
Other – write which one			

4.2.7 IPTables

Filled by	Cristina Alcaraz
Organization	University of Malaga
Date	18-05-2023
Contact	alcaraz@uma.es
License	O: open
Cost of license	Not applicable
Available link to download tool	Integrated in Linux distributions
Online manual(s)	https://man7.org/linux/man-pages/man8/iptables.8.html
Online tutorial(s)	-

Description

Summary

Guidelines:

IPTables consists of a firewall built into the Linux kernel, capable of filtering IPv4 and IPv6 packets and for different types of protocols, whether TCP, UDP or ICMP. Filtering is performed by applying a set of firewall rules, which can be inserted and maintained in separate tables (filter, nat, mangle, raw, and security), each of them maintaining specific strings by which the firewall rules are defined.

The most common tables for teaching are precisely the tables filter and nat. The former manages the INPUT (for packets entering the firewall), FORWARD (for packets crossing the firewall) and OUTPUT (for outgoing packets to the firewall) chains. The table nat, on the other hand, manages packets going to and from the Internet. In this case, students must handle rules that manage PREROUTING (Internet Intranet) and POSTROUTING (Intranet Internet), as well as NAT to perform the corresponding address translations.

In this translation process, an order of rules must be established. For example, for PREROUTING, the nat is applied first with the PREROUTING, and then the corresponding FORWARD/INPUT rule; whereas with POSTROUTING, the FORWARD/OUTPUT filtering rule is applied first, and then the POSTROUTING for masquerading with the nat. IPTables also controls the flags (SYN, SYN/ACK, ACK...) as it is considered a "stateful inspection" firewall. In this process, it checks both new connections, established connections, related connections, and even invalid connections.

In the learning process, students must show proficiency in the use of IPtables rules, but also of its commands and parameters. That is, their rules are built on generic specifications of the type: #iptables action <chain> -j <target>, such that:

Action: -A (adds a rule), -D (removes a rule), -R (replaces), etc. See the aforementioned manual.

Chain: INPUT, OUTPUT and FORWARD.

Target: the action to apply to the incoming, outgoing or routed packet, such as ACCEPT or DROP.

Apart from this, rules can contain a set of parameters. The most common ones for teaching are:

-p: protocol such as tcp, udp, icmp, esp, ah, among others.

-s and -d: source and origin of a packet.

-sport and -dport: source and ports.

-i and -o: incoming and outgoing network interface.

Some examples can be:

```
iptables -A INPUT -p tcp --dport 23 -j DROP
#Delete any incoming telnet traffic
 iptables -A OUTPUT -p tcp --dest 12.16.0.1 -j DROP
#Eliminate any outgoing traffic to IP 12.16.0.1
iptables -A FORWARD -i enp0s1 -o enp0s3 -m state –state NEW, ESTABLISHED, RELATED -j ACCEPT
iptables -t nat -A POSTROUTING -o enp0s1 -j MASQUERADE
#Control states and exit to an external network.
```

Therefore, the main learning objective of this tool is to understand: (i) how monitoring systems can detect irregular actions in a given network by "filtering" its traffic, and (i) how such systems are able to interrupt the sending or receiving of a packet as a preventive solution. In terms of KAs, IPtables could thus cover those specific areas of distributed systems security, but also those where it is possible to establish secure communication among diverse nodes (e.g., servers, routers), and also involving cloud or cyber-physical systems.

Assessment

The training tool has been used for

Commercial seminar (up to 2 days)	
Commercial course (up to 2 months)	
Academic Lab (accompanying cybersecurity course) / Academic course	**X**
Cybersecurity exercise /cyber range	
Cybersecurity hackathon	
Cybersecurity game	
Certification cybersecurity course	
Specific Cybersecurity Topic(s)	
Network security control	**X**
Penetration testing	
Incident response	
Cloud security	
Risk management	
Forensics	
Other – write which one	
Demonstration /training to Customer	
Pilot training operation	

Other (explain in free text):	

*If “**Other**”, then respond in free text.*

Is this training tool suitable for training purposes (reach the learning objectives and knowledge areas)

Yes	**X**
No	

Are there any needed compute resources (CPUs, GPU, RAM, Disk space)?

Yes	
No	**X**

*If “**Yes**”, then respond in free text.*

What is the level of difficulty to use the training tool?

Easy	
Normal	
Medium/Standard/Average	**X**
Intermediate	
Hard/Expert/difficult	

Is this training tool easily adaptable to a specific training program?

Potential	X
Most likely	
Neither likely or unlikely	
Least likely	

Is this training tool easily implementable for a specific training program?

Not implementable	
Implementable with minor issues (inconsistencies)	
Implementable with major issues (inconsistencies)	
Implementable	X

Is this training tool easily scalable for a specific training program?

Not scalable	
Scalable with minor issues (inconsistencies)	
Scalable with major issues (inconsistencies)	
Scalable	X

Does this training tool cover interoperability aspects of a specific training program?

Not interoperable	
Interoperable with minor issues (inconsistencies)	
Interoperable with major issues (inconsistencies) – it is only for Linux-based practical scenarios	**X**
Interoperable	

Is this training tool stable while used in a specific training program?

Not stable	
Stable with minor issues (inconsistencies)	
Stable with major issues (inconsistencies)	
Stable	

Does this training tool support the user's (trainer, trainee) privacy and security aspects?

Yes.	
No (it is a tool working in background)	**X**
Other	

*If "**Other**", then respond in free text*

What is the level of prior knowledge needed to use the training tool?

Knowledge of terms	
Knowledge of meanings	
Integration of knowledge	**X**
Application of knowledge	

Do the trainers/trainees find the training tool easy to use?

Yes	
No	**X**

Does this training tool support the trainers/trainees’ native language and/or multiple languages?

Yes	
No (mainly English)	**X**

Appropriateness of the training tool. Tool can be used for:

VG: very good, **G**: good, **NA**: not appropriate	**VG**	**G**	**NA**
Commercial seminar (up to 2 days)			**X**
Commercial course (up to 2 months)			**X**
Academic Lab (accompanying cybersecurity course) / Academic course	**X**		
Cybersecurity exercise /cyber range		**X**	
Cybersecurity hackathon		**X**	
Cybersecurity game			**X**
Certification cybersecurity course	**X**		
Specific Cybersecurity Topic(s)			
Network security control	**X**		
Penetration testing			**X**
Incident response		**X**	
Cloud security		**X**	
Risk management			**X**
Forensics			**X**
Other – write which one			

4.2.8 Kleopatra

Filled by	Antonio Muñoz
Organization	UMA
Date	19-05-2023
Contact	anto@uma.es
License	O
Cost of license	if not "O"
Available link to download tool	https://www.openpgp.org/software/kleopatra/
Online manual(s)	https://docs.kde.org/stable5/en/kleopatra/kleopatra/index.html
Online tutorial(s)	https://www.youtube.com/watch?v=H68y5EUSK8Q

Description

Summary
Guidelines: Kleopatra is a certificate manager and encryption tool that serves several purposes related to digital certificates and encryption: Kleopatra allows users to manage digital certificates, including importing, exporting, and viewing certificate details. It provides a user-friendly interface to handle tasks such as generating certificate requests, managing certificate stores, and verifying certificate chains. It also enables users to encrypt and decrypt files, emails, and messages using various encryption algorithms such as OpenPGP and S/MIME. It provides a graphical interface to easily perform encryption and decryption operations, ensuring data confidentiality. The tool supports creating and verifying digital signatures using OpenPGP and X.509 certificates. Users can sign documents and emails to ensure their authenticity and integrity, allowing recipients to verify the origin and integrity of the signed content. Kleopatra also facilitates the management of cryptographic keys, including generating key pairs, importing and exporting keys, and securely storing private keys. It helps users maintain control over their encryption keys and ensures proper key handling.

The tool allows users to interact with CAs by submitting certificate signing requests and managing the trust anchors, including trusted root certificates and certificate revocation lists (CRLs).

Kleopatra also integrates with keyserver networks, enabling users to search for and retrieve public keys associated with specific email addresses or identities. This simplifies the process of exchanging encrypted messages with others.

Lastly, the tool is designed to provide a user-friendly interface for managing certificates, keys, and encryption-related tasks. It is commonly used in conjunction with other encryption tools and technologies to enhance privacy and security in digital communications.

Assessment

The training tool has been used for

Commercial seminar (up to 2 days)	
Commercial course (up to 2 months)	
Academic Lab (accompanying cybersecurity course) / Academic course	**X**
Cybersecurity exercise /cyber range	
Cybersecurity hackathon	
Cybersecurity game	
Certification cybersecurity course	
Specific Cybersecurity Topic(s)	
Network security control	**X**
Penetration testing	
Incident response	
Cloud security	

Risk management	
Forensics	
Other – write which one	
Demonstration /training to Customer	
Pilot training operation	
Other (explain in free text):	

*If "**Other**", then respond in free text.*

Is this training tool suitable for training purposes (reach the learning objectives and knowledge areas)

Yes	**X**
No	

Are there any needed compute resources (CPUs, GPU, RAM, Disk space)?

Yes	
No	**X**

*If "**Yes**", then respond in free text.*

What is the level of difficulty to use the training tool?

Easy	**X**
Normal	
Medium/Standard/Average	
Intermediate	
Hard/Expert/difficult	

Is this training tool easily adaptable to a specific training program?

Potential	
Most likely	**X**
Neither likely or unlikely	
Least likely	

Is this training tool easily implementable for a specific training program?

Not implementable	
Implementable with minor issues (inconsistencies)	
Implementable with major issues (inconsistencies)	
Implementable	**X**

Is this training tool easily scalable for a specific training program?

Not scalable	
Scalable with minor issues (inconsistencies)	**X**
Scalable with major issues (inconsistencies)	
Scalable	

Does this training tool cover interoperability aspects of a specific training program?

Not interoperable	
Interoperable with minor issues (inconsistencies)	
Interoperable with major issues (inconsistencies)	
Interoperable	

Is this training tool stable while used in a specific training program?

Not stable	
Stable with minor issues (inconsistencies)	**X**
Stable with major issues (inconsistencies)	
Stable	

Does this training tool support the user's (trainer, trainee) privacy and security aspects?

Yes.	**X**
No	
Other	

*If "**Other**", then respond in free text*

What is the level of prior knowledge needed to use the training tool?

Knowledge of terms	
Knowledge of meanings	
Integration of knowledge	**X**
Application of knowledge	

Do the trainers/trainees find the training tool easy to use?

Yes	**X**
No	

Does this training tool support the trainers/trainees' native language and/or multiple languages?

Yes	**X**
No	

Appropriateness of the training tool. Tool can be used for:

VG: very good, **G**: good, **NA**: not appropriate	**VG**	**G**	**NA**
Commercial seminar (up to 2 days)			**X**
Commercial course (up to 2 months)			**X**
Academic Lab (accompanying cybersecurity course) / Academic course	**X**		
Cybersecurity exercise /cyber range		**X**	
Cybersecurity hackathon		**X**	
Cybersecurity game	**X**		
Certification cybersecurity course		**X**	
Specific Cybersecurity Topic(s)			
Network security control		**X**	
Penetration testing			**X**
Incident response			**X**
Cloud security			**X**
Risk management			**X**
Forensics			**X**
Other – write which one			

4.2.9 Sonarqube

Filled by	José Antonio Montenegro Montes
Organization	Universidad de Málaga
Date	19-05-2023
Contact	jmmontes@uma.es
License	O: open
Cost of license	Not applicable
Available link to download tool	https://www.sonarsource.com/products/sonarqube/downloads/
Online manual(s)	https://docs.sonarqube.org/latest/
Online tutorial(s)	https://docs.sonarqube.org/latest/

Description

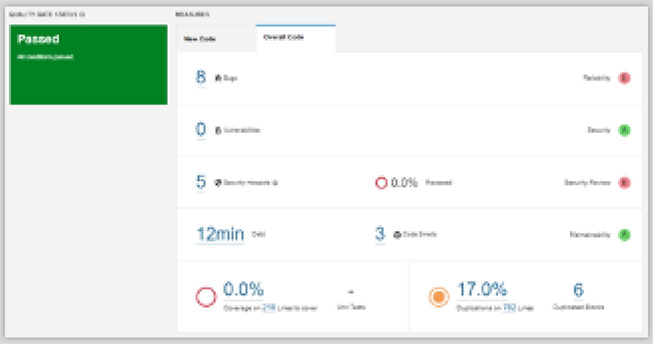
Summary

Guidelines:

SonarQube is a self-managed, automatic code review tool that systematically helps you deliver clean code. Clean code is defined as code that meets a certain defined standard, i.e. code that is reliable, secure, maintainable, readable, and modular, in addition to having other key attributes. In our case, we are primarily focused on finding vulnerabilities and security advisories in the code.

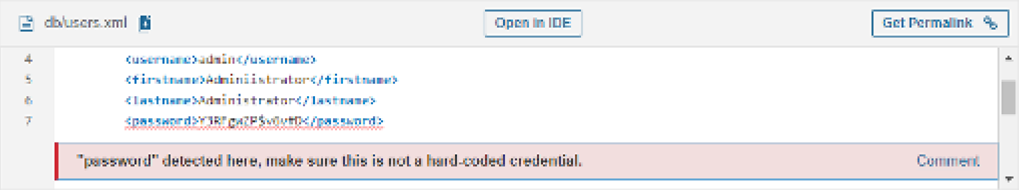
The main objective of the practice is to provide trainees with a hands-on experience that showcases the advantages and drawbacks of static code analysis tools. The tool has been specifically used in the course to identify web application vulnerabilities. Trainees either create or utilize a vulnerable web application and run the tool against the site to discover any vulnerabilities. Based on the information obtained from SonarQube, a non-vulnerable web application is then created.

In the following example the SonarQue tool has been used with the application *Damn Simple Vulnerable Python Web Application, available in the repository:* https://github.com/sgabe/DSVPWA. The interface presents a graphical format that displays 8 bugs and 5 security hotspots that have been identified.



From the 13 cases found, we are going to describe two specific cases:

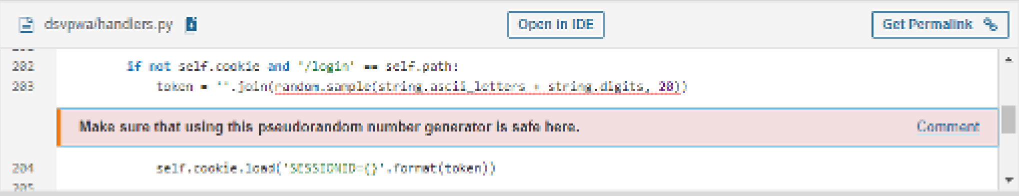
1. "password" detected here, make sure this is not a hard-coded credential:



```
        <username>admin</username>
        <firstname>Administrator</firstname>
        <lastname>Administrator</lastname>
        <password>Y3RfgxZP$v0vfD</password>
```

"password" detected here, make sure this is not a hard-coded credential.

2. Make sure that using this pseudorandom number generator is safe here:



```
        if not self.cookie and '/login' == self.path:
            token = ''.join(random.sample(string.ascii_letters + string.digits, 28))
```

Make sure that using this pseudorandom number generator is safe here.

```
            self.cookie.load('SESSIONID={}'.format(token))
```

The tool shows hints detected in a very descriptive form and provides code localization. Moreover, the tool can be integrated with the most commonly used IDE, facilitating the resolution of vulnerabilities in the code for the programmer.

Assessment

The training tool has been used for

Commercial seminar (up to 2 days)	
Commercial course (up to 2 months)	
Academic Lab (accompanying cybersecurity course) / Academic course	X
Cybersecurity exercise /cyber range	
Cybersecurity hackathon	

Cybersecurity game	
Certification cybersecurity course	
Specific Cybersecurity Topic(s)	
Network security control	
Penetration testing	**X**
Incident response	
Cloud security	
Risk management	
Forensics	
Other – vulnerability check	**X**

*If “**Other**”, then respond in free text.*

Vulnerability check

Is this training tool suitable for training purposes (reach the learning objectives and knowledge areas)

Yes	**X**
No	

Are there any needed compute resources (CPUs, GPU, RAM, Disk space)?

Yes	
No	**X**

*If "**Yes**", then respond in free text.*

What is the level of difficulty to use the training tool?

Easy	
Normal	**X**
Medium/Standard/Average	
Intermediate	
Hard/Expert/difficult	

Is this training tool easily adaptable to a specific training program?

Potential	**X**
Most likely	
Neither likely or unlikely	
Least likely	

Is this training tool easily implementable for a specific training program?

Not implementable	
Implementable with minor issues (inconsistencies)	
Implementable with major issues (inconsistencies)	
Implementable	**X**

Is this training tool easily scalable for a specific training program?

Not scalable	
Scalable with minor issues (inconsistencies)	
Scalable with major issues (inconsistencies)	
Scalable	**X**

Does this training tool cover interoperability aspects of a specific training program?

Not interoperable	
Interoperable with minor issues (inconsistencies)	
Interoperable with major issues (inconsistencies)	
Interoperable	**X**

Is this training tool stable while used in a specific training program?

Not stable	
Stable with minor issues (inconsistencies)	
Stable with major issues (inconsistencies)	
Stable	**X**

Does this training tool support the user's (trainer, trainee) privacy and security aspects?

Yes.	**X**
No	
Other	

*If "**Other**", then respond in free text*

What is the level of prior knowledge needed to use the training tool?

Knowledge of terms	
Knowledge of meanings	
Integration of knowledge	
Application of knowledge	**X**

Do the trainers/trainees find the training tool easy to use?

Yes	**X**
No	

Does this training tool support the trainers/trainees' native language and/or multiple languages?

Yes	
No	**X**

Appropriateness of the training tool. Tool can be used for:

VG: very good, **G**: good, **NA**: not appropriate	**VG**	**G**	**NA**
Commercial seminar (up to 2 days)	**X**		
Commercial course (up to 2 months)		**X**	
Academic Lab (accompanying cybersecurity course) / Academic course	**X**		
Cybersecurity exercise /cyber range		**X**	
Cybersecurity hackathon		**X**	
Cybersecurity game		**X**	
Certification cybersecurity course		**X**	
Specific Cybersecurity Topic(s)			
Network security control			**X**

Penetration testing	**X**		
Incident response			**X**
Cloud security			**X**
Risk management			**X**
Forensics			**X**
Other – vulnerabilities code	**X**		

4.2.10 Digital Torc

Filled by	Per Håkon Meland
Organization	SINTEF
Date	16-07-2023
Contact	torc@sintef.no, per.h.meland@sintef.no
License	O, C
Cost of license	TBD
Available link to download tool	The tool is an online game found here: https://digital.torc.no/
Online manual(s)	https://documentation.torc.no/
Online tutorial(s)	https://www.youtube.com/watch?v=qwGuLfDYzJw

Description

Summary
Guidelines: Training for Operational Resilience (TORC) is a training-by-gaming approach based on a board-game setup. The TORC approach was developed between 2014 and 2016 under the Safera (ERA-NET) project, coordinated by SINTEF. TORC is designed to facilitate organizations and teams that seek to reveal, understand, articulate, demonstrate and/or develop their inherent repertoire of resilient performance in face of unexpected deviations, disturbances and shocks. The training outcomes and experiences are captured in a way that prepares them to be used as raw material of technological, human, organizational and managerial priorities and resources that are needed to transform the experience from the training exercise into effective resilience capabilities under a more formal managerial supervision. Digital TORC was first developed in the STOP-IT project as a way to play TORC when it was not possible to meet physically due to the COVID situation. The organized workshops were a success

and proved that the concept of the tool was good; not only because it allows to play digitally, but also because it collects training data in a systematic manner. Digital TORC was further developed for a workshop with the European Commission in June 2021, which led to great interest in the platform among the participants. Some of the participants wanted to use the tool to lead discussions at country level.

A second version of the platform, more generic (i.e., not only for the water domain), including the option to choose between a risk mitigation and operational resilience orientation, and enhanced with a game management application, was developed and ready in fall 2021.

Assessment

The training tool has been used for

Commercial seminar (up to 2 days)	**x**
Commercial course (up to 2 months)	
Academic Lab (accompanying cybersecurity course) / Academic course	
Cybersecurity exercise /cyber range	**x**
Cybersecurity hackathon	
Cybersecurity game	**x**
Certification cybersecurity course	
Specific Cybersecurity Topic(s)	
Network security control	
Penetration testing	
Incident response	

Cloud security	
Risk management	**x**
Forensics	
Other – write which one	**x Resilience**
Demonstration /training to Customer	
Pilot training operation	**x**
Other (explain in free text):	

*If "**Other**", then respond in free text.*

Is this training tool suitable for training purposes (reach the learning objectives and knowledge areas)

Yes	**x**
No	

Are there any needed compute resources (CPUs, GPU, RAM, Disk space)?

Yes	
No	**x**

*If "**Yes**", then respond in free text.*

What is the level of difficulty to use the training tool?

Easy	
Normal	**x**
Medium/Standard/Average	
Intermediate	
Hard/Expert/difficult	

Is this training tool easily adaptable to a specific training program?

Potential	
Most likely	x
Neither likely or unlikely	
Least likely	

Is this training tool easily implementable for a specific training program?

Not implementable	
Implementable with minor issues (inconsistencies)	
Implementable with major issues (inconsistencies)	
Implementable	x

Is this training tool easily scalable for a specific training program?

Not scalable	
Scalable with minor issues (inconsistencies)	
Scalable with major issues (inconsistencies)	
Scalable	**x**

Does this training tool cover interoperability aspects of a specific training program?

Not interoperable	
Interoperable with minor issues (inconsistencies)	
Interoperable with major issues (inconsistencies)	
Interoperable	**x**

Is this training tool stable while used in a specific training program?

Not stable	
Stable with minor issues (inconsistencies)	
Stable with major issues (inconsistencies)	
Stable	

Does this training tool support the user’s (trainer, trainee) privacy and security aspects?

Yes.	**x**
No	
Other	

*If “**Other**”, then respond in free text*

What is the level of prior knowledge needed to use the training tool?

Knowledge of terms	**x**
Knowledge of meanings	**x**
Integration of knowledge	
Application of knowledge	**x**

Do the trainers/trainees find the training tool easy to use?

Yes	
No	

Does this training tool support the trainers/trainees’ native language and/or multiple languages?

Yes	
No	**x**

Appropriateness of the training tool. Tool can be used for:

VG: very good, **G**: good, **NA**: not appropriate	**VG**	**G**	**NA**
Commercial seminar (up to 2 days)		**x**	
Commercial course (up to 2 months)			
Academic Lab (accompanying cybersecurity course) / Academic course			
Cybersecurity exercise /cyber range		**x**	
Cybersecurity hackathon			
Cybersecurity game	**x**		
Certification cybersecurity course			
Specific Cybersecurity Topic(s)			
Network security control			
Penetration testing			
Incident response	**x**		
Cloud security			

Risk management	**x**		
Forensics			
Other – write which one			

4.2.11 CAINE

Filled by	Panayiotis Kotzanikolaou - Dimitris Koutras
Organization	UPRC
Date	20-05-2023
Contact	pkotzani@unipi.gr – dkoutras@unipi.gr
License	O
Cost of license	-
Available link to download tool	https://www.caine-live.net/page5/page5.html
Online manual(s)	https://www.caine-live.net/page8/page8.html
Online tutorial(s)	https://www.youtube.com/watch?v=5S-oCypcyxc https://www.youtube.com/watch?v=FoEO9p-J15w

Description

Summary
Caine is a robust digital forensic toolkit designed specifically for computer forensic analysis. It provides a comprehensive suite of tools and utilities to assist in the investigation and examination of digital evidence. With an easy-to-use interface and pre-installed software, Caine facilitates the collection, the analysis, and the documentation of data from multiple sources, helping forensic investigators uncover critical information. Caine is based on the Ubuntu distribution and provides a user-friendly desktop environment. It includes a wide range of forensic tools for disk imaging, file recovery, and memory analysis. Caine supports virtual machine introspection for analyzing virtualized environments. It offers live analysis capabilities with volatile data capture and analysis.

Assessment

The training tool has been used for

Commercial seminar (up to 2 days)	
Commercial course (up to 2 months)	
Academic Lab (accompanying cybersecurity course) / Academic course	**X**
Cybersecurity exercise /cyber range	
Cybersecurity hackathon	
Cybersecurity game	
Certification cybersecurity course	
Specific Cybersecurity Topic(s)	
Network security control	
Penetration testing	
Incident response	
Cloud security	
Risk management	
Forensics	**X**
Other – write which one	
Demonstration /training to Customer	
Pilot training operation	

Other (explain in free text):	

*If “**Other**”, then respond in free text.*

Is this training tool suitable for training purposes (reach the learning objectives and knowledge areas)

Yes	**X**
No	

Are there any needed compute resources (CPUs, GPU, RAM, Disk space)?

Yes	
No	**X**

*If “**Yes**”, then respond in free text.*

What is the level of difficulty to use the training tool?

Easy	
Normal	
Medium/Standard/Average	**X**
Intermediate	
Hard/Expert/difficult	

Is this training tool easily adaptable to a specific training program?

Potential	
Most likely	X
Neither likely or unlikely	
Least likely	

Is this training tool easily implementable for a specific training program?

Not implementable	
Implementable with minor issues (inconsistencies)	X
Implementable with major issues (inconsistencies)	
Implementable	

Is this training tool easily scalable for a specific training program?

Not scalable	
Scalable with minor issues (inconsistencies)	X
Scalable with major issues (inconsistencies)	
Scalable	

Does this training tool cover interoperability aspects of a specific training program?

Not interoperable	
Interoperable with minor issues (inconsistencies)	**X**
Interoperable with major issues (inconsistencies)	
Interoperable	

Is this training tool stable while used in a specific training program?

Not stable	
Stable with minor issues (inconsistencies)	**X**
Stable with major issues (inconsistencies)	
Stable	

Does this training tool support the user’s (trainer, trainee) privacy and security aspects?

Yes.	**X**
No	
Other	

*If "**Other**", then respond in free text*

What is the level of prior knowledge needed to use the training tool?

Knowledge of terms	**X**
Knowledge of meanings	**X**
Integration of knowledge	
Application of knowledge	

Do the trainers/trainees find the training tool easy to use?

Yes	**X**
No	

Does this training tool support the trainers/trainees’ native language and/or multiple languages?

Yes	
No	**X**

Appropriateness of the training tool. Tool can be used for:

VG: very good, **G**: good, **NA**: not appropriate	**VG**	**G**	**NA**
Commercial seminar (up to 2 days)		**X**	
Commercial course (up to 2 months)			**X**
Academic Lab (accompanying cybersecurity course) / Academic course		**X**	
Cybersecurity exercise /cyber range		**X**	

Cybersecurity hackathon		**X**	
Cybersecurity game		**X**	
Certification cybersecurity course			**X**
Specific Cybersecurity Topic(s)			
Network security control			
Penetration testing			
Incident response			
Cloud security			
Risk management			
Forensics		**X**	
Other – write which one			

4.2.12 Volatility

Filled by	Panayiotis Kotzanikolaou - Dimitris Koutras
Organization	UPRC
Date	20-05-2023
Contact	pkotzani@unipi.gr – dkoutras@unipi.gr
License	O
Cost of license	-
Available link to download tool	https://www.volatilityfoundation.org/releases
Online manual(s)	https://downloads.volatilityfoundation.org/releases/2.4/CheatSheet_v2.4.pdf
Online tutorial(s)	https://www.youtube.com/watch?v=Uk3DEgY5Ue8&embeds_referring_euri=https%3A%2F%2Fwww.google.com%2F&source_ve_path=MjM4NTE&feature=emb_title

Description

Summary
Volatility is a widely used open-source memory forensics tool. It helps forensic analysts extract valuable information from volatile memory dumps of computer systems. By analyzing memory artefacts, Volatility can identify running processes, network connections and evidence of malicious activity. Its extensive set of plug-ins provides a versatile framework for in-depth memory analysis and incident response. Volatility supports memory forensics on Windows, Linux, and macOS operating systems. It provides a plugin architecture, allowing the addition of custom analysis modules. Volatility supports the extraction of artifacts like process memory, network connections, and registry keys from memory dumps. It can analyze hibernation files and virtual machine snapshots for memory analysis.

Assessment

The training tool has been used for

Commercial seminar (up to 2 days)	
Commercial course (up to 2 months)	
Academic Lab (accompanying cybersecurity course) / Academic course	**X**
Cybersecurity exercise /cyber range	
Cybersecurity hackathon	
Cybersecurity game	
Certification cybersecurity course	
Specific Cybersecurity Topic(s)	
Network security control	
Penetration testing	
Incident response	
Cloud security	
Risk management	
Forensics	**X**
Other – write which one	
Demonstration /training to Customer	
Pilot training operation	

Other (explain in free text):	

*If "**Other**", then respond in free text.*

Is this training tool suitable for training purposes (reach the learning objectives and knowledge areas)

Yes	**X**
No	

Are there any needed compute resources (CPUs, GPU, RAM, Disk space)?

Yes	
No	**X**

*If "**Yes**", then respond in free text.*

What is the level of difficulty to use the training tool?

Easy	
Normal	
Medium/Standard/Average	
Intermediate	**X**
Hard/Expert/difficult	

Is this training tool easily adaptable to a specific training program?

Potential	**X**
Most likely	
Neither likely or unlikely	
Least likely	

Is this training tool easily implementable for a specific training program?

Not implementable	
Implementable with minor issues (inconsistencies)	**X**
Implementable with major issues (inconsistencies)	
Implementable	

Is this training tool easily scalable for a specific training program?

Not scalable	
Scalable with minor issues (inconsistencies)	**X**
Scalable with major issues (inconsistencies)	
Scalable	

Does this training tool cover interoperability aspects of a specific training program?

Not interoperable	
Interoperable with minor issues (inconsistencies)	**X**
Interoperable with major issues (inconsistencies)	
Interoperable	

Is this training tool stable while used in a specific training program?

Not stable	
Stable with minor issues (inconsistencies)	**X**
Stable with major issues (inconsistencies)	
Stable	

Does this training tool support the user's (trainer, trainee) privacy and security aspects?

Yes.	**X**
No	
Other	

*If "**Other**", then respond in free text*

What is the level of prior knowledge needed to use the training tool?

Knowledge of terms	**X**
Knowledge of meanings	**X**
Integration of knowledge	
Application of knowledge	

Do the trainers/trainees find the training tool easy to use?

Yes	**X**
No	

Does this training tool support the trainers/trainees’ native language and/or multiple languages?

Yes	
No	**X**

Appropriateness of the training tool. Tool can be used for:

VG: very good, **G**: good, **NA**: not appropriate	**VG**	**G**	**NA**
Commercial seminar (up to 2 days)		**X**	
Commercial course (up to 2 months)			**X**
Academic Lab (accompanying cybersecurity course) / Academic course		**X**	
Cybersecurity exercise /cyber range		**X**	
Cybersecurity hackathon	**X**		

Cybersecurity game		**X**	
Certification cybersecurity course		**X**	
Specific Cybersecurity Topic(s)			
Network security control			
Penetration testing			
Incident response			
Cloud security			
Risk management			
Forensics		**X**	
Other – write which one			

4.2.13 Autopsy

Filled by	Rodrigo Roman[1], Panayiotis Kotzanikolaou[2], and Dimitris Koutras[2]
Organization	(1) University of Malaga (2) UPRC
Date	16-05-2023
Contact	(1) rroman@uma.es (2) pkotzani@unipi.gr, dkoutras@unipi.gr
License	O: open
Cost of license	---
Available link to download tool	https://www.autopsy.com/ https://www.sleuthkit.org/autopsy/
Online manual(s)	http://sleuthkit.org/autopsy/docs/user-docs/ https://www.sleuthkit.org/autopsy/docs.php
Online tutorial(s)	https://www.youtube.com/watch?v=fEqx0MeCCHg https://www.autopsy.com/category/blog/ https://www.youtube.com/watch?v=S6V66G2tVr8&pp=ygUHYXV0b3BzeQ%3D%3D

Description

Summary

Autopsy is a cross-platform graphical interface to various open-source forensic tools, such as “The Sleuth Kit” (https://sleuthkit.org/). Its main goal is to provide digital investigators with the necessary tools to analyze the contents of data sources, mainly disk images.

In other words, Autopsy is a feature-rich digital forensics platform that simplifies the analysis of computer systems and storage media. It provides a graphical user interface and a wide range of modules to automate and streamline forensic investigations. Autopsy supports file system analysis, keyword search, metadata extraction and artefact recovery, making it an invaluable tool for law enforcement and digital forensics professionals.

Autopsy is a digital forensic tool with a web-based graphical interface.

It supports file system analysis for various operating systems, including NTFS, FAT, and HFS+.

Autopsy includes modules for keyword searching, timeline analysis, and data carving.

It offers built-in support for analyzing mobile device images and email artifacts.

The key functionalities of Autopsy are as follows:

Basic Analysis Interface: Autopsy provides a simple interface to navigate the contents of a data source, such as various file systems (e.g., FAT, NTFS, HFS+, Ext2, Ext3, Ext4, UFS, ISO 9660 (CD/DVD)), and display various information about files, including their metadata, hexadecimal dump, and contents (e.g., image for image files)

Advanced Analysis Interface: Autopsy provide support for more advanced analysis interfaces, such as Timeline (provides a timeline of the events of the system), Communications (shows which accounts were communicated with the most), Geolocation (shows a map for all geolocation results found in the case), and Discovery (search for different types of data).

Plugin Architecture: Autopsy incorporates various “ingest” modules that analyze the data sources in the background and provide the results to the investigator. These modules provide various advanced mechanisms, including keyword search, email analysis, extension mismatch detection, encryption detection, and hash lookup (search for known files).

The cybersecurity knowledge areas related to this tool are mostly in the realm of data security, more specifically on the subject of digital forensics. By using this tool, students can achieve various specific learning objectives, such as i) acquisition of digital evidence, ii) performing forensic analysis of data sources, and iii) carrying out verification and validation of evidence during forensic analysis, including the use of hashes. All these objectives fall under the core competency of “Apply the principles of computer forensics to the extraction and analysis of digital evidence”.

In order to allow students to acquire such skills and competences, the tool can perform all the necessary tasks that are needed to analyze the content of data sources (from mere visualization to more detailed analyses), in order to uncover the necessary evidence for a particular case. As this tool is very simple to use (imitating the functionality of any OS file explorer), the learning process is quite fast. However, students must have a basic background on OS, file systems and computer forensics principles in order to effectively use the tool.

Assessment

The training tool has been used for

Commercial seminar (up to 2 days)	
Commercial course (up to 2 months)	
Academic Lab (accompanying cybersecurity course) / Academic course	**X**
Cybersecurity exercise /cyber range	
Cybersecurity hackathon	
Cybersecurity game	
Certification cybersecurity course	
Specific Cybersecurity Topic(s)	
Network security control	
Penetration testing	
Incident response	
Cloud security	
Risk management	
Forensics	**X**
Other – write which one	
Demonstration /training to Customer	
Pilot training operation	

Other (explain in free text):	

*If “**Other**”, then respond in free text.*

Is this training tool suitable for training purposes (reach the learning objectives and knowledge areas)

Yes	**X**
No	

Are there any needed compute resources (CPUs, GPU, RAM, Disk space)?

Yes	**X**
No	

*If “**Yes**”, then respond in free text.*

2GB Disk space is needed. For resource-constrained virtual machines (<8GB RAM), it is better to use versions 3.1.X. If virtual machines with plenty of resources (e.g. 8GB RAM or more) are used, it is possible to use the latest versions, although the options should be changed to add more memory to the Java Virtual Machine.

What is the level of difficulty to use the training tool?

Easy	
Normal	
Medium/Standard/Average	
Intermediate	**X**
Hard/Expert/difficult	

Is this training tool easily adaptable to a specific training program?

Potential	**X**
Most likely	
Neither likely or unlikely	
Least likely	

Is this training tool easily implementable for a specific training program?

Not implementable	
Implementable with minor issues (inconsistencies)	**X**
Implementable with major issues (inconsistencies)	
Implementable	

Is this training tool easily scalable for a specific training program?

Not scalable	
Scalable with minor issues (inconsistencies)	**X**
Scalable with major issues (inconsistencies)	
Scalable	

Does this training tool cover interoperability aspects of a specific training program?

Not interoperable	
Interoperable with minor issues (inconsistencies)	**X**
Interoperable with major issues (inconsistencies)	
Interoperable	

Is this training tool stable while used in a specific training program?

Not stable	
Stable with minor issues (inconsistencies)	
Stable with major issues (inconsistencies)	
Stable	**X**

Does this training tool support the user’s (trainer, trainee) privacy and security aspects?

Yes.	X
No	
Other	

*If "**Other**", then respond in free text*

What is the level of prior knowledge needed to use the training tool?

Knowledge of terms	X
Knowledge of meanings	X
Integration of knowledge	
Application of knowledge	X

Do the trainers/trainees find the training tool easy to use?

Yes	X
No	

Does this training tool support the trainers/trainees' native language and/or multiple languages?

Yes	
No	X

Appropriateness of the training tool. Tool can be used for:

VG: very good, **G**: good, **NA**: not appropriate	**VG**	**G**	**NA**
Commercial seminar (up to 2 days)			**X**
Commercial course (up to 2 months)		**X**	
Academic Lab (accompanying cybersecurity course) / Academic course	**X**		
Cybersecurity exercise /cyber range		**X**	
Cybersecurity hackathon		**X**	
Cybersecurity game			**X**
Certification cybersecurity course		**X**	
Specific Cybersecurity Topic(s)			
Network security control			**X**
Penetration testing			**X**
Incident response			**X**
Cloud security			**X**
Risk management			**X**
Forensics	**X**		
Other – write which one			**X**

4.2.14 Cuckoo sandbox

Filled by	Panayiotis Kotzanikolaou - Dimitris Koutras
Organization	UPRC
Date	20-05-2023
Contact	pkotzani@unipi.gr – dkoutras@unipi.gr
License	O
Cost of license	-
Available link to download tool	https://cuckoosandbox.org/download
Online manual(s)	https://cuckoo.sh/docs/
Online tutorial(s)	https://www.youtube.com/watch?v=V4z2tLRCuIY&pp=ygUXY3Vja29vIG1hbHdhcmUgYW5hbHlzaXM%3D

Description

Summary

Cuckoo Sandbox is an open-source automated malware analysis system. It allows security analysts to safely execute suspicious files and observe their behaviour in a controlled environment. Cuckoo Sandbox provides detailed reports on the actions performed by malware, including file modifications, network communications and system interactions. It helps to detect and understand malicious software and helps organizations to strengthen their defences.

Cuckoo Sandbox is an automated malware analysis system.

It provides an isolated environment for executing and observing malware behaviour.

Cuckoo Sandbox supports dynamic analysis, including network traffic capture and API monitoring.

It generates detailed reports with behaviour analysis, network activity, and system modifications caused by malware.

Assessment

The training tool has been used for

Commercial seminar (up to 2 days)	
Commercial course (up to 2 months)	
Academic Lab (accompanying cybersecurity course) / Academic course	**X**
Cybersecurity exercise /cyber range	
Cybersecurity hackathon	
Cybersecurity game	
Certification cybersecurity course	
Specific Cybersecurity Topic(s)	
Network security control	
Penetration testing	
Incident response	
Cloud security	
Risk management	
Forensics	
Other – write which one	**X**
Demonstration /training to Customer	
Pilot training operation	

Other (explain in free text):	

*If "**Other**", then respond in free text.*

Malware analysis

Is this training tool suitable for training purposes (reach the learning objectives and knowledge areas)

Yes	**X**
No	

Are there any needed compute resources (CPUs, GPU, RAM, Disk space)?

Yes	
No	**X**

*If "**Yes**", then respond in free text.*

What is the level of difficulty to use the training tool?

Easy	
Normal	
Medium/Standard/Average	
Intermediate	
Hard/Expert/difficult	**X**

Is this training tool easily adaptable to a specific training program?

Potential	**X**
Most likely	
Neither likely or unlikely	
Least likely	

Is this training tool easily implementable for a specific training program?

Not implementable	
Implementable with minor issues (inconsistencies)	**X**
Implementable with major issues (inconsistencies)	
Implementable	

Is this training tool easily scalable for a specific training program?

Not scalable	
Scalable with minor issues (inconsistencies)	**X**
Scalable with major issues (inconsistencies)	
Scalable	

Does this training tool cover interoperability aspects of a specific training program?

Not interoperable	
Interoperable with minor issues (inconsistencies)	
Interoperable with major issues (inconsistencies)	
Interoperable	

Is this training tool stable while used in a specific training program?

Not stable	
Stable with minor issues (inconsistencies)	**X**
Stable with major issues (inconsistencies)	
Stable	

Does this training tool support the user's (trainer, trainee) privacy and security aspects?

Yes.	**X**
No	
Other	

*If "**Other**", then respond in free text*

What is the level of prior knowledge needed to use the training tool?

Knowledge of terms	
Knowledge of meanings	**X**
Integration of knowledge	
Application of knowledge	**X**

Do the trainers/trainees find the training tool easy to use?

Yes	
No	**X**

Does this training tool support the trainers/trainees’ native language and/or multiple languages?

Yes	**X**
No	

Appropriateness of the training tool. Tool can be used for

VG: very good, **G**: good, **NA**: not appropriate	**VG**	**G**	**NA**
Commercial seminar (up to 2 days)		**X**	
Commercial course (up to 2 months)			**X**
Academic Lab (accompanying cybersecurity course) / Academic course		**X**	
Cybersecurity exercise /cyber range		**X**	

Cybersecurity hackathon		**X**	
Cybersecurity game			**X**
Certification cybersecurity course			**X**
Specific Cybersecurity Topic(s)			
Network security control			
Penetration testing			
Incident response			
Cloud security			
Risk management			
Forensics			
Other – Malware analysis	**X**		

4.2.15 IDA pro

Filled by	Jose A. Onieva[1] Panayiotis Kotzanikolaou[2] Dimitris Koutras[2]
Organization	(1) University of Malaga (2) UPRC
Date	14-05-2023
Contact	(1) onieva@uma.es (2) pkotzani@unipi.gr, dkoutras@unipi.gr
License	O, Educational, with limited functionality. A free version also available
Cost of license	Previous request
Available link to download tool	Per request https://hex-rays.com/ida-free/#download
Online manual(s)	Tool integrated manual and online: https://hex-rays.com/products/ida/support/idadoc/index.shtml https://hex-rays.com/documentation/
Online tutorial(s)	https://hex-rays.com/products/ida/support/tutorials/ https://www.youtube.com/watch?v=N_3AGB9Vf9E&list=PLKwUZp9HwWoDDBPvoapdbJ1rdofowT67z

Description

Summary
IDA Pro as a disassembler is capable of creating maps of their execution to show the binary instructions that are actually executed by the processor in a symbolic representation (assembly language). Advanced techniques have been implemented into IDA Pro so that it can generate

assembly language source code from machine-executable code and make this complex code more human-readable.

In other words, IDA Pro is a widely used and powerful disassembler and debugger for software reverse engineering. It enables researchers and security professionals to analyze binary files and understand their underlying code structure. With its advanced features and plug-ins, IDA Pro supports static analysis, dynamic debugging, and scriptable interactions, making it an essential tool for vulnerability researchers and software analysts.

IDA Pro is a widely used disassembler and debugger for software reverse engineering.

It supports multiple processor architectures, including x86, ARM, and MIPS.

IDA Pro offers advanced features like graph visualization, cross-references, and function analysis.

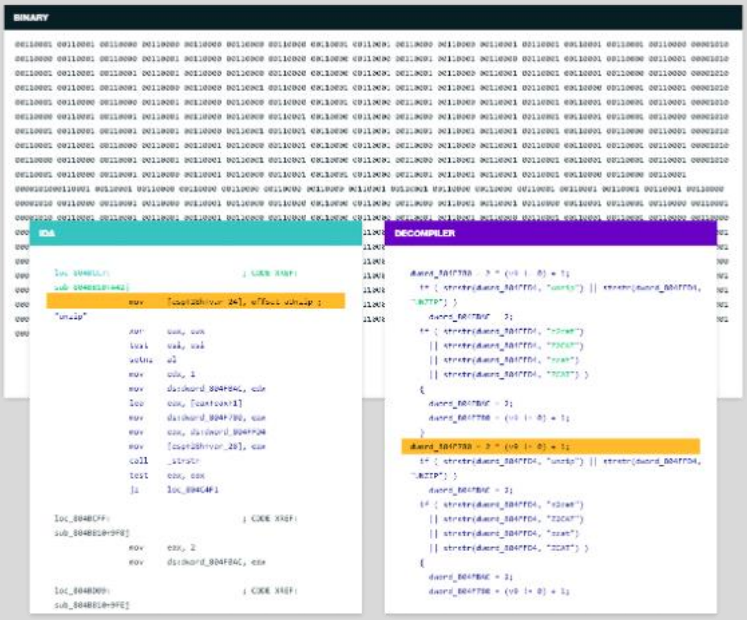
It provides a scripting interface for automation and custom analysis routines.

Moreover, the debugging feature augments IDA with the dynamic analysis. It supports multiple debugging targets and can handle remote applications. Its cross-platform debugging capability enables instant debugging, easy connection to both local and remote processes and support for 64-bit systems and new connection possibilities.

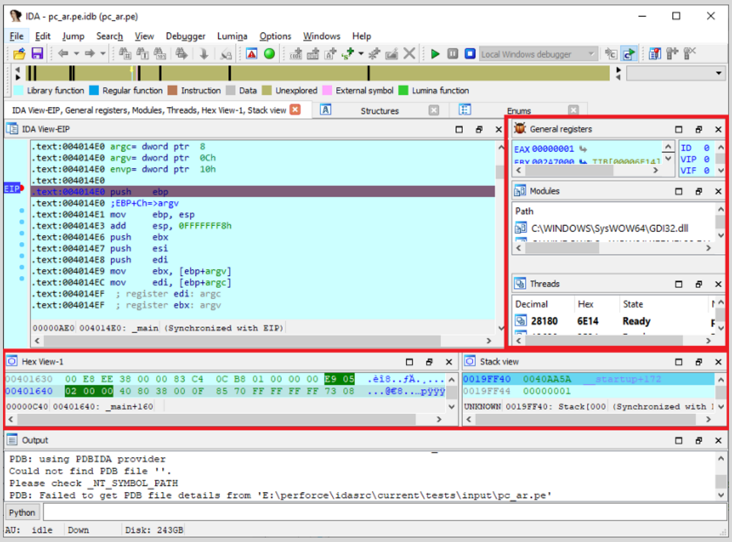
This tool is used for reverse engineering of malware samples. It is probably the de facto standard in the industry (together with NSA’s Ghidra) for reverse engineering purposes, providing the student the ability to study and practice reverse engineering. More specifically advanced static and dynamic analysis, allowing for the interpretation of malware code and following up and controlling its execution.

In order to take as much advantage as possible form this tool (and any other tool related with reverse engineering), the trainee needs to master basic concepts of the OS internals and target assembler language.

The following figures showing the process are from the Hex-Rays:



It integrates decompilers (with limited functionalityin in Educational version) disassemblers and debuggers.



```
.text:004014E0 argc= dword ptr  8
.text:004014E0 argv= dword ptr  0Ch
.text:004014E0 envp= dword ptr  10h
.text:004014E0
.text:004014E0 push    ebp
.text:004014E0 ;EBP+Ch=>argv
.text:004014E1 mov     ebp, esp
.text:004014E3 add     esp, 0FFFFFFF8h
.text:004014E6 push    ebx
.text:004014E7 push    esi
.text:004014E8 push    edi
.text:004014E9 mov     ebx, [ebp+argv]
.text:004014EC mov     edi, [ebp+argc]
.text:004014EF  ; register edi: argc
.text:004014EF  ; register ebx: argv

00000AE0 004014E0: _main (Synchronized with EIP)
```

```
EAX 00000001
EBX 00247000   TIB[00006E14]
ID  0
VIP 0
VIF 0
```

Path
C:\WINDOWS\SysWOW64\GDI32.dll

Decimal	Hex	State
28180	6E14	Ready

```
00401630  00 E8 EE 38 00 00 83 C4  0C B8 01 00 00 00 E9 05  .èî8..ƒÄ.,....
00401640  02 00 00 40 80 38 00 0F  85 70 FF FF FF FF 73 08  ...@€8...pÿÿÿ
00000C40 00401640: _main+160
```

```
0019FF40  0040AA5A  __startup+172
0019FF44  00000001
UNKNOWN 0019FF40: Stack[000 (Synchronized with
```

```
PDB: using PDBIDA provider
Could not find PDB file ''.
Please check _NT_SYMBOL_PATH
PDB: Failed to get PDB file details from 'E:\perforce\idasrc\current\tests\input\pc_ar.pe'
```

```
AU:  idle   Down    Disk: 243GB
```

Regarding the KAs, this tool is applied to cover the area “Malware & Attack Technologies & Human Behaviours”.

Assessment

The training tool has been used for

Commercial seminar (up to 2 days)	
Commercial course (up to 2 months)	
Academic Lab (accompanying cybersecurity course) / Academic course	X
Cybersecurity exercise /cyber range	
Cybersecurity hackathon	
Cybersecurity game	
Certification cybersecurity course	
Specific Cybersecurity Topic(s)	

Network security control	
Penetration testing	**X**
Incident response	
Cloud security	
Risk management	
Forensics	**X**
Other – Malware Analysis	**X**
Demonstration /training to Customer	
Pilot training operation	
Other (explain in free text):	

*If "**Other**", then respond in free text.*

Malware Analysis

Is this training tool suitable for training purposes (reach the learning objectives and knowledge areas)

Yes	**X**
No	

Are there any needed compute resources (CPUs, GPU, RAM, Disk space)?

Yes	
No	X

*If "**Yes**", then respond in free text.*

What is the level of difficulty to use the training tool?

Easy	
Normal	
Medium/Standard/Average	
Intermediate	X
Hard/Expert/difficult	X

Is this training tool easily adaptable to a specific training program?

Potential	
Most likely	
Neither likely or unlikely	X
Least likely	

Is this training tool easily implementable for a specific training program?

Not implementable	
Implementable with minor issues (inconsistencies)	**X**
Implementable with major issues (inconsistencies)	
Implementable	

Is this training tool easily scalable for a specific training program?

Not scalable	
Scalable with minor issues (inconsistencies)	**X**
Scalable with major issues (inconsistencies)	
Scalable	

Does this training tool cover interoperability aspects of a specific training program?

Not interoperable	
Interoperable with minor issues (inconsistencies)	**X**
Interoperable with major issues (inconsistencies)	
Interoperable	

Is this training tool stable while used in a specific training program?

Not stable	
Stable with minor issues (inconsistencies)	
Stable with major issues (inconsistencies)	
Stable	X

Does this training tool support the user’s (trainer, trainee) privacy and security aspects?

Yes.	**X**
No	
Other	

*If “**Other**”, then respond in free text*

What is the level of prior knowledge needed to use the training tool?

Knowledge of terms	**X**
Knowledge of meanings	**X**
Integration of knowledge	
Application of knowledge	**X**

Do the trainers/trainees find the training tool easy to use?

Yes	
No	**X**

Does this training tool support the trainers/trainees’ native language and/or multiple languages?

Yes	**X**
No	

Appropriateness of the training tool. Tool can be used for:

VG: very good, **G**: good, **NA**: not appropriate	**VG**	**G**	**NA**
Commercial seminar (up to 2 days)			**X**
Commercial course (up to 2 months)	**X**		
Academic Lab (accompanying cybersecurity course) / Academic course	**X**		
Cybersecurity exercise /cyber range		**X**	
Cybersecurity hackathon			**X**
Cybersecurity game			**X**
Certification cybersecurity course		**X**	
Specific Cybersecurity Topic(s)			
Network security control			**X**
Penetration testing		**X**	

Incident response		**X**	
Cloud security			**X**
Risk management			**X**
Forensics		**X**	
Other – Reverse Engineering	**X**		

4.2.16 OllyDbg

Filled by	Panayiotis Kotzanikolaou - Dimitris Koutras
Organization	UPRC
Date	20-05-2023
Contact	pkotzani@unipi.gr – dkoutras@unipi.gr
License	O
Cost of license	-
Available link to download tool	https://www.ollydbg.de/
Online manual(s)	https://www.ollydbg.de/Tut_rtr.htm https://www.ollydbg.de/Loaddll.htm
Online tutorial(s)	https://www.youtube.com/watch?v=D6mVIos-S2M&list=PLg2DkJr3glAbXYYR0tIZ0gLxlQtcV80IU

Description

Summary
OllyDbg is a popular and easy-to-use debugger for analysing and reverse engineering software applications. It allows users to step through code, inspect registers and memory, and analyse the execution flow of a program. OllyDbg supports both static and dynamic analysis and is useful for vulnerability assessment, malware analysis and software debugging. OllyDbg is a Windows-based debugger used for analyzing and reverse engineering software applications. It offers dynamic analysis capabilities such as code stepping, memory inspection, and breakpoints. OllyDbg supports plugins to extend its functionality and add custom analysis features. It provides a user-friendly interface with interactive debugging and disassembly views.

Assessment

The training tool has been used for

Commercial seminar (up to 2 days)	
Commercial course (up to 2 months)	
Academic Lab (accompanying cybersecurity course) / Academic course	X
Cybersecurity exercise /cyber range	
Cybersecurity hackathon	
Cybersecurity game	
Certification cybersecurity course	
Specific Cybersecurity Topic(s)	
Network security control	
Penetration testing	
Incident response	
Cloud security	
Risk management	
Forensics	
Other – write which one	
Demonstration /training to Customer	
Pilot training operation	

Other (explain in free text):	

*If "**Other**", then respond in free text.*

Is this training tool suitable for training purposes (reach the learning objectives and knowledge areas)

Yes	**X**
No	

Are there any needed compute resources (CPUs, GPU, RAM, Disk space)?

Yes	
No	**X**

*If "**Yes**", then respond in free text.*

What is the level of difficulty to use the training tool?

Easy	
Normal	
Medium/Standard/Average	
Intermediate	
Hard/Expert/difficult	**X**

Is this training tool easily adaptable to a specific training program?

Potential	**X**
Most likely	
Neither likely or unlikely	
Least likely	

Is this training tool easily implementable for a specific training program?

Not implementable	
Implementable with minor issues (inconsistencies)	
Implementable with major issues (inconsistencies)	
Implementable	**X**

Is this training tool easily scalable for a specific training program?

Not scalable	
Scalable with minor issues (inconsistencies)	**X**
Scalable with major issues (inconsistencies)	
Scalable	

Does this training tool cover interoperability aspects of a specific training program?

Not interoperable	
Interoperable with minor issues (inconsistencies)	**X**
Interoperable with major issues (inconsistencies)	
Interoperable	

Is this training tool stable while used in a specific training program?

Not stable	
Stable with minor issues (inconsistencies)	
Stable with major issues (inconsistencies)	
Stable	**X**

Does this training tool support the user's (trainer, trainee) privacy and security aspects?

Yes.	**X**
No	
Other	

*If "**Other**", then respond in free text*

What is the level of prior knowledge needed to use the training tool?

Knowledge of terms	
Knowledge of meanings	**X**
Integration of knowledge	**X**
Application of knowledge	

Do the trainers/trainees find the training tool easy to use?

Yes	
No	**X**

Does this training tool support the trainers/trainees’ native language and/or multiple languages?

Yes	**X**
No	

Appropriateness of the training tool. Tool can be used for:

VG: very good, **G**: good, **NA**: not appropriate	**VG**	**G**	**NA**
Commercial seminar (up to 2 days)	**X**		
Commercial course (up to 2 months)		**X**	**X**
Academic Lab (accompanying cybersecurity course) / Academic course	**X**		
Cybersecurity exercise /cyber range		**X**	
Cybersecurity hackathon		**X**	
Cybersecurity game		**X**	
Certification cybersecurity course			**X**
Specific Cybersecurity Topic(s)			
Network security control			
Penetration testing			
Incident response			
Cloud security			
Risk management			
Forensics			
Other – Debugger – reverse engineering	**X**		

4.2.17 angr framework

Filled by	Panayiotis Kotzanikolaou - Dimitris Koutras
Organization	UPRC
Date	20-05-2023
Contact	pkotzani@unipi.gr – dkoutras@unipi.gr
License	O
Cost of license	-
Available link to download tool	https://angr.io/
Online manual(s)	https://docs.angr.io/en/latest/
Online tutorial(s)	https://www.youtube.com/watch?v=oznsT-ptAbk https://www.youtube.com/watch?v=Fi_S2F7ud_g

Description

Summary
The angr framework is a powerful binary analysis framework that enables automated and scalable analysis of executable binaries. It provides a suite of tools and libraries for symbolic execution, program instrumentation, and constraint solving. Using angr, researchers can analyze and understand complex binary programs, discover vulnerabilities, and develop automated security analysis tools. The angr framework is a binary analysis platform designed for automated analysis and vulnerability discovery. It supports symbolic execution, allowing the exploration of all feasible program paths. angr provides APIs for program instrumentation, taint analysis, and constraint solving. It offers a powerful Python interface for scriptable analysis workflows.

Assessment

The training tool has been used for

Commercial seminar (up to 2 days)	
Commercial course (up to 2 months)	
Academic Lab (accompanying cybersecurity course) / Academic course	**X**
Cybersecurity exercise /cyber range	
Cybersecurity hackathon	
Cybersecurity game	
Certification cybersecurity course	
Specific Cybersecurity Topic(s)	
Network security control	
Penetration testing	
Incident response	
Cloud security	
Risk management	
Forensics	
Other – write which one	
Demonstration /training to Customer	
Pilot training operation	

Other (explain in free text):	

*If "**Other**", then respond in free text.*

Is this training tool suitable for training purposes (reach the learning objectives and knowledge areas)

Yes	**X**
No	

Are there any needed compute resources (CPUs, GPU, RAM, Disk space)?

Yes	
No	**X**

*If "**Yes**", then respond in free text.*

What is the level of difficulty to use the training tool?

Easy	
Normal	
Medium/Standard/Average	
Intermediate	
Hard/Expert/difficult	**X**

Is this training tool easily adaptable to a specific training program?

Potential	
Most likely	**X**
Neither likely or unlikely	
Least likely	

Is this training tool easily implementable for a specific training program?

Not implementable	
Implementable with minor issues (inconsistencies)	**X**
Implementable with major issues (inconsistencies)	
Implementable	

Is this training tool easily scalable for a specific training program?

Not scalable	
Scalable with minor issues (inconsistencies)	**X**
Scalable with major issues (inconsistencies)	
Scalable	

Does this training tool cover interoperability aspects of a specific training program?

Not interoperable	
Interoperable with minor issues (inconsistencies)	**X**
Interoperable with major issues (inconsistencies)	
Interoperable	

Is this training tool stable while used in a specific training program?

Not stable	**X**
Stable with minor issues (inconsistencies)	
Stable with major issues (inconsistencies)	
Stable	

Does this training tool support the user's (trainer, trainee) privacy and security aspects?

Yes.	**X**
No	
Other	

*If "**Other**", then respond in free text*

What is the level of prior knowledge needed to use the training tool?

Knowledge of terms	X
Knowledge of meanings	X
Integration of knowledge	
Application of knowledge	X

Do the trainers/trainees find the training tool easy to use?

Yes	
No	X

Does this training tool support the trainers/trainees' native language and/or multiple languages?

Yes	X
No	

Appropriateness of the training tool. Tool can be used for:

VG: very good, **G**: good, **NA**: not appropriate	**VG**	**G**	**NA**
Commercial seminar (up to 2 days)	**X**		
Commercial course (up to 2 months)			**X**
Academic Lab (accompanying cybersecurity course) / Academic course		**X**	
Cybersecurity exercise /cyber range		**X**	
Cybersecurity hackathon		**X**	
Cybersecurity game		**X**	
Certification cybersecurity course			**X**
Specific Cybersecurity Topic(s)			
Network security control			
Penetration testing			
Incident response			
Cloud security			
Risk management			
Forensics			
Other – Binary analysis	**X**		

4.2.18 OSSEC

Filled by	Panayiotis Kotzanikolaou - Dimitris Koutras
Organization	UPRC
Date	20-05-2023
Contact	pkotzani@unipi.gr – dkoutras@unipi.gr
License	O
Cost of license	-
Available link to download tool	https://www.ossec.net/ossec-downloads/
Online manual(s)	https://www.ossec.net/docs/
Online tutorial(s)	https://www.youtube.com/watch?v=7c8xowHz0Ko

Description

Summary
OSSEC is a host-based Intrusion Detection System (IDS) that provides real-time monitoring and response to security events on computer systems. It helps detect unauthorized access attempts, malware infections and system misconfigurations. OSSEC provides centralized management capabilities, enabling administrators to monitor multiple systems and respond effectively to potential security incidents. It supports log analysis, file integrity checking, and rootkit detection. OSSEC provides centralized management capabilities for multiple systems through a server-client architecture. It can generate alerts and notifications for security incidents based on predefined rules and policies.

Assessment

The training tool has been used for

Commercial seminar (up to 2 days)	
Commercial course (up to 2 months)	
Academic Lab (accompanying cybersecurity course) / Academic course	X
Cybersecurity exercise /cyber range	
Cybersecurity hackathon	
Cybersecurity game	
Certification cybersecurity course	
Specific Cybersecurity Topic(s)	
Network security control	X
Penetration testing	
Incident response	X
Cloud security	
Risk management	
Forensics	
Other – write which one	
Demonstration /training to Customer	
Pilot training operation	

Other (explain in free text):	

*If "**Other**", then respond in free text.*

Is this training tool suitable for training purposes (reach the learning objectives and knowledge areas)

Yes	**X**
No	

Are there any needed compute resources (CPUs, GPU, RAM, Disk space)?

Yes	
No	**X**

*If "**Yes**", then respond in free text.*

What is the level of difficulty to use the training tool?

Easy	
Normal	
Medium/Standard/Average	
Intermediate	**X**
Hard/Expert/difficult	

Is this training tool easily adaptable to a specific training program?

Potential	X
Most likely	
Neither likely or unlikely	
Least likely	

Is this training tool easily implementable for a specific training program?

Not implementable	
Implementable with minor issues (inconsistencies)	X
Implementable with major issues (inconsistencies)	
Implementable	

Is this training tool easily scalable for a specific training program?

Not scalable	
Scalable with minor issues (inconsistencies)	X
Scalable with major issues (inconsistencies)	
Scalable	

Does this training tool cover interoperability aspects of a specific training program?

Not interoperable	
Interoperable with minor issues (inconsistencies)	**X**
Interoperable with major issues (inconsistencies)	
Interoperable	

Is this training tool stable while used in a specific training program?

Not stable	
Stable with minor issues (inconsistencies)	**X**
Stable with major issues (inconsistencies)	
Stable	

Does this training tool support the user's (trainer, trainee) privacy and security aspects?

Yes.	**X**
No	
Other	

*If "**Other**", then respond in free text*

What is the level of prior knowledge needed to use the training tool?

Knowledge of terms	
Knowledge of meanings	
Integration of knowledge	
Application of knowledge	**X**

Do the trainers/trainees find the training tool easy to use?

Yes	
No	**X**

Does this training tool support the trainers/trainees’ native language and/or multiple languages?

Yes	**X**
No	

Appropriateness of the training tool. Tool can be used for:

VG: very good, **G**: good, **NA**: not appropriate	**VG**	**G**	**NA**
Commercial seminar (up to 2 days)		**X**	
Commercial course (up to 2 months)			**X**
Academic Lab (accompanying cybersecurity course) / Academic course		**X**	
Cybersecurity exercise /cyber range		**X**	
Cybersecurity hackathon		**X**	
Cybersecurity game		**X**	**X**
Certification cybersecurity course			**X**
Specific Cybersecurity Topic(s)			
Network security control		**X**	
Penetration testing			
Incident response	**X**		
Cloud security			
Risk management			
Forensics			
Other – write which one			

4.2.19 Metasploit Framework

Filled by	Panayiotis Kotzanikolaou - Dimitris Koutras
Organization	UPRC
Date	20-05-2023
Contact	pkotzani@unipi.gr – dkoutras@unipi.gr
License	O
Cost of license	-
Available link to download tool	https://www.metasploit.com/download
Online manual(s)	https://docs.metasploit.com/
Online tutorial(s)	https://www.youtube.com/watch?v=aAsOXtctrvg

Description

Summary
The Metasploit Framework is a popular penetration testing platform used to assess the security of computer systems and networks. It provides a large collection of exploits, payloads, and utilities to simulate real-world attacks. With Metasploit, security professionals can identify vulnerabilities, exploit weaknesses, and contribute to the development of effective security defences. The Metasploit Framework is a comprehensive penetration testing and vulnerability assessment tool. Metasploit supports various exploitation techniques like remote exploits, client-side attacks, and social engineering. It offers both command-line and graphical interfaces for ease of use.

Assessment

The training tool has been used for

Commercial seminar (up to 2 days)	
Commercial course (up to 2 months)	
Academic Lab (accompanying cybersecurity course) / Academic course	X
Cybersecurity exercise /cyber range	
Cybersecurity hackathon	
Cybersecurity game	
Certification cybersecurity course	
Specific Cybersecurity Topic(s)	
Network security control	
Penetration testing	X
Incident response	
Cloud security	
Risk management	
Forensics	
Other – write which one	
Demonstration /training to Customer	
Pilot training operation	

Other (explain in free text):	

*If "**Other**", then respond in free text.*

Is this training tool suitable for training purposes (reach the learning objectives and knowledge areas)

Yes	**X**
No	

Are there any needed compute resources (CPUs, GPU, RAM, Disk space)?

Yes	
No	**X**

*If "**Yes**", then respond in free text.*

What is the level of difficulty to use the training tool?

Easy	
Normal	
Medium/Standard/Average	
Intermediate	**X**
Hard/Expert/difficult	

Is this training tool easily adaptable to a specific training program?

Potential	
Most likely	**X**
Neither likely or unlikely	
Least likely	

Is this training tool easily implementable for a specific training program?

Not implementable	
Implementable with minor issues (inconsistencies)	**X**
Implementable with major issues (inconsistencies)	
Implementable	

Is this training tool easily scalable for a specific training program?

Not scalable	
Scalable with minor issues (inconsistencies)	**X**
Scalable with major issues (inconsistencies)	
Scalable	

Does this training tool cover interoperability aspects of a specific training program?

Not interoperable	
Interoperable with minor issues (inconsistencies)	X
Interoperable with major issues (inconsistencies)	
Interoperable	

Is this training tool stable while used in a specific training program?

Not stable	
Stable with minor issues (inconsistencies)	X
Stable with major issues (inconsistencies)	
Stable	

Does this training tool support the user's (trainer, trainee) privacy and security aspects?

Yes.	X
No	
Other	

*If "**Other**", then respond in free text*

What is the level of prior knowledge needed to use the training tool?

Knowledge of terms	
Knowledge of meanings	
Integration of knowledge	
Application of knowledge	**X**

Do the trainers/trainees find the training tool easy to use?

Yes	
No	**X**

Does this training tool support the trainers/trainees’ native language and/or multiple languages?

Yes	**X**
No	

Appropriateness of the training tool. Tool can be used for:

VG: very good, **G**: good, **NA**: not appropriate	**VG**	**G**	**NA**
Commercial seminar (up to 2 days)	**X**		
Commercial course (up to 2 months)			**X**
Academic Lab (accompanying cybersecurity course) / Academic course	**X**		
Cybersecurity exercise /cyber range			**X**
Cybersecurity hackathon		**X**	
Cybersecurity game		**X**	
Certification cybersecurity course			**X**
Specific Cybersecurity Topic(s)			
Network security control			
Penetration testing		**X**	
Incident response			
Cloud security			
Risk management			
Forensics			
Other – write which one			

4.2.20 CrypTool

Filled by	Panayiotis Kotzanikolaou - Dimitris Koutras
Organization	UPRC
Date	20-05-2023
Contact	pkotzani@unipi.gr – dkoutras@unipi.gr
License	O
Cost of license	-
Available link to download tool	https://www.cryptool.org/en/
Online manual(s)	https://www.cryptool.org/en/documentation/ctbook/
Online tutorial(s)	https://www.cryptool.org/en/links

Description

Summary
CrypTool is an open-source software project that offers a range of cryptographic tools and educational resources. It allows users to learn, experiment with, and apply various cryptographic techniques. CrypTool provides a user-friendly interface and modules covering encryption algorithms, digital signatures, hash functions, steganography, and more. By interacting with these tools, users can gain hands-on experience and understanding of cryptographic principles. Additionally, CrypTool offers educational materials, tutorials, and practical examples to support learning and exploration of cryptography. It serves as a valuable resource for cryptography enthusiasts, students, researchers, and professionals seeking to enhance their knowledge and skills in cryptographic concepts and applications. It supports encryption, decryption, digital signatures, and steganography techniques. CrypTool includes educational resources like tutorials and practical examples to enhance understanding of cryptographic concepts. It offers a user-friendly interface with interactive visualization of cryptographic operations.

CrypTool supports various encryption algorithms such as AES, RSA, and DES.

It provides a platform for testing and comparing different cryptographic techniques.

Assessment

The training tool has been used for

Commercial seminar (up to 2 days)	
Commercial course (up to 2 months)	
Academic Lab (accompanying cybersecurity course) / Academic course	**X**
Cybersecurity exercise /cyber range	
Cybersecurity hackathon	
Cybersecurity game	
Certification cybersecurity course	
Specific Cybersecurity Topic(s)	
Network security control	
Penetration testing	
Incident response	
Cloud security	
Risk management	
Forensics	

Other – write which one	
Demonstration /training to Customer	
Pilot training operation	
Other (explain in free text):	

*If “**Other**”, then respond in free text.*

Is this training tool suitable for training purposes (reach the learning objectives and knowledge areas)

Yes	**X**
No	

Are there any needed compute resources (CPUs, GPU, RAM, Disk space)?

Yes	
No	**X**

*If “**Yes**”, then respond in free text.*

What is the level of difficulty to use the training tool?

Easy	
Normal	**X**
Medium/Standard/Average	
Intermediate	
Hard/Expert/difficult	

Is this training tool easily adaptable to a specific training program?

Potential	**X**
Most likely	
Neither likely or unlikely	
Least likely	

Is this training tool easily implementable for a specific training program?

Not implementable	
Implementable with minor issues (inconsistencies)	
Implementable with major issues (inconsistencies)	
Implementable	**X**

Is this training tool easily scalable for a specific training program?

Not scalable	
Scalable with minor issues (inconsistencies)	
Scalable with major issues (inconsistencies)	
Scalable	X

Does this training tool cover interoperability aspects of a specific training program?

Not interoperable	
Interoperable with minor issues (inconsistencies)	
Interoperable with major issues (inconsistencies)	
Interoperable	X

Is this training tool stable while used in a specific training program?

Not stable	
Stable with minor issues (inconsistencies)	
Stable with major issues (inconsistencies)	
Stable	X

Does this training tool support the user's (trainer, trainee) privacy and security aspects?

Yes.	**X**
No	
Other	

*If "**Other**", then respond in free text*

What is the level of prior knowledge needed to use the training tool?

Knowledge of terms	**X**
Knowledge of meanings	
Integration of knowledge	
Application of knowledge	

Do the trainers/trainees find the training tool easy to use?

Yes	**X**
No	

Does this training tool support the trainers/trainees' native language and/or multiple languages?

Yes	**X**
No	

Appropriateness of the training tool. Tool can be used for:

VG: very good, **G**: good, **NA**: not appropriate	**VG**	**G**	**NA**
Commercial seminar (up to 2 days)	**X**		
Commercial course (up to 2 months)			**X**
Academic Lab (accompanying cybersecurity course) / Academic course	**X**		
Cybersecurity exercise /cyber range		**X**	
Cybersecurity hackathon		**X**	
Cybersecurity game		**X**	
Certification cybersecurity course			**X**
Specific Cybersecurity Topic(s)			
Network security control			
Penetration testing			
Incident response			
Cloud security			
Risk management			
Forensics			
Other – Cryptography	**X**		

4.2.21 John the Ripper

Filled by	Panayiotis Kotzanikolaou - Dimitris Koutras
Organization	UPRC
Date	20-05-2023
Contact	pkotzani@unipi.gr – dkoutras@unipi.gr
License	O
Cost of license	-
Available link to download tool	https://www.openwall.com/john/
Online manual(s)	https://www.openwall.com/john/doc/
Online tutorial(s)	https://www.youtube.com/watch?v=VSBkelymaEo

Description

Summary
John the Ripper is a widely recognized open-source password cracking tool. It is specifically designed to help security professionals, administrators and penetration testers evaluate the strength of passwords. Using various techniques including brute force, dictionary and hybrid attacks, John the Ripper attempts to crack passwords and evaluate their security. The tool supports several password hash formats used by different operating systems and applications. By using John the Ripper, security professionals can test password security, identify weak passwords and enforce stronger password policies. John the Ripper is a command-line password cracking tool. It supports multiple password hash formats, including Unix, Windows, and Kerberos. John the Ripper utilizes different cracking modes, such as brute-force, dictionary attacks, and rule-based attacks.It can leverage GPU acceleration for faster password cracking on compatible hardware. The tool is highly customizable with options for tuning performance and attack methods.

Assessment

The training tool has been used for

Commercial seminar (up to 2 days)	
Commercial course (up to 2 months)	
Academic Lab (accompanying cybersecurity course) / Academic course	**X**
Cybersecurity exercise /cyber range	
Cybersecurity hackathon	
Cybersecurity game	
Certification cybersecurity course	
Specific Cybersecurity Topic(s)	
Network security control	
Penetration testing	
Incident response	
Cloud security	
Risk management	
Forensics	
Other – write which one	
Demonstration /training to Customer	
Pilot training operation	

Other (explain in free text):	

*If “**Other**”, then respond in free text.*

Is this training tool suitable for training purposes (reach the learning objectives and knowledge areas)

Yes	**X**
No	

Are there any needed compute resources (CPUs, GPU, RAM, Disk space)?

Yes	
No	**X**

*If “**Yes**”, then respond in free text.*

What is the level of difficulty to use the training tool?

Easy	
Normal	**X**
Medium/Standard/Average	
Intermediate	
Hard/Expert/difficult	

Is this training tool easily adaptable to a specific training program?

Potential	**X**
Most likely	
Neither likely or unlikely	
Least likely	

Is this training tool easily implementable for a specific training program?

Not implementable	
Implementable with minor issues (inconsistencies)	
Implementable with major issues (inconsistencies)	
Implementable	**X**

Is this training tool easily scalable for a specific training program?

Not scalable	
Scalable with minor issues (inconsistencies)	**X**
Scalable with major issues (inconsistencies)	
Scalable	

Does this training tool cover interoperability aspects of a specific training program?

Not interoperable	
Interoperable with minor issues (inconsistencies)	
Interoperable with major issues (inconsistencies)	
Interoperable	**X**

Is this training tool stable while used in a specific training program?

Not stable	
Stable with minor issues (inconsistencies)	**X**
Stable with major issues (inconsistencies)	
Stable	

Does this training tool support the user's (trainer, trainee) privacy and security aspects?

Yes.	**X**
No	
Other	

*If "**Other**", then respond in free text*

What is the level of prior knowledge needed to use the training tool?

Knowledge of terms	
Knowledge of meanings	X
Integration of knowledge	X
Application of knowledge	

Do the trainers/trainees find the training tool easy to use?

Yes	X
No	

Does this training tool support the trainers/trainees' native language and/or multiple languages?

Yes	X
No	

Appropriateness of the training tool. Tool can be used for:

VG: very good, **G**: good, **NA**: not appropriate	**VG**	**G**	**NA**
Commercial seminar (up to 2 days)		**X**	
Commercial course (up to 2 months)			**X**
Academic Lab (accompanying cybersecurity course) / Academic course		**X**	
Cybersecurity exercise /cyber range	**X**		
Cybersecurity hackathon	**X**		
Cybersecurity game		**X**	
Certification cybersecurity course			**X**
Specific Cybersecurity Topic(s)			
Network security control			
Penetration testing			
Incident response			
Cloud security			
Risk management			
Forensics			
Other – Password cracking		**X**	

4.2.22 OWASP ZAP

Filled by	José Antonio Montenegro Montes[1] Panayiotis Kotzanikolaou[2] Dimitris Koutras[2]
Organization	(1) Universidad de Málaga (2) UPRC
Date	19-05-2023
Contact	(1) jmmontes@uma.es (2) pkotzani@unipi.gr – dkoutras@unipi.gr
License	O: open
Cost of license	Not applicable
Available link to download tool	https://www.zaproxy.org/
Online manual(s)	https://www.zaproxy.org/docs/
Online tutorial(s)	https://www.zaproxy.org/videos/

Description

Summary
OWASP ZAP (Zed Attack Proxy) is a popular open-source web application security testing tool. It provides numerous advantages for identifying and mitigating security vulnerabilities. This tool has been selected to demonstrate to students the use of dynamic analysis tools and to compare its characteristics with those of static analysis tools. It was specifically designed to help developers, security testers and penetration testers identify vulnerabilities and security issues in web applications. OWASP ZAP provides features for intercepting and modifying HTTP requests and responses, automated scanning for common web vulnerabilities, and manual testing capabilities. It helps detect vulnerabilities such as cross-site scripting (XSS), SQL injection and unsafe direct object references. OWASP ZAP generates detailed reports and alerts, enabling users to prioritize and address security issues. It can be integrated with

other security testing tools and plays a vital role in securing web applications throughout the software development lifecycle.

OWASP ZAP supports both manual and automated scanning for web vulnerabilities.

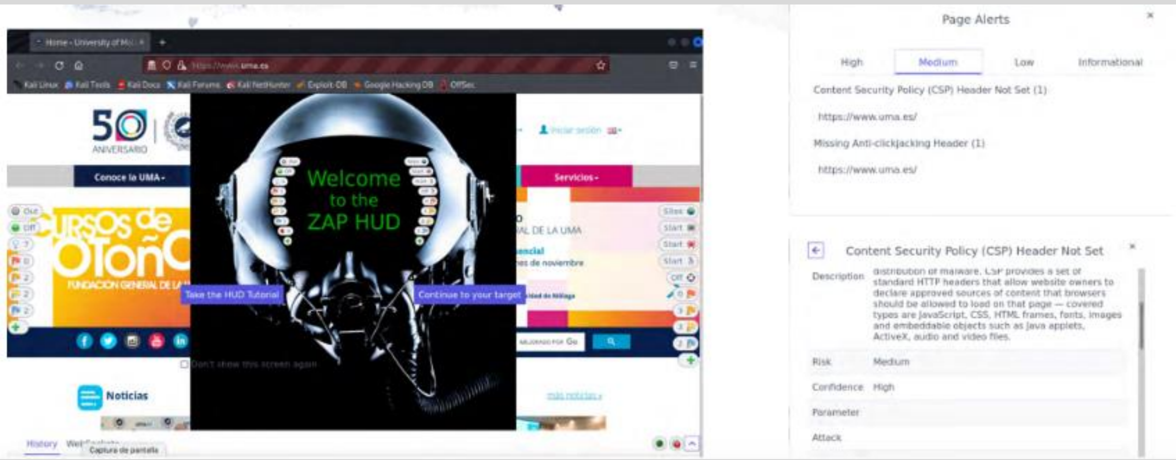
OWASP ZAP can intercept and modify HTTP requests and responses for in-depth analysis.

It provides vulnerability detection for common issues like XSS, SQL injection, and insecure direct object references.

OWASP ZAP generates detailed reports with identified vulnerabilities and recommendations for remediation.

Moreover, OWASP ZAP offers a wide range of security testing capabilities, including scanning for common vulnerabilities such as XSS, SQL injection, and insecure direct object references. It helps identify security flaws early in the development lifecycle. Moreover, OWASP ZAP supports active and Passive scanning, where it actively interacts with the target application to identify vulnerabilities, and passive scanning, where it monitors and analyzes traffic to detect potential issues.

To make the practice more engaging, we have used the OWASP ZAP to check the vulnerabilities of a real web site, http://www.uma.es. The following figure shows the result of the analysis, only medium and low risks are found. In addition to describing the risk, the tool also shows how to fix it.



Content Security Policy (CSP) Header Not Set (1)

https://www.uma.es/

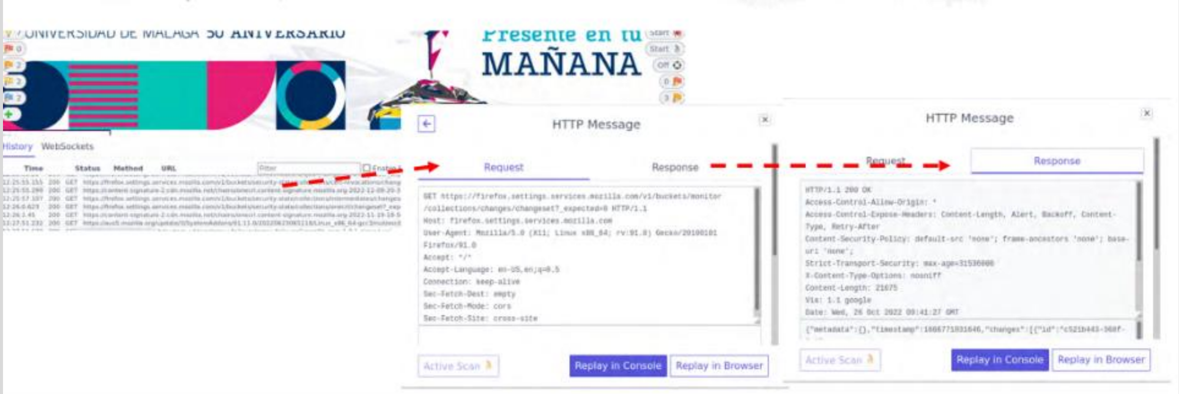
Missing Anti-clickjacking Header (1)

https://www.uma.es/

Content Security Policy (CSP) Header Not Set

Description	distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.
Risk	Medium
Confidence	High
Parameter	
Attack	

Another use case for the tool is traffic analysis. The following figure displays the request and response of an HTTP message. Students can interact with the HTTP protocol by modifying elements within the message to observe how the web application responds to these modifications.



```
GET https://firefox.settings.services.mozilla.com/v1/buckets/monitor
/collections/changes/changeset?_expected=0 HTTP/1.1
Host: firefox.settings.services.mozilla.com
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101
Firefox/91.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Connection: keep-alive
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: cross-site
```

```
HTTP/1.1 200 OK
Access-Control-Allow-Origin: *
Access-Control-Expose-Headers: Content-Length, Alert, Backoff, Content-
Type, Retry-After
Content-Security-Policy: default-src 'none'; frame-ancestors 'none'; base-
uri 'none';
Strict-Transport-Security: max-age=31536000
X-Content-Type-Options: nosniff
Content-Length: 21675
Via: 1.1 google
Date: Wed, 26 Oct 2022 09:41:27 GMT
{"metadata":{},"timestamp":1666771831646,"changes":[{"id":"c521b443-368f-
```

Assessment

The training tool has been used for

Commercial seminar (up to 2 days)	
Commercial course (up to 2 months)	
Academic Lab (accompanying cybersecurity course) / Academic course	**X**
Cybersecurity exercise /cyber range	
Cybersecurity hackathon	
Cybersecurity game	
Certification cybersecurity course	
Specific Cybersecurity Topic(s)	
Network security control	
Penetration testing	**X**
Incident response	
Cloud security	
Risk management	**X**
Forensics	
Other – vulnerability check	**X**
Demonstration /training to Customer	
Pilot training operation	

Other (explain in free text):	

*If “**Other**”, then respond in free text.*

Is this training tool suitable for training purposes (reach the learning objectives and knowledge areas)

Yes	**X**
No	

Are there any needed compute resources (CPUs, GPU, RAM, Disk space)?

Yes	
No	**X**

*If “**Yes**”, then respond in free text.*

What is the level of difficulty to use the training tool?

Easy	
Normal	**X**
Medium/Standard/Average	**X**
Intermediate	
Hard/Expert/difficult	

Is this training tool easily adaptable to a specific training program?

Potential	**X**
Most likely	
Neither likely or unlikely	
Least likely	

Is this training tool easily implementable for a specific training program?

Not implementable	
Implementable with minor issues (inconsistencies)	**X**
Implementable with major issues (inconsistencies)	
Implementable	

Is this training tool easily scalable for a specific training program?

Not scalable	
Scalable with minor issues (inconsistencies)	**X**
Scalable with major issues (inconsistencies)	
Scalable	

Does this training tool cover interoperability aspects of a specific training program?

Not interoperable	
Interoperable with minor issues (inconsistencies)	**X**
Interoperable with major issues (inconsistencies)	
Interoperable	

Is this training tool stable while used in a specific training program?

Not stable	
Stable with minor issues (inconsistencies)	X
Stable with major issues (inconsistencies)	
Stable	

Does this training tool support the user's (trainer, trainee) privacy and security aspects?

Yes.	**X**
No	
Other	

*If "**Other**", then respond in free text*

What is the level of prior knowledge needed to use the training tool?

Knowledge of terms	X
Knowledge of meanings	
Integration of knowledge	X
Application of knowledge	X

Do the trainers/trainees find the training tool easy to use?

Yes	
No	X

Does this training tool support the trainers/trainees' native language and/or multiple languages?

Yes	X
No	

Appropriateness of the training tool. Tool can be used for:

VG: very good, **G**: good, **NA**: not appropriate	**VG**	**G**	**NA**
Commercial seminar (up to 2 days)		X	
Commercial course (up to 2 months)			X
Academic Lab (accompanying cybersecurity course) / Academic course	X		
Cybersecurity exercise /cyber range		X	
Cybersecurity hackathon		X	

Cybersecurity game		X	
Certification cybersecurity course		X	
Specific Cybersecurity Topic(s)			
Network security control			X
Penetration testing	X		
Incident response			X
Cloud security			X
Risk management	X		
Forensics			X
Other – vulnerabilities code	X		

4.2.23 BACS

Filled by	Danijela Boberic Krstićev
Organization	UNSPMF
Date	22-05-2023
Contact	dboberic@uns.ac.rs
License	O
Cost of license	n/a

Available link to download tool	n/a
Online manual(s)	n/a
Online tutorial(s)	n/a

Description

Summary
Anomaly Detection (AD) is examining specific data points and detecting rare occurrences that seem suspicious because they are different from the established pattern of behaviours. Detection and evaluation of such patterns are essential to identification of security breaches. Behavioural anomaly detection is the continuous monitoring process of IT systems and network traffic to identify unusual events or abnormal behavioural patterns. These patterns indicate network changes either that an external attack is underway, or an intrusion is taking over. Early detection of potential security events may facilitate organisations to decrease the impact of these events and mitigate their propagation. Besides anomalies in network data flows, anomalies can be found in application data sent across networks, too. Unlike the network data structure, this data can be very diverse making the process of finding anomalies even harder. Those problems can be solved by applying machine learning techniques. Behavioural Analysis and Cognitive Security (BACS) is a software component offering AD in time series data and network traffic flows based on machine learning and deep learning algorithms. BACS contains Python modules that cover representation of different types of datasets for training unsupervised and supervised AD models. Unsupervised anomaly detection is based on outlier detection algorithms implemented in the scikit-learn library, PyOD library, and Tensorflow. Supervised AD is using the scikit-learn library and Tensorflow2 deep neural networks. To use the BACS component, it is necessary to create and validate machine learning models on real data sets. This tool is suitable for students with some previous knowledge related to machine learning and Python programming. By creating their machine learning models they will be able to detect anomalies in time series data.

Assessment

The training tool has been used for

Commercial seminar (up to 2 days)	

Commercial course (up to 2 months)	
Academic Lab (accompanying cybersecurity course) / Academic course	**x**
Cybersecurity exercise /cyber range	
Cybersecurity hackathon	
Cybersecurity game	
Certification cybersecurity course	
Specific Cybersecurity Topic(s)	
Network security control	
Penetration testing	
Incident response	
Cloud security	
Risk management	
Forensics	
Other – write which one	**x**
Demonstration /training to Customer	
Pilot training operation	
Other (explain in free text):	

*If "**Other**", then respond in free text.*

Anomaly detection

Is this training tool suitable for training purposes (reach the learning objectives and knowledge areas)

Yes	**x**
No	

Are there any needed compute resources (CPUs, GPU, RAM, Disk space)?

Yes	**x**
No	

*If "**Yes**", then respond in free text.*

It requires a Python environment and machine learning models need hardware that can work well with extensive computations.

What is the level of difficulty to use the training tool?

Easy	
Normal	
Medium/Standard/Average	
Intermediate	
Hard/Expert/difficult	**x**

Is this training tool easily adaptable to a specific training program?

Potential	
Most likely	x
Neither likely or unlikely	
Least likely	

Is this training tool easily implementable for a specific training program?

Not implementable	
Implementable with minor issues (inconsistencies)	
Implementable with major issues (inconsistencies)	
Implementable	x

Is this training tool easily scalable for a specific training program?

Not scalable	
Scalable with minor issues (inconsistencies)	
Scalable with major issues (inconsistencies)	
Scalable	x

Does this training tool cover interoperability aspects of a specific training program?

Not interoperable	

Interoperable with minor issues (inconsistencies)	
Interoperable with major issues (inconsistencies)	
Interoperable	x

Is this training tool stable while used in a specific training program?

Not stable	
Stable with minor issues (inconsistencies)	x
Stable with major issues (inconsistencies)	
Stable	

Does this training tool support the user's (trainer, trainee) privacy and security aspects?

Yes.	
No	x
Other	

*If "**Other**", then respond in free text*

What is the level of prior knowledge needed to use the training tool?

Knowledge of terms	
Knowledge of meanings	
Integration of knowledge	
Application of knowledge	x

Do the trainers/trainees find the training tool easy to use?

Yes	x
No	

Does this training tool support the trainers/trainees' native language and/or multiple languages?

Yes	
No	x

Appropriateness of the training tool. Tool can be used for:

VG: very good, **G**: good, **NA**: not appropriate	**VG**	**G**	**NA**
Commercial seminar (up to 2 days)			x
Commercial course (up to 2 months)			x
Academic Lab (accompanying cybersecurity course) / Academic course	x		
Cybersecurity exercise /cyber range	x		

Cybersecurity hackathon			x
Cybersecurity game			x
Certification cybersecurity course			x
Specific Cybersecurity Topic(s)			
Network security control		x	
Penetration testing			x
Incident response			x
Cloud security			x
Risk management			x
Forensics		x	
Other – write which one			

4.2.24 gdb

Filled by	Elias Athanasopoulos
Organization	UCY
Date	10-07-2023
Contact	athanasopoulos.elias@ucy.ac.cy
License	O

Cost of license	-
Available link to download tool	https://www.sourceware.org/gdb/
Online manual(s)	https://www.sourceware.org/gdb/
Online tutorial(s)	https://www.sourceware.org/gdb/

Description

Summary
The GNU debugger (gdb) is one of the established tools for dynamic analysis of programs. Beyond assisting programmers to find bugs, the tool can be used for analysing binary code in general. We provide an in-depth training of how gdb internally works. Specifically, we analyse the steps needed for someone to use basic OS features in Unix, such as fork()/ptrace(), for constructing gdb from scratch. Through the training, the trainee learns how to construct custom tools based on dynamic analysis, as well as low-level mechanics, such as realising software breakpoints for the Intel architecture.

Assessment

The training tool has been used for

Commercial seminar (up to 2 days)	
Commercial course (up to 2 months)	
Academic Lab (accompanying cybersecurity course) / Academic course	**X**
Cybersecurity exercise /cyber range	
Cybersecurity hackathon	
Cybersecurity game	
Certification cybersecurity course	
Specific Cybersecurity Topic(s)	
Network security control	
Penetration testing	
Incident response	
Cloud security	
Risk management	
Forensics	
Other – write which one	
Demonstration /training to Customer	
Pilot training operation	

Other (explain in free text):	

*If “**Other**”, then respond in free text.*

Is this training tool suitable for training purposes (reach the learning objectives and knowledge areas)

Yes	**X**
No	

Are there any needed compute resources (CPUs, GPU, RAM, Disk space)?

Yes	
No	**X**

*If “**Yes**”, then respond in free text.*

What is the level of difficulty to use the training tool?

Easy	
Normal	
Medium/Standard/Average	**X**
Intermediate	
Hard/Expert/difficult	

Is this training tool easily adaptable to a specific training program?

Potential	
Most likely	**X**
Neither likely or unlikely	
Least likely	

Is this training tool easily implementable for a specific training program?

Not implementable	
Implementable with minor issues (inconsistencies)	**X**
Implementable with major issues (inconsistencies)	
Implementable	

Is this training tool easily scalable for a specific training program?

Not scalable	
Scalable with minor issues (inconsistencies)	
Scalable with major issues (inconsistencies)	
Scalable	**X**

Does this training tool cover interoperability aspects of a specific training program?

Not interoperable	
Interoperable with minor issues (inconsistencies)	
Interoperable with major issues (inconsistencies)	
Interoperable	**X**

Is this training tool stable while used in a specific training program?

Not stable	
Stable with minor issues (inconsistencies)	
Stable with major issues (inconsistencies)	
Stable	**X**

Does this training tool support the user's (trainer, trainee) privacy and security aspects?

Yes.	**X**
No	
Other	

*If "**Other**", then respond in free text*

What is the level of prior knowledge needed to use the training tool?

Knowledge of terms	
Knowledge of meanings	
Integration of knowledge	
Application of knowledge	**X**

Do the trainers/trainees find the training tool easy to use?

Yes	**X**
No	

Does this training tool support the trainers/trainees' native language and/or multiple languages?

Yes	**X**
No	

Appropriateness of the training tool. Tool can be used for:

VG: very good, **G**: good, **NA**: not appropriate	**VG**	**G**	**NA**
Commercial seminar (up to 2 days)		**X**	
Commercial course (up to 2 months)		**X**	
Academic Lab (accompanying cybersecurity course) / Academic course	**X**		
Cybersecurity exercise /cyber range	**X**		
Cybersecurity hackathon	**X**		
Cybersecurity game	**X**		
Certification cybersecurity course		**X**	
Specific Cybersecurity Topic(s)			
Network security control			**X**
Penetration testing			**X**
Incident response			**X**
Cloud security			**X**
Risk management			**X**
Forensics	**X**		
Other – write which one			

4.2.25 webFuzz

Filled by	Elia Athanasopoulos
Organization	UCY
Date	10-07-2023
Contact	athanasopoulos.elias@ucy.ac.cy
License	O
Cost of license	-
Available link to download tool	https://bitbucket.org/srecgrp/webfuzz-fuzzer/src/v1.2.1/
Online manual(s)	https://bitbucket.org/srecgrp/webfuzz-fuzzer/src/v1.2.1/
Online tutorial(s)	https://bitbucket.org/srecgrp/webfuzz-fuzzer/src/v1.2.1/

Description

Summary
Fuzzing is significantly evolved in analysing native code, but web applications, invariably, have received limited attention until now. webFuuz is a gray-box fuzzing prototype for discovering vulnerabilities in web applications. webFuzz is successful in leveraging instrumentation for detecting cross-site scripting (XSS) vulnerabilities, as well as covering more code faster than black-box fuzzers. In particular, webFuzz has discovered one zero-day vulnerability in WordPress, a leading CMS platform, and five in an online commerce application named CE-Phoenix. In this training we learn how to instrument web applications written in PHP and how webFuzz can analyse them for discovering XSS vulnerabilities.

Assessment

The training tool has been used for

Commercial seminar (up to 2 days)	
Commercial course (up to 2 months)	
Academic Lab (accompanying cybersecurity course) / Academic course	**X**
Cybersecurity exercise /cyber range	
Cybersecurity hackathon	
Cybersecurity game	
Certification cybersecurity course	
Specific Cybersecurity Topic(s)	
Network security control	
Penetration testing	
Incident response	
Cloud security	
Risk management	
Forensics	
Other – write which one	
Demonstration /training to Customer	
Pilot training operation	

Other (explain in free text):	

*If “**Other**”, then respond in free text.*

Is this training tool suitable for training purposes (reach the learning objectives and knowledge areas)

Yes	**X**
No	

Are there any needed compute resources (CPUs, GPU, RAM, Disk space)?

Yes	
No	**X**

*If “**Yes**”, then respond in free text.*

What is the level of difficulty to use the training tool?

Easy	
Normal	**X**
Medium/Standard/Average	
Intermediate	
Hard/Expert/difficult	

Is this training tool easily adaptable to a specific training program?

Potential	
Most likely	**X**
Neither likely or unlikely	
Least likely	

Is this training tool easily implementable for a specific training program?

Not implementable	
Implementable with minor issues (inconsistencies)	
Implementable with major issues (inconsistencies)	
Implementable	**X**

Is this training tool easily scalable for a specific training program?

Not scalable	
Scalable with minor issues (inconsistencies)	
Scalable with major issues (inconsistencies)	
Scalable	**X**

Does this training tool cover interoperability aspects of a specific training program?

Not interoperable	
Interoperable with minor issues (inconsistencies)	
Interoperable with major issues (inconsistencies)	
Interoperable	**X**

Is this training tool stable while used in a specific training program?

Not stable	
Stable with minor issues (inconsistencies)	**X**
Stable with major issues (inconsistencies)	
Stable	

Does this training tool support the user's (trainer, trainee) privacy and security aspects?

Yes.	**X**
No	
Other	

*If "**Other**", then respond in free text*

What is the level of prior knowledge needed to use the training tool?

Knowledge of terms	
Knowledge of meanings	
Integration of knowledge	
Application of knowledge	**X**

Do the trainers/trainees find the training tool easy to use?

Yes	**X**
No	

Does this training tool support the trainers/trainees' native language and/or multiple languages?

Yes	**X**
No	

Appropriateness of the training tool. Tool can be used for:

VG: very good, **G**: good, **NA**: not appropriate	**VG**	**G**	**NA**
Commercial seminar (up to 2 days)			
Commercial course (up to 2 months)			
Academic Lab (accompanying cybersecurity course) / Academic course	**X**		
Cybersecurity exercise /cyber range	**X**		
Cybersecurity hackathon	**X**		
Cybersecurity game	**X**		
Certification cybersecurity course			**X**
Specific Cybersecurity Topic(s)			
Network security control			
Penetration testing	**X**		
Incident response			
Cloud security			
Risk management			
Forensics			
Other – write which one			

4.2.26 Simulation on movement profiles in cellular mobile networks

Filled by	Rannenberg Kai
Organization	GUF
Date	24-05-2023
Contact	Kai.Rannenberg@m-chair.de
License	O
Cost of license	
Available link to download tool	https://interactive.zeit.de/opendata/widgets/vorratsdatenspeicherung/index.html (not download but usage on provider website)
Online manual(s)	https://interactive.zeit.de/opendata/widgets/vorratsdatenspeicherung/index.html
Online tutorial(s)	https://interactive.zeit.de/opendata/widgets/vorratsdatenspeicherung/index.html

Description

Summary
Visual (graphical) simulation of movement profiles in cellular mobile networks. Students can "follow" a user in a cellular mobile network and learn about cell sizes, cell shapes, and the fine granularity of mobile and partially usage profiles enabled by cellular mobile networks

Assessment

The training tool has been used for

Commercial seminar (up to 2 days)	
Commercial course (up to 2 months)	
Academic Lab (accompanying cybersecurity course) / Academic course	**x**
Cybersecurity exercise /cyber range	**x**
Cybersecurity hackathon	
Cybersecurity game	
Certification cybersecurity course	
Specific Cybersecurity Topic(s)	
Network security control	
Penetration testing	
Incident response	
Cloud security	
Risk management	
Forensics	
Other – write which one	**x**
Demonstration /training to Customer	
Pilot training operation	

Other (explain in free text):	

*If “**Other**”, then respond in free text.*

Movement profiles in cellular mobile networks

Is this training tool suitable for training purposes (reach the learning objectives and knowledge areas)

Yes	**x**
No	

Are there any needed compute resources (CPUs, GPU, RAM, Disk space)?

Yes	**x**
No	

*If “**Yes**”, then respond in free text.*

Internet access and a browser, ideally Firefox

What is the level of difficulty to use the training tool?

Easy	**x**
Normal	
Medium/Standard/Average	
Intermediate	
Hard/Expert/difficult	

Is this training tool easily adaptable to a specific training program?

Potential	**x**
Most likely	
Neither likely or unlikely	
Least likely	

Is this training tool easily implementable for a specific training program?

Not implementable	
Implementable with minor issues (inconsistencies)	
Implementable with major issues (inconsistencies)	
Implementable	**x**

Is this training tool easily scalable for a specific training program?

Not scalable	
Scalable with minor issues (inconsistencies)	
Scalable with major issues (inconsistencies)	
Scalable	**x**

Does this training tool cover interoperability aspects of a specific training program?

Not interoperable	
Interoperable with minor issues (inconsistencies)	
Interoperable with major issues (inconsistencies)	
Interoperable	**x**

Is this training tool stable while used in a specific training program?

Not stable	
Stable with minor issues (inconsistencies)	
Stable with major issues (inconsistencies)	
Stable X	**x**

Does this training tool support the user’s (trainer, trainee) privacy and security aspects?

Yes.	**x**
No	
Other	

*If “**Other**”, then respond in free text*

What is the level of prior knowledge needed to use the training tool?

Knowledge of terms	x
Knowledge of meanings	
Integration of knowledge	
Application of knowledge	

Do the trainers/trainees find the training tool easy to use?

Yes	x
o	

Does this training tool support the trainers/trainees' native language and/or multiple languages?

Yes	
No	x

Appropriateness of the training tool. Tool can be used for:

VG: very good, **G**: good, **NA**: not appropriate	**VG**	**G**	**NA**
Commercial seminar (up to 2 days)			
Commercial course (up to 2 months)			
Academic Lab (accompanying cybersecurity course) / Academic course	**x**		
Cybersecurity exercise /cyber range	**x**		
Cybersecurity hackathon			
Cybersecurity game	**x**		
Certification cybersecurity course			
Specific Cybersecurity Topic(s)			
Network security control			
Penetration testing			
Incident response			
Cloud security			
Risk management	**x**		
Forensics	**x**		
Other – write which one	**x**		

4.2.27 Penetration Testing Methodology

Filled by	Nuno Mateus-Coelho
Organization	COFAC
Date	10th of October 2023
Contact	nuno.coelho@ulusofona.pt
License	N/A
Cost of license	N/A
Available link to download tool	N/A
Online manual(s)	N/A
Online tutorial(s)	N/A

Summary
COFAC Training “Penetration Testing Methodology" training session. In this session, we will provide an overview of penetration testing and the methodology used by cybersecurity professionals to identify vulnerabilities in computer systems, networks, and applications.

The training tool has been used for:

Commercial seminar (up to 2 days)	
Commercial course (up to 2 months)	
Academic Lab (accompanying cybersecurity course) / Academic course	**x**

Cybersecurity exercise /cyber range	x
Cybersecurity hackathon	
Cybersecurity game	
Certification cybersecurity course	
Specific Cybersecurity Topic(s)	
Network security control	
Penetration testing	x
Incident response	
Cloud security	
Risk management	
Forensics	x
Other – write which one	
Demonstration /training to Customer	x
Pilot training operation	
Other (explain in free text):	

If “**Other**”, then respond in free text.

Is this training tool suitable for training purposes (reach the learning objectives and knowledge areas

Yes	x
No	

Are there any needed compute resources (CPUs, GPU, RAM, Disk space)?

Yes	x

No	

If “**Yes**”, then respond in free text.

Desktop / Laptop with CPU 8 Core and 12GB Ram. Capacity for virtualization of 6 environments

What is the level of difficulty to use the training tool?

Easy	
Normal	**x**
Medium/Standard/Average	
Intermediate	
Hard/Expert/difficult	

Is this training tool easily adaptable to a specific training program?

Potential	**x**
Most likely	
Neither likely nor unlikely	
Least likely	

Is this training tool easily implementable for a specific training program?

Not implementable	
Implementable with minor issues (inconsistencies)	
Implementable with major issues (inconsistencies)	
Implementable	**x**

Is this training tool easily scalable for a specific training program?

Not scalable	**x**
Scalable with minor issues (inconsistencies)	
Scalable with major issues (inconsistencies)	
Scalable	

Does this training tool cover interoperability aspects of a specific training program?

Not interoperable	
Interoperable with minor issues (inconsistencies)	
Interoperable with major issues (inconsistencies)	
Interoperable	**x**

Is this training tool stable while used in a specific training program?

Not stable	
Stable with minor issues (inconsistencies)	
Stable with major issues (inconsistencies)	
Stable	**x**

Does this training tool support the user's (trainer, trainee) privacy and security aspects?

Yes.	x
No	
Other	x

If "**Other**", then respond in free text.

Some aspects of the Pentest methodology comprehend the use of OS that can be challenging in terms of privacy. Setting up the environment as sandbox will suffice.

What is the level of prior knowledge needed to use the training tool?

Knowledge of terms	x
Knowledge of meanings	x
Integration of knowledge	x
Application of knowledge	

Do the trainers/trainees find the training tool easy to use?

Yes	x
No	

Does this training tool support the trainers/trainees' native language and/or multiple languages?

Yes	x
No	

Appropriateness of the training tool. Tool can be used for:

VG: very good, **G**: good, **NA**: not appropriate	**VG**	**G**	**NA**
Commercial seminar (up to 2 days)			**x**
Commercial course (up to 2 months)	**x**		
Academic Lab (accompanying cybersecurity course) / Academic course	**x**		
Cybersecurity exercise /cyber range	**x**		
Cybersecurity hackathon	**x**		
Cybersecurity game		**x**	
Certification cybersecurity course	**x**		
Specific Cybersecurity Topic(s)			
Network security control			
Penetration testing	**x**		
Incident response			
Cloud security			
Risk management	**x**		
Forensics	**x**		
Other – write which one			

4.2.28 OSINT with MALTEGO

Filled by	Nuno Mateus-Coelho
Organization	COFAC
Date	10th of October 2023
Contact	nuno.coelho@ulusofona.pt
License	N/A
Cost of license	N/A
Available link to download tool	N/A
Online manual(s)	N/A
Online tutorial(s)	N/A

Summary
COFAC Training Maltego OSINT Session aims the training "hands-on" to grasp the ability to harness open-source intelligence, becoming vital skills for individuals and organizations alike. Maltego, a powerful and versatile data mining tool, is at the forefront of transforming open-source data into actionable insights. This training session will equip trainees with the knowledge and skills to leverage Maltego for your OSINT needs.

The training tool has been used for:

Commercial seminar (up to 2 days)	
Commercial course (up to 2 months)	
Academic Lab (accompanying cybersecurity course) / Academic course	x
Cybersecurity exercise /cyber range	x
Cybersecurity hackathon	x
Cybersecurity game	
Certification cybersecurity course	
Specific Cybersecurity Topic(s)	
Network security control	
Penetration testing	
Incident response	
Cloud security	
Risk management	x
Forensics	x
Other – write which one	
Demonstration /training to Customer	x
Pilot training operation	
Other (explain in free text):	

If “**Other**”, then respond in free text.

Is this training tool suitable for training purposes (reach the learning objectives and knowledge areas

Yes	**X**
No	

Are there any needed compute resources (CPUs, GPU, RAM, Disk space)?

Yes	**X**
No	

If "**Yes**", then respond in free text.

Internet access and disc capacity to store large datasets.

What is the level of difficulty to use the training tool?

Easy	
Normal	
Medium/Standard/Average	**x**
Intermediate	
Hard/Expert/difficult	

Is this training tool easily adaptable to a specific training program?

Potential	
Most likely	**x**
Neither likely or unlikely	
Least likely	

Is this training tool easily implementable for a specific training program?

Not implementable	
Implementable with minor issues (inconsistencies)	
Implementable with major issues (inconsistencies)	
Implementable	**x**

Is this training tool easily scalable for a specific training program?

Not scalable	**x**
Scalable with minor issues (inconsistencies)	
Scalable with major issues (inconsistencies)	
Scalable	

Does this training tool cover interoperability aspects of a specific training program?

Not interoperable	
Interoperable with minor issues (inconsistencies)	
Interoperable with major issues (inconsistencies)	
Interoperable	**x**

Is this training tool stable while used in a specific training program?

Not stable	
Stable with minor issues (inconsistencies)	
Stable with major issues (inconsistencies)	

Stable	**x**

Does this training tool support the user’s (trainer, trainee) privacy and security aspects?

Yes.	**x**
No	
Other	

If “**Other**”, then respond in free text.

What is the level of prior knowledge needed to use the training tool?

Knowledge of terms	**x**
Knowledge of meanings	**x**
Integration of knowledge	**x**
Application of knowledge	

Do the trainers/trainees find the training tool easy to use?

Yes	**x**
No	

Does this training tool support the trainers/trainees' native language and/or multiple languages?

Yes	**x**
No	

Appropriateness of the training tool. Tool can be used for:

VG: very good, **G**: good, **NA**: not appropriate	**VG**	**G**	**NA**
Commercial seminar (up to 2 days)	**x**		
Commercial course (up to 2 months)	**x**		
Academic Lab (accompanying cybersecurity course) / Academic course	**x**		
Cybersecurity exercise /cyber range	**x**		
Cybersecurity hackathon	**x**		
Cybersecurity game	**x**		
Certification cybersecurity course	**x**		
Specific Cybersecurity Topic(s)			
Network security control		**x**	
Penetration testing			
Incident response		**x**	
Cloud security			
Risk management		**x**	
Forensics		**x**	
Other – write which one			

4.3 CSP Commercial Partner Cybersecurity Training Tools and Platforms

4.3.1 FP_TTX

Filled by	Paris Laras
Organization	Focal Point
Date	21-05-2023
Contact	plaras@focalpoint-sprl.be
License	P
Cost of license	TBD
Available link to download tool	TBD
Online manual(s)	TBD
Online tutorial(s)	TBD

Description

Summary
The tabletop exercise is designed and delivered as an interactive, gamified experience by Focal Point for multiple participating persons. Participants are divided into groups with each group led by a moderator trained by Focal Point in preparing the exercise, assisting in the distribution of relevant materials, educating the participants, moderating the exercise, and reporting on the outcomes of the exercise. The exercise itself is supported by printed materials such as a rulebook, cards, and other supplementary items (such as dice, boards etc). Furthermore, the rules of the exercise are provided digitally for sharing with participants and event coordinators, along with dedicated guidelines for moderators addressing specific scenarios. The outcomes of the tabletop exercise are increased cyber-awareness, the introduction of cyber hygiene concepts to the participants and supplementary soft skills with increased transferability due to the group aspects of the tool.

Assessment

The training tool has been used for

Commercial seminar (up to 2 days)	
Commercial course (up to 2 months)	
Academic Lab (accompanying cybersecurity course) / Academic course	
Cybersecurity exercise /cyber range	
Cybersecurity hackathon	
Cybersecurity game	x
Certification cybersecurity course	
Specific Cybersecurity Topic(s)	
Network security control	
Penetration testing	
Incident response	
Cloud security	
Risk management	
Forensics	
Other – write which one	
Demonstration /training to Customer	
Pilot training operation	✓

Other (explain in free text):	✓

*If “**Other**”, then respond in free text.*

Is this training tool suitable for training purposes (reach the learning objectives and knowledge areas)

Yes	✓
No	

Are there any needed compute resources (CPUs, GPU, RAM, Disk space)?

Yes	
No	✓

*If “**Yes**”, then respond in free text.*

What is the level of difficulty to use the training tool?

Easy	✓
Normal	
Medium/Standard/Average	

Intermediate	
Hard/Expert/difficult	

Is this training tool easily adaptable to a specific training program?

Potential	✓
Most likely	✓
Neither likely or unlikely	
Least likely	

Is this training tool easily implementable for a specific training program?

Not implementable	
Implementable with minor issues (inconsistencies)	
Implementable with major issues (inconsistencies)	
Implementable	✓

Is this training tool easily scalable for a specific training program?

Not scalable	
Scalable with minor issues (inconsistencies)	
Scalable with major issues (inconsistencies)	

Scalable	✓

Does this training tool cover interoperability aspects of a specific training program?

Not interoperable	
Interoperable with minor issues (inconsistencies)	✓
Interoperable with major issues (inconsistencies)	
Interoperable	

Is this training tool stable while used in a specific training program?

Not stable	
Stable with minor issues (inconsistencies)	
Stable with major issues (inconsistencies)	
Stable	✓

Does this training tool support the user’s (trainer, trainee) privacy and security aspects?

Yes.	✓
No	
Other	

*If "**Other**", then respond in free text*

What is the level of prior knowledge needed to use the training tool?

Knowledge of terms	
Knowledge of meanings	
Integration of knowledge	
Application of knowledge	

Do the trainers/trainees find the training tool easy to use?

Yes	✓
No	

Does this training tool support the trainers/trainees' native language and/or multiple languages?

Yes	✓
No	

Appropriateness of the training tool. Tool can be used for:

VG: very good, **G**: good, **NA**: not appropriate	**VG**	**G**	**NA**
Commercial seminar (up to 2 days)	✓		
Commercial course (up to 2 months)	✓		

Academic Lab (accompanying cybersecurity course) / Academic course		✓	
Cybersecurity exercise /cyber range	✓		
Cybersecurity hackathon	✓		
Cybersecurity game	✓		
Certification cybersecurity course			✓
Specific Cybersecurity Topic(s)		✓	
Network security control		✓	
Penetration testing		✓	
Incident response		✓	
Cloud security		✓	
Risk management		✓	
Forensics		✓	
Other – write which one		✓	

4.3.2 FP_CDX

Filled by	Christos Grigoriadis
Organization	Focal Point
Date	21-05-2023

Contact	cgrigor@focalpoint-sprl.be
License	-
Cost of license	-
Available link to download tool	Not any
Online manual(s)	Not any
Online tutorial(s)	Not any

Description

Summary
Focal Point's cyber defense exercise cyber-range is a cutting-edge training tool that immerses learners in a dynamic active directory environment, consisting of three powerful DC Windows Servers. This sophisticated cyber range is purposefully designed with integrated vulnerabilities and attack paths, providing a realistic simulation of real-world cybersecurity challenges. Within this range, experienced professors orchestrate a series of simulated attacks to generate a comprehensive set of intrusion logs. These logs serve as invaluable learning resources for the students. A pfsense firewall implementation is setup to gather and forward logs for further analysis. One of the remarkable features of the platform is its integration with a Security Information and Event Management (SIEM) system called Sentinel. The SIEM seamlessly collects and centralizes the produced intrusion logs, enabling in-depth analysis and monitoring of the cyber range environment.

Assessment

The training tool has been used for

Commercial seminar (up to 2 days)	
Commercial course (up to 2 months)	

Academic Lab (accompanying cybersecurity course) / Academic course	✓
Cybersecurity exercise /cyber range	✓
Cybersecurity hackathon	
Cybersecurity game	
Certification cybersecurity course	
Specific Cybersecurity Topic(s)	
Network security control	
Penetration testing	
Incident response	✓
Cloud security	
Risk management	
Forensics	✓
Other – write which one	
Demonstration /training to Customer	
Pilot training operation	
Other (explain in free text):	

*If “**Other**”, then respond in free text.*

Is this training tool suitable for training purposes (reach the learning objectives and knowledge areas)

Yes	✓
No	

Are there any needed compute resources (CPUs, GPU, RAM, Disk space)?

Yes	✓
No	

*If "**Yes**", then respond in free text.*

What is the level of difficulty to use the training tool?

Easy	
Normal	
Medium/Standard/Average	✓
Intermediate	
Hard/Expert/difficult	

Is this training tool easily adaptable to a specific training program?

Potential	
Most likely	✓
Neither likely or unlikely	
Least likely	

Is this training tool easily implementable for a specific training program?

Not implementable	✓
Implementable with minor issues (inconsistencies)	✓
Implementable with major issues (inconsistencies)	
Implementable	

Is this training tool easily scalable for a specific training program?

Not scalable	
Scalable with minor issues (inconsistencies)	
Scalable with major issues (inconsistencies)	✓
Scalable	

Does this training tool cover interoperability aspects of a specific training program?

Not interoperable	✓
Interoperable with minor issues (inconsistencies)	
Interoperable with major issues (inconsistencies)	
Interoperable	

Is this training tool stable while used in a specific training program?

Not stable	
Stable with minor issues (inconsistencies)	
Stable with major issues (inconsistencies)	
Stable	✓

Does this training tool support the user’s (trainer, trainee) privacy and security aspects?

Yes.	✓
No	
Other	

*If "**Other**", then respond in free text*

What is the level of prior knowledge needed to use the training tool?

Knowledge of terms	✓
Knowledge of meanings	✓
Integration of knowledge	
Application of knowledge	✓

Do the trainers/trainees find the training tool easy to use?

Yes	✓
No	

Does this training tool support the trainers/trainees' native language and/or multiple languages?

Yes	
No	✓

Appropriateness of the training tool. Tool can be used for:

VG: very good, **G**: good, **NA**: not appropriate	**VG**	**G**	**NA**
Commercial seminar (up to 2 days)		✓	
Commercial course (up to 2 months)		✓	
Academic Lab (accompanying cybersecurity course) / Academic course	✓		
Cybersecurity exercise /cyber range	✓		
Cybersecurity hackathon	✓		
Cybersecurity game		✓	
Certification cybersecurity course		✓	
Specific Cybersecurity Topic(s)			
Network security control			
Penetration testing			
Incident response		✓	
Cloud security			
Risk management			
Forensics		✓	
Other – write which one			

4.3.3 FP Training Lab

Filled by	Christos Grigoriadis
Organization	Focal Point
Date	21-05-2023
Contact	cgrigor@focalpoint-sprl.be
License	-
Cost of license	-
Available link to download tool	Not any
Online manual(s)	Not any
Online tutorial(s)	Not any

Description

Summary

The FP Training Lab provides a rich set of resources and support to enhance the learning process. Trainees have access to comprehensive documentation, tutorials, and case studies that illustrate real-world red teaming engagements. They also benefit from interactive demonstrations and walkthroughs, where instructors showcase best practices and demonstrate the step-by-step execution of various attacks.

In the Lab a Healthcare infrastructure is simulated, where various deprecated equipment and services are virtualized, including an openemr server back by an sql type database.

The infrastructure offers a wide vulnerability surface to familiarize the students with a wide range of attacks such as:

- DDOS
- SQL injection
- exploitation of known vulnerabilities in unsafe components
- privilege elevation
- persistence

Assessment

The training tool has been used for

Commercial seminar (up to 2 days)	
Commercial course (up to 2 months)	
Academic Lab (accompanying cybersecurity course) / Academic course	✓
Cybersecurity exercise /cyber range	✓
Cybersecurity hackathon	
Cybersecurity game	
Certification cybersecurity course	
Specific Cybersecurity Topic(s)	
Network security control	
Penetration testing	✓
Incident response	
Cloud security	
Risk management	
Forensics	
Other – write which one	
Demonstration /training to Customer	

Pilot training operation	
Other (explain in free text):	

*If "**Other**", then respond in free text.*

Is this training tool suitable for training purposes (reach the learning objectives and knowledge areas)

Yes	✓
No	

Are there any needed compute resources (CPUs, GPU, RAM, Disk space)?

Yes	✓
No	

*If "**Yes**", then respond in free text.*

What is the level of difficulty to use the training tool?

Easy	
Normal	
Medium/Standard/Average	✓
Intermediate	
Hard/Expert/difficult	

Is this training tool easily adaptable to a specific training program?

Potential	
Most likely	✓
Neither likely or unlikely	
Least likely	

Is this training tool easily implementable for a specific training program?

Not implementable	
Implementable with minor issues (inconsistencies)	✓
Implementable with major issues (inconsistencies)	
Implementable	

Is this training tool easily scalable for a specific training program?

Not scalable	
Scalable with minor issues (inconsistencies)	
Scalable with major issues (inconsistencies)	✓
Scalable	

Does this training tool cover interoperability aspects of a specific training program?

Not interoperable	✓
Interoperable with minor issues (inconsistencies)	
Interoperable with major issues (inconsistencies)	
Interoperable	

Is this training tool stable while used in a specific training program?

Not stable	
Stable with minor issues (inconsistencies)	
Stable with major issues (inconsistencies)	
Stable	✓

Does this training tool support the user's (trainer, trainee) privacy and security aspects?

Yes.	✓
No	
Other	

*If "**Other**", then respond in free text*

What is the level of prior knowledge needed to use the training tool?

Knowledge of terms	✓
Knowledge of meanings	✓
Integration of knowledge	
Application of knowledge	✓

Do the trainers/trainees find the training tool easy to use?

Yes	✓
No	

Does this training tool support the trainers/trainees' native language and/or multiple languages?

Yes	
No	✓

Appropriateness of the training tool. Tool can be used for:

VG: very good, **G**: good, **NA**: not appropriate	**VG**	**G**	**NA**
Commercial seminar (up to 2 days)		✓	
Commercial course (up to 2 months)		✓	
Academic Lab (accompanying cybersecurity course) / Academic course	✓		
Cybersecurity exercise /cyber range	✓		
Cybersecurity hackathon	✓		
Cybersecurity game			✓
Certification cybersecurity course		✓	
Specific Cybersecurity Topic(s)			
Network security control			
Penetration testing	✓		
Incident response			
Cloud security			
Risk management			
Forensics			
Other – write which one			

4.3.4 HtB Enterprise Labs

Filled by	Christos Grigoriadis
Organization	Focal Point
Date	21-05-2023
Contact	cgrigor@focalpoint-sprl.be
License	till December 23
Cost of license	15.000 euros
Available link to download tool	Not any
Online manual(s)	Not any
Online tutorial(s)	Not any

Description

Summary
Dedicated Labs are a safe environment for students to experience curated and unique hacking content that is created by security professionals for security professionals. The cybersecurity content features mechanics and techniques inspired by gaming that make the entire user experience fun and captivating, resulting in increased team engagement. The two forms of content included in Dedicated Lab are “Boxes” and “Challenges”: Boxes are instances of vulnerable virtual machines. These are virtualized services, virtualized operating systems, and virtualized hardware that all run on our servers. Boxes tend to have multi-step exploit paths and can host different Operating Systems; Linux, Windows, FreeBSD, and more. Challenges are bite-sized applications for different penetration testing techniques. While they may feature chained exploits, they generally are meant to showcase one concept and are composed of a single application. Each Box has a difficulty level that signifies the complexity and amount of steps in the exploit path. The five different difficulty levels are as follows: Very Easy: simple Boxes, with typically only a single main exploit step.

Easy: These Boxes are still simple but offer a bit more of a challenge compared to the previous level. They generally comprise 2-3 steps, and have a relatively clear exploit path, with only the most basic scripting required.

Medium: Medium Boxes are where things can start getting complex. They usually have around 3 steps and may require some custom exploitation. The path is generally clear and free of rabbit-holes. Some scripting or programming knowledge may be required.

Hard: These are complex Boxes with 3-5 steps that involve custom exploitation and chaining together different vulnerabilities. Heavy enumeration may be required, and the path may not always be obvious.

Insane: These are the most difficult Boxes HtB dedicated labs have to offer. They are targeted towards highly experienced pentesters who are looking to push themselves to the limit. They typically involve more than 5 steps and can have extremely complex exploit chains. They may include rabbit-holes and deadends.

Assessment

The training tool has been used for

Commercial seminar (up to 2 days)	✓
Commercial course (up to 2 months)	✓
Academic Lab (accompanying cybersecurity course) / Academic course	✓
Cybersecurity exercise /cyber range	✓
Cybersecurity hackathon	✓
Cybersecurity game	
Certification cybersecurity course	✓
Specific Cybersecurity Topic(s)	
Network security control	✓
Penetration testing	✓

Incident response	
Cloud security	
Risk management	
Forensics	
Other – write which one	
Demonstration /training to Customer	
Pilot training operation	
Other (explain in free text):	

*If "**Other**", then respond in free text.*

Is this training tool suitable for training purposes (reach the learning objectives and knowledge areas)

Yes	✓
No	

Are there any needed compute resources (CPUs, GPU, RAM, Disk space)?

Yes	
No	✓

*If "**Yes**", then respond in free text.*

What is the level of difficulty to use the training tool?

Easy	✓
Normal	
Medium/Standard/Average	
Intermediate	
Hard/Expert/difficult	

Is this training tool easily adaptable to a specific training program?

Potential	
Most likely	✓
Neither likely or unlikely	
Least likely	

Is this training tool easily implementable for a specific training program?

Not implementable	
Implementable with minor issues (inconsistencies)	
Implementable with major issues (inconsistencies)	
Implementable	✓

Is this training tool easily scalable for a specific training program?

Not scalable	
Scalable with minor issues (inconsistencies)	
Scalable with major issues (inconsistencies)	
Scalable	✓

Does this training tool cover interoperability aspects of a specific training program?

Not interoperable	✓
Interoperable with minor issues (inconsistencies)	
Interoperable with major issues (inconsistencies)	
Interoperable	

Is this training tool stable while used in a specific training program?

Not stable	
Stable with minor issues (inconsistencies)	
Stable with major issues (inconsistencies)	
Stable	✓

Does this training tool support the user's (trainer, trainee) privacy and security aspects?

Yes.	✓
No	
Other	

*If "**Other**", then respond in free text*

What is the level of prior knowledge needed to use the training tool?

Knowledge of terms	✓
Knowledge of meanings	✓
Integration of knowledge	
Application of knowledge	✓

Do the trainers/trainees find the training tool easy to use?

Yes	✓
No	

Does this training tool support the trainers/trainees’ native language and/or multiple languages?

Yes	
No	✓

Appropriateness of the training tool. Tool can be used for:

VG: very good, **G**: good, **NA**: not appropriate	**VG**	**G**	**NA**
Commercial seminar (up to 2 days)	✓		
Commercial course (up to 2 months)	✓		
Academic Lab (accompanying cybersecurity course) / Academic course	✓		
Cybersecurity exercise /cyber range	✓		
Cybersecurity hackathon	✓		
Cybersecurity game			
Certification cybersecurity course	✓		
Specific Cybersecurity Topic(s)			
Network security control			
Penetration testing	✓		
Incident response			
Cloud security			
Risk management			
Forensics			
Other – write which one			

4.3.5 Moodle

Filled by	Spiros Borotis
Organization	Maggioli
Date	15-09-2023
Contact	spiros.borotis@maggioli.gr
License	O
Cost of license	-
Available link to download tool	https://elearning.maggioli.it/
Online manual(s)	https://docs.moodle.org/19/en/Moodle_manuals
Online tutorial(s)	https://docs.moodle.org/dev/Tutorial https://docs.moodle.org/22/en/Moodle_video_tutorials

Description

Summary
Guidelines: Moodle is an open-source Learning Management System (LMS) which is widely used by trainers and institutions to create and manage online courses and learning activities environments. The key characteristics of Moodle include the following: Course Management: Trainers may use Moodle to create and organize a course training content (text, multimedia, assignments, quizzes, etc). It provides tools for structuring the course materials. Communication and Collaboration: Moodle provides various communication tools such as forums, chat, and messaging in order to facilitate interactions between trainers and trainees or among trainees. Assessment and Grading: Trainers may set up quizzes, assignments, and other assessment activities. It supports various question types and allows for automated grading.

Customization: Moodle is highly customizable, allowing training administrators to modify its appearance and functionality so as to meet their specific needs. It also supports the integration of multiple third-party plugins and extensions.

User Management: Moodle provides tools for managing user accounts, roles, and permissions.

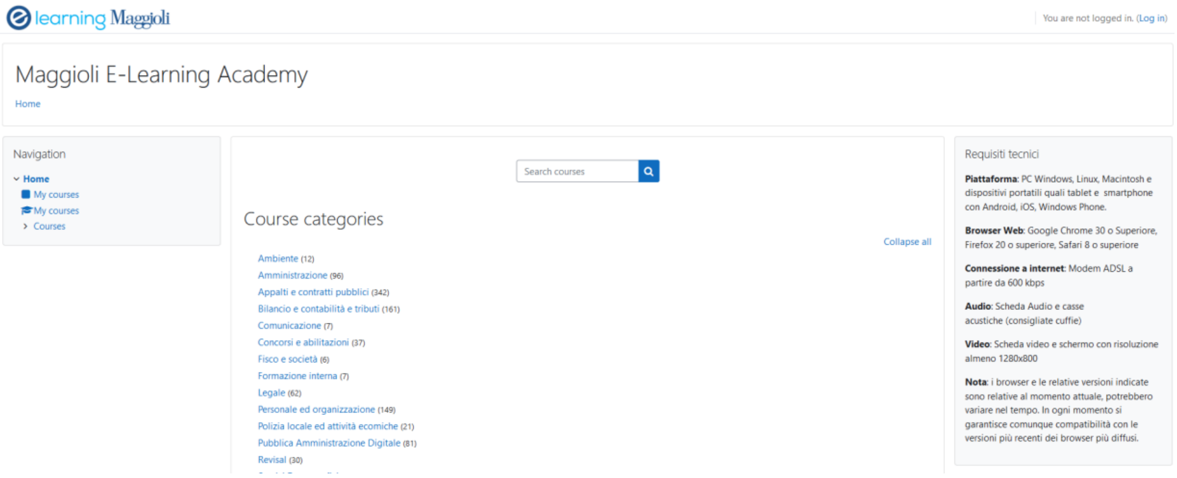
Reporting and Analytics: It provides reporting functionalities to enable trainers to track their students' progress and engagement.

Mobile-Friendly: Moodle is accessible from various devices, including smartphones and tablets, through responsive design or mobile apps.

Multilingual Support: Moodle supports multiple languages, making it suitable for international and diverse user communities.

Moodle is quite popular in educational institutions, including schools, universities, and corporate training environments, as it allows for the creation of online courses and the administration of learning activities. Its open-source nature means that it is freely available for anyone to use and can be modified and extended to suit specific educational needs.

Given its nature, Moodle is not linked to only some cybersecurity knowledge areas, but may support the delivery of training materials (in particular formats that it supports) in all of them.



You are not logged in. (Log in)

Maggioli E-Learning Academy

Home

Navigation

- Home
  - My courses
  - My courses
  - Courses

Course categories

- Ambiente (12)
- Amministrazione (96)
- Appalti e contratti pubblici (342)
- Bilancio e contabilità e tributi (161)
- Comunicazione (7)
- Concorsi e abilitazioni (37)
- Fisco e società (6)
- Formazione interna (7)
- Legale (62)
- Personale ed organizzazione (149)
- Polizia locale ed attività ecomiche (21)
- Pubblica Amministrazione Digitale (81)
- Revisal (30)

Requisiti tecnici

Piattaforma: PC Windows, Linux, Macintosh e dispositivi portatili quali tablet e smartphone con Android, iOS, Windows Phone.

Browser Web: Google Chrome 30 o Superiore, Firefox 20 o superiore, Safari 8 o superiore

Connessione a internet: Modem ADSL a partire da 600 kbps

Audio: Scheda Audio e casse acustiche (consigliate cuffie)

Video: Scheda video e schermo con risoluzione almeno 1280x800

Nota: i browser e le relative versioni indicate sono relative al momento attuale, potrebbero variare nel tempo. In ogni momento si garantisce comunque compatibilità con le versioni più recenti dei browser più diffusi.

Assessment

The training tool has been used for

Commercial seminar (up to 2 days)	
Commercial course (up to 2 months)	√
Academic Lab (accompanying cybersecurity course) / Academic course	
Cybersecurity exercise /cyber range	
Cybersecurity hackathon	
Cybersecurity game	
Certification cybersecurity course	
Specific Cybersecurity Topic(s)	
Network security control	
Penetration testing	
Incident response	
Cloud security	
Risk management	
Forensics	
Other – write which one	
Demonstration /training to Customer	

Pilot training operation	√
Other (explain in free text):	

*If "**Other**", then respond in free text.*

Is this training tool suitable for training purposes (reach the learning objectives and knowledge areas)

Yes	√
No	

Are there any needed compute resources (CPUs, GPU, RAM, Disk space)?

Yes	√
No	

*If "**Yes**", then respond in free text.*

Technical requirements:

Platform: Windows PC, Linux, Macintosh and portable devices such as tablets and smartphones with Android, iOS, Windows Phone.

Web browser: Google Chrome 30 or higher, Firefox 20 or higher, Safari 8 or higher

Internet connection: ADSL modem starting at 600 kbps

Audio: Sound card and speakers (headphones recommended)

Video: Video card and screen with at least 1280x800 resolution

Note: the browsers and related versions indicated are relevant to the current moment, they may vary over time. However, compatibility with the most recent versions of the most popular browsers is guaranteed at all times.

What is the level of difficulty to use the training tool?

Easy	
Normal	√
Medium/Standard/Average	
Intermediate	
Hard/Expert/difficult	

Is this training tool easily adaptable to a specific training program?

Potential	
Most likely	
Neither likely or unlikely	√
Least likely	

Is this training tool easily implementable for a specific training program?

Not implementable	
Implementable with minor issues (inconsistencies)	√
Implementable with major issues (inconsistencies)	
Implementable	

Is this training tool easily scalable for a specific training program?

Not scalable	
Scalable with minor issues (inconsistencies)	√
Scalable with major issues (inconsistencies)	
Scalable	

Does this training tool cover interoperability aspects of a specific training program?

Not interoperable	
Interoperable with minor issues (inconsistencies)	√
Interoperable with major issues (inconsistencies)	
Interoperable	

Is this training tool stable while used in a specific training program?

Not interoperable	
Interoperable with minor issues (inconsistencies)	
Interoperable with major issues (inconsistencies)	
Interoperable	√

Does this training tool support the user's (trainer, trainee) privacy and security aspects?

Yes.	√
No	
Other	

*If “**Other**”, then respond in free text*

What is the level of prior knowledge needed to use the training tool?

Knowledge of terms	√
Knowledge of meanings	
Integration of knowledge	
Application of knowledge	

Do the trainers/trainees find the training tool easy to use?

Yes	√
No	

Does this training tool support the trainers/trainees’ native language and/or multiple languages?

Yes	√
No	

Appropriateness of the training tool. Tool can be used for:

VG: very good, **G**: good, **NA**: not appropriate	**VG**	**G**	**NA**
Commercial seminar (up to 2 days)		√	
Commercial course (up to 2 months)	√		
Academic Lab (accompanying cybersecurity course) / Academic course		√	
Cybersecurity exercise /cyber range			
Cybersecurity hackathon			
Cybersecurity game			
Certification cybersecurity course		√	
Specific Cybersecurity Topic(s)			
Network security control			
Penetration testing			
Incident response			
Cloud security			
Risk management			
Forensics			
Other – write which one			

4.3.6 SPA

Filled by	Stylianos Karagiannis
Organization	PDMFC
Date	18-07-2023
Contact	stylianos.karagiannis@pdmfc.com
License	C
Cost of license	O for the project
Available link to download tool	Gitlab Repository
Online manual(s)	Private
Online tutorial(s)	Not available

Description

Summary
SPA (Secure Personal Access) is a powerful identity management software designed to enhance access control, user authentication, and identity governance within organizations. It offers a wide range of functionalities, including user authentication, authorization management, identity lifecycle management, and compliance and governance features. By implementing role-based access control, integrating with external systems, and providing a self-service portal, SPA streamlines identity management processes, mitigates cybersecurity risks, and promotes compliance with regulatory standards. The learning objectives linked to SPA encompass understanding identity management principles, authentication mechanisms, role-based access control, compliance requirements, and automating identity provisioning processes. The tool addresses various cybersecurity knowledge areas, including access control systems, authentication systems, identity management, security policy development, and compliance aspects. SPA enables organizations to solve problems related to secure access control, password management, identity lifecycle management, and regulatory compliance. The learning process for SPA may involve training sessions, workshops, and practical exercises, providing both theoretical knowledge and hands-on experience with the software. Technical aspects

of SPA include on-premises or cloud-based deployment, encryption protocols, integration APIs, and adherence to security best practices.

Assessment

The training tool has been used for

Commercial seminar (up to 2 days)	X
Commercial course (up to 2 months)	
Academic Lab (accompanying cybersecurity course) / Academic course	
Cybersecurity exercise /cyber range	
Cybersecurity hackathon	X
Cybersecurity game	
Certification cybersecurity course	
Specific Cybersecurity Topic(s)	X
Network security control	X
Penetration testing	
Incident response	
Cloud security	X
Risk management	
Forensics	
Other – write which one	

Demonstration /training to Customer	X
Pilot training operation	
Other (explain in free text):	

If “Other”, then respond in free text.

Is this training tool suitable for training purposes (reach the learning objectives and knowledge areas)

Yes	X
No	

Are there any needed compute resources (CPUs, GPU, RAM, Disk space)?

Yes	X
No	

If “Yes”, then respond in free text.

4-core CPU, 8GB RAM

What is the level of difficulty to use the training tool?

Easy	
Normal	
Medium/Standard/Average	X
Intermediate	
Hard/Expert/difficult	

Is this training tool easily adaptable to a specific training program?

Potential	
Most likely	X
Neither likely or unlikely	
Least likely	

Is this training tool easily implementable for a specific training program?

Not implementable	
Implementable with minor issues (inconsistencies)	
Implementable with major issues (inconsistencies)	X
Implementable	

Is this training tool easily scalable for a specific training program?

Not scalable	
Scalable with minor issues (inconsistencies)	X
Scalable with major issues (inconsistencies)	
Scalable	

Does this training tool cover interoperability aspects of a specific training program?

Not interoperable	
Interoperable with minor issues (inconsistencies)	X
Interoperable with major issues (inconsistencies)	
Interoperable	

Is this training tool stable while used in a specific training program?

Not stable	
Stable with minor issues (inconsistencies)	X
Stable with major issues (inconsistencies)	
Stable	

Does this training tool support the user’s (trainer, trainee) privacy and security aspects?

Yes.	X
No	
Other	

If “Other”, then respond in free text

What is the level of prior knowledge needed to use the training tool?

Knowledge of terms	
Knowledge of meanings	
Integration of knowledge	X
Application of knowledge	

Do the trainers/trainees find the training tool easy to use?

Yes	
No	X

Does this training tool support the trainers/trainees’ native language and/or multiple languages?

Yes	
No	X

Appropriateness of the training tool. Tool can be used for:

VG: very good, G: good, NA: not appropriate	VG	G	NA
Commercial seminar (up to 2 days)		X	
Commercial course (up to 2 months)		X	
Academic Lab (accompanying cybersecurity course) / Academic course		X	
Cybersecurity exercise /cyber range		X	
Cybersecurity hackathon		X	
Cybersecurity game		X	
Certification cybersecurity course		X	
Specific Cybersecurity Topic(s)	X		
Network security control			X
Penetration testing			X
Incident response			X
Cloud security	X		
Risk management			X
Forensics		X	
Other – write which one			

4.3.7 UFED

Filled by	Stylianos Karagiannis
Organization	PDMFC
Date	15-08-2023
Contact	stylianos.karagiannis@pdmfc.com
License	O
Cost of license	O for the project
Available link to download tool	Gitlab Repository
Online manual(s)	Private
Online tutorial(s)	Not available

Description

Summary
UFED, forms a formidable module with core functionalities that encompass data extraction from diverse devices, in-depth data analysis, and professional report generation, making it an indispensable asset in cybercrime investigations, incident response, and legal proceedings. Commercial tools like Cellebrite and open-source tools like Kuiper extends UFED's capabilities by introducing advanced data analysis and visualization, enhancing data interpretation and pattern recognition. A tool from PDM (Chimera/Metago), will be used for forensic data collection and distribution. This module's goal is to equip students with comprehensive digital forensics skills, including the ethical and legal aspects, linked to knowledge areas, skills, and competencies in cybersecurity. Data Extraction: UFED can extract data from mobile phones, computers, and digital media, bypassing security measures. Data Analysis: It enables in-depth analysis of extracted data, including recovering deleted files, call logs, messages, and more. Reporting: UFED supports the creation of professional forensic reports for legal and investigative purposes.

Integration with Kuiper: Kuiper software enhances UFED by offering advanced data analysis and visualization.

Assessment

The training tool has been used for

Commercial seminar (up to 2 days)	X
Commercial course (up to 2 months)	X
Academic Lab (accompanying cybersecurity course) / Academic course	
Cybersecurity exercise /cyber range	
Cybersecurity hackathon	
Cybersecurity game	X
Certification cybersecurity course	
Specific Cybersecurity Topic(s)	X
Network security control	X
Penetration testing	
Incident response	X
Cloud security	
Risk management	
Forensics	X
Other – write which one	

Demonstration /training to Customer	
Pilot training operation	
Other (explain in free text):	

If “Other”, then respond in free text.

Is this training tool suitable for training purposes (reach the learning objectives and knowledge areas)

Yes	X
No	

Are there any needed compute resources (CPUs, GPU, RAM, Disk space)?

Yes	X
No	

If “Yes”, then respond in free text.

Server running Kuiper (RAM: 4Gb+, CPU: At least 4-core, SSD disk)

What is the level of difficulty to use the training tool?

Easy	
Normal	X
Medium/Standard/Average	
Intermediate	
Hard/Expert/difficult	

Is this training tool easily adaptable to a specific training program?

Potential	
Most likely	X
Neither likely or unlikely	
Least likely	

Is this training tool easily implementable for a specific training program?

Not implementable	
Implementable with minor issues (inconsistencies)	
Implementable with major issues (inconsistencies)	
Implementable	X

Is this training tool easily scalable for a specific training program?

Not scalable	
Scalable with minor issues (inconsistencies)	
Scalable with major issues (inconsistencies)	
Scalable	X

Does this training tool cover interoperability aspects of a specific training program?

Not interoperable	
Interoperable with minor issues (inconsistencies)	
Interoperable with major issues (inconsistencies)	
Interoperable	X

Is this training tool stable while used in a specific training program?

Not stable	
Stable with minor issues (inconsistencies)	X
Stable with major issues (inconsistencies)	
Stable	

Does this training tool support the user's (trainer, trainee) privacy and security aspects?

Yes.	X
No	
Other	

If "Other", then respond in free text

What is the level of prior knowledge needed to use the training tool?

Knowledge of terms	
Knowledge of meanings	X
Integration of knowledge	
Application of knowledge	

Do the trainers/trainees find the training tool easy to use?

Yes	
No	X

Does this training tool support the trainers/trainees' native language and/or multiple languages?

Yes	
No	X

Appropriateness of the training tool. Tool can be used for:

VG: very good, G: good, NA: not appropriate	VG	G	NA
Commercial seminar (up to 2 days)	X		
Commercial course (up to 2 months)		X	
Academic Lab (accompanying cybersecurity course) / Academic course			
Cybersecurity exercise /cyber range		X	
Cybersecurity hackathon			
Cybersecurity game		X	
Certification cybersecurity course			
Specific Cybersecurity Topic(s)		X	
Network security control		X	
Penetration testing			
Incident response	X		
Cloud security			
Risk management		X	
Forensics	X		
Other – write which one			

4.3.8 Chimera

Filled by	Stylianos Karagiannis
Organization	PDMFC
Date	18-07-2023
Contact	stylianos.karagiannis@pdmfc.com
License	C
Cost of license	O for the project
Available link to download tool	Gitlab
Online manual(s)	Private
Online tutorial(s)	Possible

Description

Summary
Chimera is an advanced software tool designed to parse logs and live network traffic, with a primary objective of enabling privacy on datasets and secure distribution using TCP flows. It combines powerful log parsing capabilities with privacy-preserving techniques to protect sensitive information and ensures secure transmission. Chimera addresses the critical need for privacy preservation and secure data distribution in log analysis and network monitoring scenarios. Chimera's core functionality includes efficient log parsing, enabling structured data extraction from various log file formats, and real-time analysis of live network traffic. It provides valuable insights into network behaviour, anomaly detection, and identification of potential security threats. The distinguishing feature of Chimera is its focus on privacy preservation. By employing techniques such as data anonymization, aggregation, and encryption, Chimera ensures that personally identifiable information and other sensitive data within logs and network traffic remain secure and confidential. This protection of sensitive information is crucial in compliance with privacy regulations and safeguarding the privacy rights of individuals. Additionally, Chimera facilitates the secure distribution of parsed log data and network traffic using TCP flows. By establishing secure connections and encrypting data during transmission, Chimera ensures that sensitive information is protected from unauthorized access or interception.

The learning process for Chimera may involve training sessions, workshops, and practical exercises. Participants gain theoretical knowledge about log analysis, network monitoring, privacy preservation, and secure data transmission. Hands-on experience with the Chimera software allows them to practice log parsing, network traffic analysis, and implement privacy-enhancing measures. Practical scenarios and examples are provided to reinforce learning objectives.

Assessment

The training tool has been used for

Commercial seminar (up to 2 days)	X
Commercial course (up to 2 months)	
Academic Lab (accompanying cybersecurity course) / Academic course	
Cybersecurity exercise /cyber range	
Cybersecurity hackathon	
Cybersecurity game	
Certification cybersecurity course	
Specific Cybersecurity Topic(s)	X
Network security control	X
Penetration testing	X
Incident response	X
Cloud security	X
Risk management	

Forensics	X
Other – write which one	
Demonstration /training to Customer	X
Pilot training operation	X
Other (explain in free text):	

If "Other", then respond in free text.

Is this training tool suitable for training purposes (reach the learning objectives and knowledge areas)

Yes	X
No	

Are there any needed compute resources (CPUs, GPU, RAM, Disk space)?

Yes	
No	X

If "Yes", then respond in free text.

What is the level of difficulty to use the training tool?

Easy	
Normal	X
Medium/Standard/Average	
Intermediate	
Hard/Expert/difficult	

Is this training tool easily adaptable to a specific training program?

Potential	X
Most likely	
Neither likely or unlikely	
Least likely	

Is this training tool easily implementable for a specific training program?

Not implementable	
Implementable with minor issues (inconsistencies)	
Implementable with major issues (inconsistencies)	
Implementable	X

Is this training tool easily scalable for a specific training program?

Not scalable	
Scalable with minor issues (inconsistencies)	
Scalable with major issues (inconsistencies)	
Scalable	X

Does this training tool cover interoperability aspects of a specific training program?

Not interoperable	
Interoperable with minor issues (inconsistencies)	
Interoperable with major issues (inconsistencies)	
Interoperable	X

Is this training tool stable while used in a specific training program?

Not stable	
Stable with minor issues (inconsistencies)	X
Stable with major issues (inconsistencies)	
Stable	

Does this training tool support the user’s (trainer, trainee) privacy and security aspects?

Yes.	X
No	
Other	

If “Other”, then respond in free text

What is the level of prior knowledge needed to use the training tool?

Knowledge of terms	
Knowledge of meanings	X
Integration of knowledge	
Application of knowledge	

Do the trainers/trainees find the training tool easy to use?

Yes	X
No	

Does this training tool support the trainers/trainees’ native language and/or multiple languages?

Yes	
No	X

Appropriateness of the training tool. Tool can be used for:

VG: very good, G: good, NA: not appropriate	VG	G	NA
Commercial seminar (up to 2 days)	X		
Commercial course (up to 2 months)	X		
Academic Lab (accompanying cybersecurity course) / Academic course	X		
Cybersecurity exercise /cyber range	X		
Cybersecurity hackathon	X		
Cybersecurity game		X	
Certification cybersecurity course	X		
Specific Cybersecurity Topic(s)	X		
Network security control	X		
Penetration testing			X
Incident response	X		
Cloud security	X		
Risk management			X
Forensics	X		
Other – write which one			

4.3.9 Metago

Filled by	Stylianos Karagiannis
Organization	PDMFC
Date	18-07-2023
Contact	stylianos.karagiannis@pdmfc.com
License	C
Cost of license	O for the project
Available link to download tool	Gitlab
Online manual(s)	Private
Online tutorial(s)	Implementable

Description

Summary
Metago is a powerful software tool designed for log retrieval and analysis, with a focus on enhancing learning in the areas of log management, cybersecurity, and IT operations. Its core functionality includes efficient log retrieval from diverse sources, centralized log management, log parsing and filtering, and log analysis and visualization. The goal of learning with Metago is to develop proficiency in with log retrieval and analysis processes, leading to improved system monitoring, incident detection, and operational efficiency. The learning objectives associated with Metago include understanding the importance of log retrieval and analysis, gaining knowledge of log formats and protocols, acquiring skills in log retrieval techniques, parsing, filtering, and analysis, and developing competencies in log visualization and interpreting log data for security incident detection. The learning process for Metago may involve training sessions, workshops, and hands-on exercises. Participants gain theoretical knowledge about log management, log formats, and protocols. Practical training the Metago software allows users to retrieve logs, perform parsing, filtering, and analysis. Practical scenarios and examples are provided to reinforce learning objectives.

Assessment

The training tool has been used for

Commercial seminar (up to 2 days)	X
Commercial course (up to 2 months)	X
Academic Lab (accompanying cybersecurity course) / Academic course	
Cybersecurity exercise /cyber range	X
Cybersecurity hackathon	X
Cybersecurity game	
Certification cybersecurity course	
Specific Cybersecurity Topic(s)	X
Network security control	X
Penetration testing	
Incident response	X
Cloud security	X
Risk management	
Forensics	X
Other – write which one	
Demonstration /training to Customer	X
Pilot training operation	X

Other (explain in free text):	

If "Other", then respond in free text.

Is this training tool suitable for training purposes (reach the learning objectives and knowledge areas)

Yes	X
No	

Are there any needed compute resources (CPUs, GPU, RAM, Disk space)?

Yes	
No	X

If "Yes", then respond in free text.

What is the level of difficulty to use the training tool?

Easy	
Normal	X
Medium/Standard/Average	
Intermediate	
Hard/Expert/difficult	

Is this training tool easily adaptable to a specific training program?

Potential	
Most likely	X
Neither likely or unlikely	
Least likely	

Is this training tool easily implementable for a specific training program?

Not implementable	
Implementable with minor issues (inconsistencies)	
Implementable with major issues (inconsistencies)	
Implementable	X

Is this training tool easily scalable for a specific training program?

Not scalable	
Scalable with minor issues (inconsistencies)	X
Scalable with major issues (inconsistencies)	
Scalable	

Does this training tool cover interoperability aspects of a specific training program?

Not interoperable	
Interoperable with minor issues (inconsistencies)	X
Interoperable with major issues (inconsistencies)	
Interoperable	

Is this training tool stable while used in a specific training program?

Not stable	
Stable with minor issues (inconsistencies)	
Stable with major issues (inconsistencies)	
Stable	X

Does this training tool support the user’s (trainer, trainee) privacy and security aspects?

Yes.	X
No	
Other	

If “Other”, then respond in free text

What is the level of prior knowledge needed to use the training tool?

Knowledge of terms	
Knowledge of meanings	X
Integration of knowledge	
Application of knowledge	

Do the trainers/trainees find the training tool easy to use?

Yes	X
No	

Does this training tool support the trainers/trainees’ native language and/or multiple languages?

Yes	
No	X

Appropriateness of the training tool. Tool can be used for:

VG: very good, G: good, NA: not appropriate	VG	G	NA
Commercial seminar (up to 2 days)	X		
Commercial course (up to 2 months)	X		
Academic Lab (accompanying cybersecurity course) / Academic course	X		
Cybersecurity exercise /cyber range	X		
Cybersecurity hackathon	X		
Cybersecurity game		X	
Certification cybersecurity course	X		
Specific Cybersecurity Topic(s)	X		
Network security control	X		
Penetration testing			X
Incident response	X		
Cloud security	X		
Risk management			X
Forensics	X		
Other – write which one			

4.3.10 IDPS

Filled by	Stylianos Karagiannis
Organization	PDMFC
Date	18-07-2023
Contact	stylianos.karagiannis@pdmfc.com
License	O
Cost of license	O
Available link to download tool	https://github.com/OISF/suricata
Online manual(s)	Online
Online tutorial(s)	Online and Implementable new material

Description

Summary
Learning about Suricata as an Intrusion Detection and Prevention System (IDPS) involves gaining knowledge and developing skills to effectively deploy, configure, and utilize Suricata for network threat detection and prevention. The learning process encompasses understanding Suricata's purpose, architecture, and key components, along with practical skills in deployment, configuration, rule creation, network traffic analysis, and incident response. Participants engage in training sessions, workshops, and practical exercises to acquire proficiency in Suricata's deployment, configuration, rule management, network traffic analysis, and effective incident response. This learning journey covers various cybersecurity knowledge areas, skills, and technical aspects associated with intrusion detection and prevention systems, network security and threats, incident detection and response, network protocols, and traffic analysis. By acquiring skills in Suricata, learners develop the expertise to enhance network security through the proactive identification and prevention of potential threats.

Assessment

The training tool has been used for

Commercial seminar (up to 2 days)	
Commercial course (up to 2 months)	
Academic Lab (accompanying cybersecurity course) / Academic course	X
Cybersecurity exercise /cyber range	X
Cybersecurity hackathon	X
Cybersecurity game	
Certification cybersecurity course	X
Specific Cybersecurity Topic(s)	X
Network security control	X
Penetration testing	
Incident response	X
Cloud security	X
Risk management	
Forensics	X
Other – write which one	
Demonstration /training to Customer	
Pilot training operation	
Other (explain in free text):	

If “Other”, then respond in free text.

Is this training tool suitable for training purposes (reach the learning objectives and knowledge areas)

Yes	X
No	

Are there any needed compute resources (CPUs, GPU, RAM, Disk space)?

Yes	X
No	

If “Yes”, then respond in free text.

4-core, 8GB RAM

What is the level of difficulty to use the training tool?

Easy	
Normal	X
Medium/Standard/Average	
Intermediate	
Hard/Expert/difficult	

Is this training tool easily adaptable to a specific training program?

Potential	X

Most likely	
Neither likely or unlikely	
Least likely	

Is this training tool easily implementable for a specific training program?

Not implementable	
Implementable with minor issues (inconsistencies)	
Implementable with major issues (inconsistencies)	
Implementable	X

Is this training tool easily scalable for a specific training program?

Not scalable	
Scalable with minor issues (inconsistencies)	
Scalable with major issues (inconsistencies)	
Scalable	X

Does this training tool cover interoperability aspects of a specific training program?

Not interoperable	

Interoperable with minor issues (inconsistencies)	
Interoperable with major issues (inconsistencies)	
Interoperable	X

Is this training tool stable while used in a specific training program?

Not stable	
Stable with minor issues (inconsistencies)	
Stable with major issues (inconsistencies)	
Stable	X

Does this training tool support the user's (trainer, trainee) privacy and security aspects?

Yes.	X
No	
Other	

If "Other", then respond in free text

What is the level of prior knowledge needed to use the training tool?

Knowledge of terms	

Knowledge of meanings	X
Integration of knowledge	
Application of knowledge	

Do the trainers/trainees find the training tool easy to use?

Yes	X
No	

Does this training tool support the trainers/trainees’ native language and/or multiple languages?

Yes	
No	X

Appropriateness of the training tool. Tool can be used for:

VG: very good, G: good, NA: not appropriate	VG	G	NA
Commercial seminar (up to 2 days)	X		
Commercial course (up to 2 months)	X		
Academic Lab (accompanying cybersecurity course) / Academic course	X		
Cybersecurity exercise /cyber range	X		
Cybersecurity hackathon	X		
Cybersecurity game		X	
Certification cybersecurity course	X		
Specific Cybersecurity Topic(s)	X		
Network security control	X		
Penetration testing		X	
Incident response	X		
Cloud security	X		
Risk management			X
Forensics	X		
Other – write which one			

4.3.11 Metadon

Filled by	Stylianos Karagiannis
Organization	PDMFC
Date	18-07-2023
Contact	stylianos.karagiannis@pdmfc.com
License	C
Cost of license	O for the project
Available link to download tool	Gitlab
Online manual(s)	Private
Online tutorial(s)	Implementable

Description

Summary
Metadon is a feature-rich Security Information and Event Management (SIEM) software that offers organizations a comprehensive solution for log management, event correlation, and security incident detection. With its custom detection rules and regex parser for logs, Metadon provides the flexibility to tailor log analysis and efficiently identify specific security threats and patterns. The learning process associated with Metadon aims to develop a deep understanding of SIEM concepts, log management practices, custom detection rule creation, and regex parsing for effective log analysis. By gaining proficiency in Metadon, learners acquire the knowledge and skills needed to optimize log analysis, perform event correlation, and detect security incidents with precision. Learning about Metadon involves grasping the fundamentals of SIEM systems and their significance in cybersecurity and incident response. Participants acquire knowledge of log management principles, including log formats, protocols, and analysis techniques for effective security monitoring. They also develop skills in creating and configuring custom detection rules to detect specific security threats and vulnerabilities. Additionally, learners gain expertise in utilizing the regex parser to extract valuable information from logs and identify patterns. The learning process incorporates training sessions, workshops, and practical exercises, enabling participants to gain hands-on experience with Metadon's functionalities. By exploring practical scenarios and examples, learners reinforce their

understanding and develop competence in log management, event correlation, custom detection rule creation, and regex parsing for log analysis.

Assessment

The training tool has been used for

Commercial seminar (up to 2 days)	X
Commercial course (up to 2 months)	
Academic Lab (accompanying cybersecurity course) / Academic course	
Cybersecurity exercise /cyber range	X
Cybersecurity hackathon	X
Cybersecurity game	
Certification cybersecurity course	
Specific Cybersecurity Topic(s)	X
Network security control	X
Penetration testing	
Incident response	X
Cloud security	X
Risk management	
Forensics	X

Other – write which one	
Demonstration /training to Customer	X
Pilot training operation	X
Other (explain in free text):	

If “Other”, then respond in free text.

Is this training tool suitable for training purposes (reach the learning objectives and knowledge areas)

Yes	X
No	

Are there any needed compute resources (CPUs, GPU, RAM, Disk space)?

Yes	X
No	

If “Yes”, then respond in free text.

4,8-Core CPU, 16GB RAM, 256GB SSD hard disk as minimum

What is the level of difficulty to use the training tool?

Easy	
Normal	X
Medium/Standard/Average	
Intermediate	
Hard/Expert/difficult	

Is this training tool easily adaptable to a specific training program?

Potential	X
Most likely	
Neither likely or unlikely	
Least likely	

Is this training tool easily implementable for a specific training program?

Not implementable	
Implementable with minor issues (inconsistencies)	
Implementable with major issues (inconsistencies)	
Implementable	X

Is this training tool easily scalable for a specific training program?

Not scalable	
Scalable with minor issues (inconsistencies)	X
Scalable with major issues (inconsistencies)	
Scalable	

Does this training tool cover interoperability aspects of a specific training program?

Not interoperable	
Interoperable with minor issues (inconsistencies)	
Interoperable with major issues (inconsistencies)	
Interoperable	X

Is this training tool stable while used in a specific training program?

Not stable	
Stable with minor issues (inconsistencies)	
Stable with major issues (inconsistencies)	
Stable	X

Does this training tool support the user’s (trainer, trainee) privacy and security aspects?

Yes.	X
No	
Other	

If “Other”, then respond in free text

What is the level of prior knowledge needed to use the training tool?

Knowledge of terms	
Knowledge of meanings	
Integration of knowledge	X
Application of knowledge	

Do the trainers/trainees find the training tool easy to use?

Yes	X
No	

Does this training tool support the trainers/trainees’ native language and/or multiple languages?

Yes	
No	X

Appropriateness of the training tool. Tool can be used for:

VG: very good, G: good, NA: not appropriate	VG	G	NA
Commercial seminar (up to 2 days)	X		
Commercial course (up to 2 months)	X		
Academic Lab (accompanying cybersecurity course) / Academic course	X		
Cybersecurity exercise /cyber range	X		
Cybersecurity hackathon	X		
Cybersecurity game		X	
Certification cybersecurity course	X		
Specific Cybersecurity Topic(s)	X		
Network security control	X		
Penetration testing			X
Incident response	X		
Cloud security	X		
Risk management		X	
Forensics	X		
Other – write which one			

4.3.12 Chidroid

Filled by	Stylianos Karagiannis
Organization	PDMFC
Date	18-07-2023
Contact	stylianos.karagiannis@pdmfc.com
License	C
Cost of license	O for the project
Available link to download tool	Gitlab
Online manual(s)	Private
Online tutorial(s)	Implementable

Description

Summary
Chidroid, the Android log retrieval tool, involves gaining knowledge and developing skills in effectively retrieving and analyzing log data from Android devices. The learning process focuses on understanding the functionalities of Chidroid, including log retrieval, analysis, and real-time monitoring. Participants acquire the necessary skills to diagnose issues, debug applications, and identify potential security vulnerabilities within the Android operating system using Chidroid. The learning objectives associated with Chidroid include understanding the process of Android log retrieval, developing skills in log analysis and debugging to identify errors and performance issues, and gaining knowledge of security vulnerability assessment within the Android system. By engaging in training sessions, workshops, and hands-on exercises, learners gain theoretical knowledge about Android log retrieval and analysis techniques, as well as practical experience in using Chidroid to retrieve logs, analyze log data, and address system errors and potential security vulnerabilities. Through practical scenarios and examples, learners reinforce their understanding and develop proficiency in log retrieval, analysis, and real-time monitoring using Chidroid.

Assessment

The training tool has been used for

Commercial seminar (up to 2 days)	
Commercial course (up to 2 months)	
Academic Lab (accompanying cybersecurity course) / Academic course	
Cybersecurity exercise /cyber range	X
Cybersecurity hackathon	X
Cybersecurity game	
Certification cybersecurity course	
Specific Cybersecurity Topic(s)	X
Network security control	X
Penetration testing	
Incident response	X
Cloud security	
Risk management	
Forensics	X
Other – write which one	
Demonstration /training to Customer	
Pilot training operation	X

Other (explain in free text):	

If "Other", then respond in free text.

Is this training tool suitable for training purposes (reach the learning objectives and knowledge areas)

Yes	X
No	

Are there any needed compute resources (CPUs, GPU, RAM, Disk space)?

Yes	
No	X

If "Yes", then respond in free text.

What is the level of difficulty to use the training tool?

Easy	
Normal	X
Medium/Standard/Average	
Intermediate	
Hard/Expert/difficult	

Is this training tool easily adaptable to a specific training program?

Potential	X
Most likely	
Neither likely or unlikely	
Least likely	

Is this training tool easily implementable for a specific training program?

Not implementable	
Implementable with minor issues (inconsistencies)	X
Implementable with major issues (inconsistencies)	
Implementable	

Is this training tool easily scalable for a specific training program?

Not scalable	
Scalable with minor issues (inconsistencies)	
Scalable with major issues (inconsistencies)	
Scalable	X

Does this training tool cover interoperability aspects of a specific training program?

Not interoperable	
Interoperable with minor issues (inconsistencies)	
Interoperable with major issues (inconsistencies)	
Interoperable	X

Is this training tool stable while used in a specific training program?

Not stable	
Stable with minor issues (inconsistencies)	X
Stable with major issues (inconsistencies)	
Stable	

Does this training tool support the user's (trainer, trainee) privacy and security aspects?

Yes.	X
No	
Other	

If "Other", then respond in free text

What is the level of prior knowledge needed to use the training tool?

Knowledge of terms	
Knowledge of meanings	
Integration of knowledge	X
Application of knowledge	

Do the trainers/trainees find the training tool easy to use?

Yes	X
No	

Does this training tool support the trainers/trainees’ native language and/or multiple languages?

Yes	
No	X

Appropriateness of the training tool. Tool can be used for:

VG: very good, G: good, NA: not appropriate	VG	G	NA
Commercial seminar (up to 2 days)	X		
Commercial course (up to 2 months)	X		
Academic Lab (accompanying cybersecurity course) / Academic course	X		
Cybersecurity exercise /cyber range	X		
Cybersecurity hackathon	X		
Cybersecurity game		X	
Certification cybersecurity course	X		
Specific Cybersecurity Topic(s)	X		
Network security control		X	
Penetration testing		X	
Incident response	X		
Cloud security	X		
Risk management		X	
Forensics	X		
Other – write which one			

4.3.13 Wazuh

Filled by	Stylianos Karagiannis
Organization	PDMFC
Date	18-07-2023
Contact	stylianos.karagiannis@pdmfc.com
License	O
Cost of license	
Available link to download tool	https://documentation.wazuh.com/current/deployment-options/index.html
Online manual(s)	Available: https://documentation.wazuh.com/current/index.html
Online tutorial(s)	Available free online on Youtube

Description

Summary
Learning about Wazuh entails acquiring knowledge and skills in utilizing the open-source security monitoring and threat detection platform. The learning process focuses on understanding the functionalities, architecture, and core components of Wazuh. Participants gain proficiency in deploying and configuring Wazuh to monitor and analyze logs from various sources, creating and managing detection rules, and performing log analysis to identify security incidents effectively. The learning journey covers cybersecurity knowledge areas such as security monitoring, log analysis, and incident response, and develops skills in Wazuh deployment, log analysis, and rule creation. The learning process for Wazuh involves training sessions, workshops, and hands-on exercises. Participants acquire theoretical knowledge about security monitoring, log analysis techniques, and incident response best practices. Through practical training with Wazuh, learners gain hands-on experience in deploying agents, configuring log sources, creating detection rules, and analyzing log data for effective security monitoring and incident detection. Real-world scenarios and examples further reinforce their understanding and proficiency in utilizing Wazuh for security monitoring, log analysis, and incident response.

Assessment

The training tool has been used for

Commercial seminar (up to 2 days)	
Commercial course (up to 2 months)	
Academic Lab (accompanying cybersecurity course) / Academic course	X
Cybersecurity exercise /cyber range	X
Cybersecurity hackathon	X
Cybersecurity game	X
Certification cybersecurity course	X
Specific Cybersecurity Topic(s)	X
Network security control	X
Penetration testing	X
Incident response	X
Cloud security	X
Risk management	X
Forensics	X
Other – write which one	
Demonstration /training to Customer	
Pilot training operation	

Other (explain in free text):	

If “Other”, then respond in free text.

Is this training tool suitable for training purposes (reach the learning objectives and knowledge areas)

Yes	X
No	

Are there any needed compute resources (CPUs, GPU, RAM, Disk space)?

Yes	X
No	

If “Yes”, then respond in free text.

4-core, 8/16GB RAM, 60/256GB/512 SSD HD space

What is the level of difficulty to use the training tool?

Easy	
Normal	X
Medium/Standard/Average	
Intermediate	
Hard/Expert/difficult	

Is this training tool easily adaptable to a specific training program?

Potential	X
Most likely	
Neither likely or unlikely	
Least likely	

Is this training tool easily implementable for a specific training program?

Not implementable	
Implementable with minor issues (inconsistencies)	
Implementable with major issues (inconsistencies)	
Implementable	X

Is this training tool easily scalable for a specific training program?

Not scalable	
Scalable with minor issues (inconsistencies)	
Scalable with major issues (inconsistencies)	
Scalable	X

Does this training tool cover interoperability aspects of a specific training program?

Not interoperable	
Interoperable with minor issues (inconsistencies)	
Interoperable with major issues (inconsistencies)	
Interoperable	X

Is this training tool stable while used in a specific training program?

Not stable	
Stable with minor issues (inconsistencies)	
Stable with major issues (inconsistencies)	
Stable	X

Does this training tool support the user's (trainer, trainee) privacy and security aspects?

Yes.	X
No	
Other	

If "Other", then respond in free text

What is the level of prior knowledge needed to use the training tool?

Knowledge of terms	
Knowledge of meanings	
Integration of knowledge	X
Application of knowledge	

Do the trainers/trainees find the training tool easy to use?

Yes	X
No	

Does this training tool support the trainers/trainees’ native language and/or multiple languages?

Yes	
No	X

Appropriateness of the training tool. Tool can be used for:

VG: very good, G: good, NA: not appropriate	VG	G	NA
Commercial seminar (up to 2 days)	X		
Commercial course (up to 2 months)	X		
Academic Lab (accompanying cybersecurity course) / Academic course	X		
Cybersecurity exercise /cyber range	X		
Cybersecurity hackathon	X		
Cybersecurity game		X	
Certification cybersecurity course	X		
Specific Cybersecurity Topic(s)	X		
Network security control	X		
Penetration testing		X	
Incident response	X		
Cloud security		X	
Risk management		X	
Forensics	X		
Other – write which one			

4.3.14 Lynis

Filled by	Stylianos Karagiannis
Organization	PDMFC
Date	18-07-2023
Contact	stylianos.karagiannis@pdmfc.com
License	O
Cost of license	
Available link to download tool	https://github.com/CISOfy/lynis
Online manual(s)	Online: https://cisofy.com/documentation/lynis/
Online tutorial(s)	Online (https://adamtheautomator.com/lynis/) and Implementable

Description

Summary
Learning about Lynis involves gaining knowledge and developing skills in utilizing the open-source security auditing tool for Linux and Unix systems. The learning process focuses on understanding the functionalities, features, and capabilities of Lynis to perform system vulnerability assessments, security audits, and configuration checks. Participants acquire proficiency in deploying and configuring Lynis, analyzing system security settings, and identifying potential vulnerabilities and security weaknesses within Linux and Unix environments. The learning goals associated with Lynis include comprehending the purpose and scope of security auditing, understanding the architecture and components of Lynis, and gaining skills in conducting comprehensive system security assessments using the tool. Participants learn to interpret Lynis reports, implement recommended security measures, and strengthen the overall security posture of Linux and Unix systems.

Assessment

The training tool has been used for

Commercial seminar (up to 2 days)	
Commercial course (up to 2 months)	
Academic Lab (accompanying cybersecurity course) / Academic course	X
Cybersecurity exercise /cyber range	X
Cybersecurity hackathon	X
Cybersecurity game	
Certification cybersecurity course	X
Specific Cybersecurity Topic(s)	
Network security control	
Penetration testing	
Incident response	X
Cloud security	X
Risk management	X
Forensics	
Other – write which one	
Demonstration /training to Customer	
Pilot training operation	X

Other (explain in free text):	

If "Other", then respond in free text.

Is this training tool suitable for training purposes (reach the learning objectives and knowledge areas)

Yes	X
No	

Are there any needed compute resources (CPUs, GPU, RAM, Disk space)?

Yes	
No	X

If "Yes", then respond in free text.

What is the level of difficulty to use the training tool?

Easy	X
Normal	
Medium/Standard/Average	
Intermediate	
Hard/Expert/difficult	

Is this training tool easily adaptable to a specific training program?

Potential	X
Most likely	
Neither likely or unlikely	
Least likely	

Is this training tool easily implementable for a specific training program?

Not implementable	
Implementable with minor issues (inconsistencies)	
Implementable with major issues (inconsistencies)	
Implementable	X

Is this training tool easily scalable for a specific training program?

Not scalable	
Scalable with minor issues (inconsistencies)	
Scalable with major issues (inconsistencies)	
Scalable	X

Does this training tool cover interoperability aspects of a specific training program?

Not interoperable	
Interoperable with minor issues (inconsistencies)	
Interoperable with major issues (inconsistencies)	
Interoperable	X

Is this training tool stable while used in a specific training program?

Not stable	
Stable with minor issues (inconsistencies)	
Stable with major issues (inconsistencies)	
Stable	X

Does this training tool support the user’s (trainer, trainee) privacy and security aspects?

Yes.	X
No	
Other	

If “Other”, then respond in free text

What is the level of prior knowledge needed to use the training tool?

Knowledge of terms	
Knowledge of meanings	X
Integration of knowledge	
Application of knowledge	

Do the trainers/trainees find the training tool easy to use?

Yes	X
No	

Does this training tool support the trainers/trainees' native language and/or multiple languages?

Yes	
No	X

Appropriateness of the training tool. Tool can be used for:

VG: very good, G: good, NA: not appropriate	VG	G	NA
Commercial seminar (up to 2 days)	X		
Commercial course (up to 2 months)	X		
Academic Lab (accompanying cybersecurity course) / Academic course	X		
Cybersecurity exercise /cyber range	X		
Cybersecurity hackathon	X		
Cybersecurity game			X
Certification cybersecurity course	X		
Specific Cybersecurity Topic(s)		X	
Network security control			X
Penetration testing			X
Incident response			
Cloud security		X	
Risk management	X		
Forensics			
Other – write which one			

4.3.15 OpenSCAP

Filled by	Stylianos Karagiannis
Organization	PDMFC
Date	18-07-2023
Contact	stylianos.karagiannis@pdmfc.com
License	O
Cost of license	
Available link to download tool	https://github.com/OpenSCAP/openscap
Online manual(s)	https://www.open-scap.org/resources/documentation/
Online tutorial(s)	Online Youtube and blogs (e.g., https://blog.knoldus.com/openscap/)

Description

Summary
Learning about OpenScap involves gaining knowledge and developing skills in utilizing the open-source Security Content Automation Protocol (SCAP) framework for system vulnerability assessments, security compliance checks, and configuration management. The learning process focuses on understanding the functionalities, features, and capabilities of OpenScap to automate security scanning, perform compliance checks against industry standards, and provide remediation guidance. Participants acquire proficiency in deploying and configuring OpenScap, analyzing system security settings, and ensuring compliance with security policies and regulations. The learning goals associated with OpenScap include comprehending the purpose and benefits of security automation frameworks, understanding the architecture and components of OpenScap, and gaining skills in conducting automated vulnerability assessments and security compliance checks using the tool. Participants learn to interpret OpenScap reports, implement recommended configuration changes, and ensure the adherence of systems to security standards and regulations.

Assessment

The training tool has been used for

Commercial seminar (up to 2 days)	
Commercial course (up to 2 months)	
Academic Lab (accompanying cybersecurity course) / Academic course	
Cybersecurity exercise /cyber range	
Cybersecurity hackathon	X
Cybersecurity game	
Certification cybersecurity course	
Specific Cybersecurity Topic(s)	
Network security control	
Penetration testing	
Incident response	
Cloud security	X
Risk management	X
Forensics	
Other – write which one	
Demonstration /training to Customer	
Pilot training operation	

Other (explain in free text):	

If “Other”, then respond in free text.

Is this training tool suitable for training purposes (reach the learning objectives and knowledge areas)

Yes	X
No	

Are there any needed compute resources (CPUs, GPU, RAM, Disk space)?

Yes	
No	X

If “Yes”, then respond in free text.

What is the level of difficulty to use the training tool?

Easy	
Normal	X
Medium/Standard/Average	
Intermediate	
Hard/Expert/difficult	

Is this training tool easily adaptable to a specific training program?

Potential	X
Most likely	
Neither likely or unlikely	
Least likely	

Is this training tool easily implementable for a specific training program?

Not implementable	
Implementable with minor issues (inconsistencies)	
Implementable with major issues (inconsistencies)	
Implementable	X

Is this training tool easily scalable for a specific training program?

Not scalable	
Scalable with minor issues (inconsistencies)	
Scalable with major issues (inconsistencies)	
Scalable	X

Does this training tool cover interoperability aspects of a specific training program?

Not interoperable	
Interoperable with minor issues (inconsistencies)	
Interoperable with major issues (inconsistencies)	
Interoperable	X

Is this training tool stable while used in a specific training program?

Not stable	
Stable with minor issues (inconsistencies)	
Stable with major issues (inconsistencies)	
Stable	X

Does this training tool support the user's (trainer, trainee) privacy and security aspects?

Yes.	X
No	
Other	

If "Other", then respond in free text

What is the level of prior knowledge needed to use the training tool?

Knowledge of terms	
Knowledge of meanings	X
Integration of knowledge	
Application of knowledge	

Do the trainers/trainees find the training tool easy to use?

Yes	X
No	

Does this training tool support the trainers/trainees’ native language and/or multiple languages?

Yes	
No	X

Appropriateness of the training tool. Tool can be used for:

VG: very good, G: good, NA: not appropriate	VG	G	NA
Commercial seminar (up to 2 days)	X		
Commercial course (up to 2 months)	X		
Academic Lab (accompanying cybersecurity course) / Academic course	X		
Cybersecurity exercise /cyber range		X	
Cybersecurity hackathon	X		
Cybersecurity game		X	
Certification cybersecurity course	X		
Specific Cybersecurity Topic(s)		X	
Network security control			X
Penetration testing		X	
Incident response			X
Cloud security	X		
Risk management	X		
Forensics			X
Other – write which one			

4.3.16 MS Modelling Tool

Filled by	Stylianos Karagiannis
Organization	PDMFC
Date	18-07-2023
Contact	stylianos.karagiannis@pdmfc.com
License	O
Cost of license	
Available link to download tool	https://learn.microsoft.com/en-us/azure/security/develop/threat-modeling-tool
Online manual(s)	https://learn.microsoft.com/en-us/azure/security/develop/threat-modeling-tool
Online tutorial(s)	https://learn.microsoft.com/en-us/azure/security/develop/threat-modeling-tool and Online youtube videos

Description

Summary
Learning about the Microsoft Threat Modeling Tool involves gaining knowledge and developing skills in utilizing this software for systematic and structured threat modeling. The learning process focuses on understanding the functionalities, features, and capabilities of the tool to effectively identify potential threats and vulnerabilities in software systems and applications. Participants acquire proficiency in utilizing the Microsoft Threat Modeling Tool to create threat models, analyze risks, and make informed decisions regarding security controls and mitigations. The learning goals associated with the Microsoft Threat Modeling Tool include comprehending the principles and importance of threat modeling, understanding the tool's architecture and components, and gaining skills in creating and analyzing threat models for software systems. Participants learn to identify potential threats, evaluate their impact, and prioritize security controls based on risk assessment. They also acquire knowledge of security best practices and industry standards relevant to threat modeling and software security.

Assessment

The training tool has been used for

Commercial seminar (up to 2 days)	
Commercial course (up to 2 months)	
Academic Lab (accompanying cybersecurity course) / Academic course	X
Cybersecurity exercise /cyber range	
Cybersecurity hackathon	X
Cybersecurity game	
Certification cybersecurity course	
Specific Cybersecurity Topic(s)	X
Network security control	
Penetration testing	
Incident response	
Cloud security	
Risk management	X
Forensics	
Other – write which one	
Demonstration /training to Customer	X
Pilot training operation	X

Other (explain in free text):	

If "Other", then respond in free text.

Is this training tool suitable for training purposes (reach the learning objectives and knowledge areas)

Yes	X
No	

Are there any needed compute resources (CPUs, GPU, RAM, Disk space)?

Yes	
No	X

If "Yes", then respond in free text.

What is the level of difficulty to use the training tool?

Easy	X
Normal	
Medium/Standard/Average	
Intermediate	
Hard/Expert/difficult	

Is this training tool easily adaptable to a specific training program?

Potential	X
Most likely	
Neither likely or unlikely	
Least likely	

Is this training tool easily implementable for a specific training program?

Not implementable	
Implementable with minor issues (inconsistencies)	
Implementable with major issues (inconsistencies)	
Implementable	X

Is this training tool easily scalable for a specific training program?

Not scalable	
Scalable with minor issues (inconsistencies)	
Scalable with major issues (inconsistencies)	
Scalable	X

Does this training tool cover interoperability aspects of a specific training program?

Not interoperable	
Interoperable with minor issues (inconsistencies)	
Interoperable with major issues (inconsistencies)	
Interoperable	X

Is this training tool stable while used in a specific training program?

Not stable	
Stable with minor issues (inconsistencies)	
Stable with major issues (inconsistencies)	
Stable	X

Does this training tool support the user's (trainer, trainee) privacy and security aspects?

Yes.	X
No	
Other	

If "Other", then respond in free text

What is the level of prior knowledge needed to use the training tool?

Knowledge of terms	X
Knowledge of meanings	
Integration of knowledge	
Application of knowledge	

Do the trainers/trainees find the training tool easy to use?

Yes	X
No	

Does this training tool support the trainers/trainees' native language and/or multiple languages?

Yes	
No	X

Appropriateness of the training tool. Tool can be used for:

VG: very good, G: good, NA: not appropriate	VG	G	NA
Commercial seminar (up to 2 days)	X		
Commercial course (up to 2 months)	X		
Academic Lab (accompanying cybersecurity course) / Academic course	X		
Cybersecurity exercise /cyber range			X
Cybersecurity hackathon	X		
Cybersecurity game			
Certification cybersecurity course	X		
Specific Cybersecurity Topic(s)	X		
Network security control		X	
Penetration testing			X
Incident response			X
Cloud security		X	
Risk management	X		
Forensics			X
Other – write which one			

4.3.17 STRIDE

Filled by	Stylianos Karagiannis
Organization	PDMFC
Date	18-07-2023
Contact	stylianos.karagiannis@pdmfc.com
License	O
Cost of license	
Available link to download tool	Methodology
Online manual(s)	https://download.microsoft.com/download/9/3/5/935520EC-D9E2-413E-BEA7-0B865A79B18C/Introduction_to_Threat_Modeling.ppsx
Online tutorial(s)	Available online on PDFs

Description

Summary
Learning about STRIDE from Microsoft involves gaining knowledge and developing skills in utilizing this threat modeling framework to identify and mitigate potential security threats in software systems. The learning process focuses on understanding the six threat categories within STRIDE - Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, and Elevation of Privilege. Participants acquire proficiency in applying the STRIDE framework to analyze software systems, identify vulnerabilities, and make informed decisions regarding security countermeasures. The learning goals associated with STRIDE include comprehending the principles and importance of threat modeling, understanding the six threat categories within STRIDE, and gaining skills in applying STRIDE to analyze and mitigate potential threats. Participants learn to systematically identify possible attack vectors and evaluate their impact on the security of software systems. They also acquire knowledge of security best practices and countermeasures relevant to each STRIDE category.

Assessment

The training tool has been used for

Commercial seminar (up to 2 days)	
Commercial course (up to 2 months)	
Academic Lab (accompanying cybersecurity course) / Academic course	X
Cybersecurity exercise /cyber range	
Cybersecurity hackathon	X
Cybersecurity game	
Certification cybersecurity course	
Specific Cybersecurity Topic(s)	
Network security control	
Penetration testing	
Incident response	
Cloud security	
Risk management	X
Forensics	
Other – write which one	
Demonstration /training to Customer	
Pilot training operation	

Other (explain in free text):	

If “Other”, then respond in free text.

Is this training tool suitable for training purposes (reach the learning objectives and knowledge areas)

Yes	X
No	

Are there any needed compute resources (CPUs, GPU, RAM, Disk space)?

Yes	
No	X

If “Yes”, then respond in free text.

What is the level of difficulty to use the training tool?

Easy	
Normal	X
Medium/Standard/Average	
Intermediate	
Hard/Expert/difficult	

Is this training tool easily adaptable to a specific training program?

Potential	X
Most likely	
Neither likely or unlikely	
Least likely	

Is this training tool easily implementable for a specific training program?

Not implementable	
Implementable with minor issues (inconsistencies)	
Implementable with major issues (inconsistencies)	
Implementable	X

Is this training tool easily scalable for a specific training program?

Not scalable	
Scalable with minor issues (inconsistencies)	
Scalable with major issues (inconsistencies)	
Scalable	X

Does this training tool cover interoperability aspects of a specific training program?

Not interoperable	
Interoperable with minor issues (inconsistencies)	
Interoperable with major issues (inconsistencies)	
Interoperable	X

Is this training tool stable while used in a specific training program?

Not stable	
Stable with minor issues (inconsistencies)	
Stable with major issues (inconsistencies)	
Stable	X

Does this training tool support the user's (trainer, trainee) privacy and security aspects?

Yes.	X
No	
Other	

If "Other", then respond in free text

What is the level of prior knowledge needed to use the training tool?

Knowledge of terms	
Knowledge of meanings	X
Integration of knowledge	
Application of knowledge	

Do the trainers/trainees find the training tool easy to use?

Yes	X
No	

Does this training tool support the trainers/trainees' native language and/or multiple languages?

Yes	
No	X

Appropriateness of the training tool. Tool can be used for:

VG: very good, G: good, NA: not appropriate	VG	G	NA
Commercial seminar (up to 2 days)	X		
Commercial course (up to 2 months)	X		
Academic Lab (accompanying cybersecurity course) / Academic course	X		
Cybersecurity exercise /cyber range		X	
Cybersecurity hackathon	X		
Cybersecurity game	X		
Certification cybersecurity course		X	
Specific Cybersecurity Topic(s)		X	
Network security control			X
Penetration testing			X
Incident response			X
Cloud security		X	
Risk management	X		
Forensics			X
Other – write which one			

4.3.18 LINDDUN

Filled by	Stylianos Karagiannis
Organization	PDMFC
Date	18-07-2023
Contact	stylianos.karagiannis@pdmfc.com
License	O
Cost of license	
Available link to download tool	Methodology
Online manual(s)	https://linddun.org/
Online tutorial(s)	https://linddun.org/

Description

Summary
Learning about LINDDUN (Linkability, Identifiability, Non-repudiation, Detectability, and Unlinkability) involves gaining knowledge and developing skills in assessing and enhancing the privacy and security aspects of systems and applications. The learning process focuses on understanding the LINDDUN framework and its five core principles to evaluate and mitigate potential privacy risks. Participants acquire proficiency in applying the LINDDUN framework to analyze system components, identify linkability and identifiability issues, ensure non-repudiation and detectability, and enhance unlinkability for improved privacy protection. The learning goals associated with LINDDUN include comprehending the principles and significance of privacy protection, understanding the five core principles of the LINDDUN framework, and gaining skills in applying LINDDUN to evaluate and enhance the privacy and security of systems and applications. Participants learn to assess potential privacy risks, identify vulnerabilities, and recommend appropriate measures to ensure privacy protection. They also acquire knowledge of privacy laws, regulations, and best practices relevant to system design and development.

Assessment

The training tool has been used for

Commercial seminar (up to 2 days)	
Commercial course (up to 2 months)	
Academic Lab (accompanying cybersecurity course) / Academic course	X
Cybersecurity exercise /cyber range	
Cybersecurity hackathon	X
Cybersecurity game	
Certification cybersecurity course	X
Specific Cybersecurity Topic(s)	
Network security control	
Penetration testing	
Incident response	
Cloud security	
Risk management	X
Forensics	
Other – write which one	
Demonstration /training to Customer	
Pilot training operation	

Other (explain in free text):	

If "Other", then respond in free text.

Is this training tool suitable for training purposes (reach the learning objectives and knowledge areas)

Yes	X
No	

Are there any needed compute resources (CPUs, GPU, RAM, Disk space)?

Yes	
No	X

If "Yes", then respond in free text.

What is the level of difficulty to use the training tool?

Easy	
Normal	X
Medium/Standard/Average	
Intermediate	
Hard/Expert/difficult	

Is this training tool easily adaptable to a specific training program?

Potential	X
Most likely	
Neither likely or unlikely	
Least likely	

Is this training tool easily implementable for a specific training program?

Not implementable	
Implementable with minor issues (inconsistencies)	
Implementable with major issues (inconsistencies)	
Implementable	X

Is this training tool easily scalable for a specific training program?

Not scalable	
Scalable with minor issues (inconsistencies)	
Scalable with major issues (inconsistencies)	
Scalable	X

Does this training tool cover interoperability aspects of a specific training program?

Not interoperable	
Interoperable with minor issues (inconsistencies)	
Interoperable with major issues (inconsistencies)	
Interoperable	X

Is this training tool stable while used in a specific training program?

Not stable	
Stable with minor issues (inconsistencies)	
Stable with major issues (inconsistencies)	
Stable	X

Does this training tool support the user's (trainer, trainee) privacy and security aspects?

Yes.	X
No	
Other	

If "Other", then respond in free text

What is the level of prior knowledge needed to use the training tool?

Knowledge of terms	X
Knowledge of meanings	
Integration of knowledge	
Application of knowledge	

Do the trainers/trainees find the training tool easy to use?

Yes	X
No	

Does this training tool support the trainers/trainees’ native language and/or multiple languages?

Yes	
No	X

Appropriateness of the training tool. Tool can be used for:

VG: very good, G: good, NA: not appropriate	VG	G	NA
Commercial seminar (up to 2 days)	X		
Commercial course (up to 2 months)	X		
Academic Lab (accompanying cybersecurity course) / Academic course	X		
Cybersecurity exercise /cyber range		X	
Cybersecurity hackathon	X		
Cybersecurity game	X		
Certification cybersecurity course		X	
Specific Cybersecurity Topic(s)		X	
Network security control			X
Penetration testing			X
Incident response			X
Cloud security			X
Risk management	X		
Forensics			X
Other – write which one			

4.3.19 Vulnhub

Filled by	Stylianos Karagiannis
Organization	PDMFC
Date	18-07-2023
Contact	stylianos.karagiannis@pdmfc.com
License	O
Cost of license	
Available link to download tool	https://www.vulnhub.com/
Online manual(s)	https://www.vulnhub.com/
Online tutorial(s)	https://www.vulnhub.com/

Description

Summary
VulnHub is a platform that offers a range of materials and resources to facilitate practical, hands-on experience in the field of digital security, computer applications, and network administration. The learning process with VulnHub focuses on gaining knowledge and developing skills through interactive and immersive exercises. Participants have the opportunity to explore real-world scenarios, work with vulnerable systems and applications, and apply their knowledge in simulated environments to enhance their understanding of cybersecurity concepts and techniques. The learning goals associated with VulnHub include obtaining practical experience in digital security, developing skills in penetration testing and vulnerability assessment, and gaining proficiency in network administration tasks. By utilizing the materials provided by VulnHub, participants can engage in real-world simulations, interact with vulnerable systems, and practice various security techniques and methodologies. This hands-on approach helps learners gain insights into the challenges of securing computer applications and networks, and equips them with the necessary skills to identify vulnerabilities, implement appropriate security controls, and effectively respond to security incidents.

Assessment

The training tool has been used for

Commercial seminar (up to 2 days)	
Commercial course (up to 2 months)	
Academic Lab (accompanying cybersecurity course) / Academic course	X
Cybersecurity exercise /cyber range	X
Cybersecurity hackathon	X
Cybersecurity game	X
Certification cybersecurity course	
Specific Cybersecurity Topic(s)	
Network security control	X
Penetration testing	X
Incident response	X
Cloud security	
Risk management	
Forensics	X
Other – write which one	
Demonstration /training to Customer	
Pilot training operation	

Other (explain in free text):	

If “Other”, then respond in free text.

Is this training tool suitable for training purposes (reach the learning objectives and knowledge areas)

Yes	X
No	

Are there any needed compute resources (CPUs, GPU, RAM, Disk space)?

Yes	X
No	

If “Yes”, then respond in free text.

2-core, 2GB RAM, SSD Disk <40GB

What is the level of difficulty to use the training tool?

Easy	X
Normal	
Medium/Standard/Average	
Intermediate	
Hard/Expert/difficult	

Is this training tool easily adaptable to a specific training program?

Potential	X
Most likely	
Neither likely or unlikely	
Least likely	

Is this training tool easily implementable for a specific training program?

Not implementable	
Implementable with minor issues (inconsistencies)	
Implementable with major issues (inconsistencies)	
Implementable	X

Is this training tool easily scalable for a specific training program?

Not scalable	
Scalable with minor issues (inconsistencies)	
Scalable with major issues (inconsistencies)	
Scalable	X

Does this training tool cover interoperability aspects of a specific training program?

Not interoperable	
Interoperable with minor issues (inconsistencies)	
Interoperable with major issues (inconsistencies)	
Interoperable	X

Is this training tool stable while used in a specific training program?

Not stable	
Stable with minor issues (inconsistencies)	
Stable with major issues (inconsistencies)	
Stable	X

Does this training tool support the user's (trainer, trainee) privacy and security aspects?

Yes.	X
No	
Other	

If "Other", then respond in free text

What is the level of prior knowledge needed to use the training tool?

Knowledge of terms	
Knowledge of meanings	X
Integration of knowledge	
Application of knowledge	

Do the trainers/trainees find the training tool easy to use?

Yes	X
No	

Does this training tool support the trainers/trainees’ native language and/or multiple languages?

Yes	
No	X

Appropriateness of the training tool. Tool can be used for:

VG: very good, G: good, NA: not appropriate	VG	G	NA
Commercial seminar (up to 2 days)	X		
Commercial course (up to 2 months)	X		
Academic Lab (accompanying cybersecurity course) / Academic course	X		
Cybersecurity exercise /cyber range	X		
Cybersecurity hackathon	X		
Cybersecurity game	X		
Certification cybersecurity course		X	
Specific Cybersecurity Topic(s)			
Network security control	X		
Penetration testing	X		
Incident response	X		
Cloud security		X	
Risk management		X	
Forensics		X	
Other – write which one			

4.3.20 CTFd

Filled by	Stylianos Karagiannis
Organization	PDMFC
Date	18-07-2023
Contact	stylianos.karagiannis@pdmfc.com
License	O
Cost of license	
Available link to download tool	https://github.com/CTFd/CTFd
Online manual(s)	https://docs.ctfd.io/
Online tutorial(s)	Online https://docs.ctfd.io/tutorials/getting-started and Youtube

Description

Summary
CTFd, a Capture The Flag framework, provides an accessible and customizable platform for traineess to learn about cybersecurity. By gamifying the learning process, CTFd engages trainees through challenges and puzzles, motivating them to actively participate and solve problems. Trainers can create Capture The Flag events where students compete to find hidden flags, gaining practical knowledge and hands-on experience in various cybersecurity domains. CTFd’s customizability further enhances the learning experience, allowing educators to tailor the platform to their specific objectives and curriculum. With the ability to customize challenges, develop new plugins, and modify existing ones, trainers can create a personalized learning environment that meets the unique needs and skill levels of their trainees. Through CTFd, students can actively engage in cybersecurity learning and develop essential problem-solving skills. In summary, CTFd's gamified approach and customizability make it a valuable tool for cybersecurity education. It enables trainees to actively participate in solving security challenges, fostering practical knowledge and skills. By adapting CTFd to their specific requirements, trainers can create a personalized and engaging learning experience, empowering students to develop a deeper understanding of cybersecurity concepts and problem-solving abilities.

Assessment

The training tool has been used for

Commercial seminar (up to 2 days)	
Commercial course (up to 2 months)	
Academic Lab (accompanying cybersecurity course) / Academic course	X
Cybersecurity exercise /cyber range	X
Cybersecurity hackathon	X
Cybersecurity game	X
Certification cybersecurity course	
Specific Cybersecurity Topic(s)	
Network security control	X
Penetration testing	X
Incident response	X
Cloud security	
Risk management	
Forensics	X
Other – write which one	
Demonstration /training to Customer	
Pilot training operation	

Other (explain in free text):	

If "Other", then respond in free text.

Is this training tool suitable for training purposes (reach the learning objectives and knowledge areas)

Yes	X
No	

Are there any needed compute resources (CPUs, GPU, RAM, Disk space)?

Yes	X
No	

If "Yes", then respond in free text.

4-Core CPU, 4GB RAM, 20GB SSD disk, good network speed on the server side

What is the level of difficulty to use the training tool?

Easy	
Normal	X
Medium/Standard/Average	
Intermediate	
Hard/Expert/difficult	

Is this training tool easily adaptable to a specific training program?

Potential	X
Most likely	
Neither likely or unlikely	
Least likely	

Is this training tool easily implementable for a specific training program?

Not implementable	
Implementable with minor issues (inconsistencies)	
Implementable with major issues (inconsistencies)	
Implementable	X

Is this training tool easily scalable for a specific training program?

Not scalable	
Scalable with minor issues (inconsistencies)	
Scalable with major issues (inconsistencies)	
Scalable	X

Does this training tool cover interoperability aspects of a specific training program?

Not interoperable	
Interoperable with minor issues (inconsistencies)	
Interoperable with major issues (inconsistencies)	
Interoperable	X

Is this training tool stable while used in a specific training program?

Not stable	
Stable with minor issues (inconsistencies)	
Stable with major issues (inconsistencies)	
Stable	X

Does this training tool support the user’s (trainer, trainee) privacy and security aspects?

Yes.	
No	
Other	X

If “Other”, then respond in free text

Participants are encouraged not to put any private data.

What is the level of prior knowledge needed to use the training tool?

Knowledge of terms	
Knowledge of meanings	X
Integration of knowledge	
Application of knowledge	

Do the trainers/trainees find the training tool easy to use?

Yes	X
No	

Does this training tool support the trainers/trainees’ native language and/or multiple languages?

Yes	
No	X

Appropriateness of the training tool. Tool can be used for:

VG: very good, G: good, NA: not appropriate	VG	G	NA
Commercial seminar (up to 2 days)	X		
Commercial course (up to 2 months)	X		
Academic Lab (accompanying cybersecurity course) / Academic course	X		
Cybersecurity exercise /cyber range	X		
Cybersecurity hackathon	X		
Cybersecurity game	X		
Certification cybersecurity course		X	
Specific Cybersecurity Topic(s)		X	
Network security control	X		
Penetration testing	X		
Incident response	X		
Cloud security		X	
Risk management			X
Forensics		X	
Other – write which one			

4.3.21 TryHackMe

Filled by	Stylianos Karagiannis
Organization	PDMFC
Date	18-07-2023
Contact	stylianos.karagiannis@pdmfc.com
License	O/C
Cost of license	Open and commercial pricing plans
Available link to download tool	Online Platform: https://tryhackme.com/
Online manual(s)	https://tryhackme.com/
Online tutorial(s)	https://tryhackme.com/

Description

Summary
TryHackMe is an online platform designed to teach cybersecurity through short, gamified real-world labs. It offers an interactive learning environment that accommodates both beginners and experienced hackers. With a range of content available, TryHackMe provides comprehensive resources, including incorporation guides and challenges, catering to different learning styles. Through its gamified approach, TryHackMe engages students in hands-on cybersecurity exercises, allowing them to apply theoretical knowledge in practical scenarios. By immersing students in real-world labs, they gain practical experience in tackling security challenges, improving their problem-solving abilities. The platform's content caters to learners at various skill levels, ensuring that beginners can grasp foundational concepts while seasoned hackers can further enhance their expertise. TryHackMe's incorporation guides and challenges provide structured learning paths, enabling students to progress systematically and gain a deeper understanding of cybersecurity concepts. Any information about (i) the learning process and/or (ii) technical aspects

Assessment

The training tool has been used for

Commercial seminar (up to 2 days)	
Commercial course (up to 2 months)	
Academic Lab (accompanying cybersecurity course) / Academic course	X
Cybersecurity exercise /cyber range	X
Cybersecurity hackathon	X
Cybersecurity game	
Certification cybersecurity course	
Specific Cybersecurity Topic(s)	
Network security control	
Penetration testing	
Incident response	
Cloud security	
Risk management	
Forensics	
Other – write which one	
Demonstration /training to Customer	
Pilot training operation	

Other (explain in free text):	

If “Other”, then respond in free text.

Is this training tool suitable for training purposes (reach the learning objectives and knowledge areas)

Yes	X
No	

Are there any needed compute resources (CPUs, GPU, RAM, Disk space)?

Yes	
No	X

If “Yes”, then respond in free text.

What is the level of difficulty to use the training tool?

Easy	
Normal	X
Medium/Standard/Average	
Intermediate	
Hard/Expert/difficult	

Is this training tool easily adaptable to a specific training program?

Potential	X
Most likely	
Neither likely or unlikely	
Least likely	

Is this training tool easily implementable for a specific training program?

Not implementable	
Implementable with minor issues (inconsistencies)	
Implementable with major issues (inconsistencies)	
Implementable	X

Is this training tool easily scalable for a specific training program?

Not scalable	
Scalable with minor issues (inconsistencies)	
Scalable with major issues (inconsistencies)	
Scalable	X

Does this training tool cover interoperability aspects of a specific training program?

Not interoperable	

Interoperable with minor issues (inconsistencies)	
Interoperable with major issues (inconsistencies)	
Interoperable	X

Is this training tool stable while used in a specific training program?

Not stable	
Stable with minor issues (inconsistencies)	
Stable with major issues (inconsistencies)	
Stable	X

Does this training tool support the user's (trainer, trainee) privacy and security aspects?

Yes.	X
No	
Other	

If "Other", then respond in free text

What is the level of prior knowledge needed to use the training tool?

Knowledge of terms	X

Knowledge of meanings	
Integration of knowledge	
Application of knowledge	

Do the trainers/trainees find the training tool easy to use?

Yes	X
No	

Does this training tool support the trainers/trainees’ native language and/or multiple languages?

Yes	
No	X

Appropriateness of the training tool. Tool can be used for:

VG: very good, G: good, NA: not appropriate	VG	G	NA
Commercial seminar (up to 2 days)	X		
Commercial course (up to 2 months)	X		
Academic Lab (accompanying cybersecurity course) / Academic course	X		
Cybersecurity exercise /cyber range	X		
Cybersecurity hackathon	X		
Cybersecurity game	X		
Certification cybersecurity course	X		
Specific Cybersecurity Topic(s)		X	
Network security control	X		
Penetration testing	X		
Incident response	X		
Cloud security	X		
Risk management		X	
Forensics		X	
Other – write which one			

4.3.22 CyberDefenders

Filled by	Stylianos Karagiannis
Organization	PDMFC
Date	18-07-2023
Contact	stylianos.karagiannis@pdmfc.com
License	O with C plan
Cost of license	
Available link to download tool	https://cyberdefenders.org/
Online manual(s)	https://cyberdefenders.org/
Online tutorial(s)	https://cyberdefenders.org/ and Youtube or online writeups

Description

Summary
CyberDefenders is a specialized blue team training platform that places a strong emphasis on the defensive aspects of cybersecurity. It provides a comprehensive environment for individuals to learn, validate, and advance their CyberDefense skills. By focusing on the defensive side of cybersecurity, CyberDefenders equips learners with the knowledge and tools to protect systems and networks against potential threats. The platform offers a wide range of training resources and hands-on exercises that enable individuals to gain practical experience in defending against cyber-attacks. Through interactive labs and simulations, users can apply defensive techniques, monitor network traffic, and detect and respond to security incidents. With CyberDefenders, learners can validate their skills by tackling real-world scenarios and honing their abilities to protect digital assets effectively. The platform's specialized focus on blue team training ensures that individuals are well-prepared to address the evolving cybersecurity challenges faced by organizations today.

Assessment

The training tool has been used for

Commercial seminar (up to 2 days)	
Commercial course (up to 2 months)	
Academic Lab (accompanying cybersecurity course) / Academic course	
Cybersecurity exercise /cyber range	
Cybersecurity hackathon	X
Cybersecurity game	
Certification cybersecurity course	
Specific Cybersecurity Topic(s)	
Network security control	
Penetration testing	
Incident response	
Cloud security	
Risk management	
Forensics	
Other – write which one	
Demonstration /training to Customer	
Pilot training operation	
Other (explain in free text):	

If "Other", then respond in free text.

Is this training tool suitable for training purposes (reach the learning objectives and knowledge areas)

Yes	X
No	

Are there any needed compute resources (CPUs, GPU, RAM, Disk space)?

Yes	
No	X

If "Yes", then respond in free text.

What is the level of difficulty to use the training tool?

Easy	
Normal	X
Medium/Standard/Average	
Intermediate	
Hard/Expert/difficult	

Is this training tool easily adaptable to a specific training program?

Potential	X

Most likely	
Neither likely or unlikely	
Least likely	

Is this training tool easily implementable for a specific training program?

Not implementable	
Implementable with minor issues (inconsistencies)	
Implementable with major issues (inconsistencies)	
Implementable	X

Is this training tool easily scalable for a specific training program?

Not scalable	
Scalable with minor issues (inconsistencies)	
Scalable with major issues (inconsistencies)	
Scalable	X

Does this training tool cover interoperability aspects of a specific training program?

Not interoperable	

Interoperable with minor issues (inconsistencies)	
Interoperable with major issues (inconsistencies)	
Interoperable	X

Is this training tool stable while used in a specific training program?

Not stable	
Stable with minor issues (inconsistencies)	
Stable with major issues (inconsistencies)	
Stable	X

Does this training tool support the user’s (trainer, trainee) privacy and security aspects?

Yes.	X
No	
Other	

If “Other”, then respond in free text

What is the level of prior knowledge needed to use the training tool?

Knowledge of terms	

Knowledge of meanings	X
Integration of knowledge	
Application of knowledge	

Do the trainers/trainees find the training tool easy to use?

Yes	X
No	

Does this training tool support the trainers/trainees' native language and/or multiple languages?

Yes	
No	X

Appropriateness of the training tool. Tool can be used for:

VG: very good, G: good, NA: not appropriate	VG	G	NA
Commercial seminar (up to 2 days)	X		
Commercial course (up to 2 months)	X		
Academic Lab (accompanying cybersecurity course) / Academic course	X		
Cybersecurity exercise /cyber range	X		
Cybersecurity hackathon	X		
Cybersecurity game		X	
Certification cybersecurity course	X		
Specific Cybersecurity Topic(s)		X	
Network security control	X		
Penetration testing		X	
Incident response	X		
Cloud security	X		
Risk management			X
Forensics	X		
Other – write which one			

4.3.23 Tshark

Filled by	Stylianos Karagiannis
Organization	PDMFC
Date	18-07-2023
Contact	stylianos.karagiannis@pdmfc.com
License	O
Cost of license	
Available link to download tool	https://linux.die.net/man/1/tshark
Online manual(s)	https://www.wireshark.org/docs/man-pages/tshark.html
Online tutorial(s)	Online on Youtube

Description

Summary
TShark is a powerful network protocol analyzer that provides users with the ability to capture and analyze packet data from live networks or saved capture files. With TShark, individuals can gain deep insights into network traffic, decoding packets, and analyzing network protocols. The tool offers flexibility in displaying the decoded form of packets to the standard output or writing them to a file for further analysis. TShark's live packet capturing capability allows users to monitor and capture network traffic in real-time. By examining the captured packets, individuals can analyze network behavior, identify potential security vulnerabilities, and troubleshoot network issues. Additionally, TShark supports the reading of previously saved capture files, enabling users to analyze packet data offline and conduct in-depth investigations into network incidents.

Assessment

The training tool has been used for

Commercial seminar (up to 2 days)	
Commercial course (up to 2 months)	
Academic Lab (accompanying cybersecurity course) / Academic course	X
Cybersecurity exercise /cyber range	
Cybersecurity hackathon	X
Cybersecurity game	
Certification cybersecurity course	
Specific Cybersecurity Topic(s)	
Network security control	
Penetration testing	
Incident response	
Cloud security	
Risk management	
Forensics	
Other – write which one	
Demonstration /training to Customer	
Pilot training operation	X

Other (explain in free text):	

If “Other”, then respond in free text.

Is this training tool suitable for training purposes (reach the learning objectives and knowledge areas)

Yes	X
No	

Are there any needed compute resources (CPUs, GPU, RAM, Disk space)?

Yes	
No	X

If “Yes”, then respond in free text.

What is the level of difficulty to use the training tool?

Easy	
Normal	X
Medium/Standard/Average	
Intermediate	
Hard/Expert/difficult	

Is this training tool easily adaptable to a specific training program?

Potential	X
Most likely	
Neither likely or unlikely	
Least likely	

Is this training tool easily implementable for a specific training program?

Not implementable	
Implementable with minor issues (inconsistencies)	
Implementable with major issues (inconsistencies)	
Implementable	X

Is this training tool easily scalable for a specific training program?

Not scalable	
Scalable with minor issues (inconsistencies)	
Scalable with major issues (inconsistencies)	
Scalable	X

Does this training tool cover interoperability aspects of a specific training program?

Not interoperable	

Interoperable with minor issues (inconsistencies)	
Interoperable with major issues (inconsistencies)	
Interoperable	X

Is this training tool stable while used in a specific training program?

Not stable	
Stable with minor issues (inconsistencies)	
Stable with major issues (inconsistencies)	
Stable	X

Does this training tool support the user’s (trainer, trainee) privacy and security aspects?

Yes.	X
No	
Other	

If “Other”, then respond in free text

What is the level of prior knowledge needed to use the training tool?

Knowledge of terms	

Knowledge of meanings	X
Integration of knowledge	
Application of knowledge	

Do the trainers/trainees find the training tool easy to use?

Yes	X
No	

Does this training tool support the trainers/trainees’ native language and/or multiple languages?

Yes	
No	X

Appropriateness of the training tool. Tool can be used for:

VG: very good, G: good, NA: not appropriate	VG	G	NA
Commercial seminar (up to 2 days)	X		
Commercial course (up to 2 months)	X		
Academic Lab (accompanying cybersecurity course) / Academic course	X		
Cybersecurity exercise /cyber range	X		
Cybersecurity hackathon	X		
Cybersecurity game			X
Certification cybersecurity course		X	
Specific Cybersecurity Topic(s)			X
Network security control	X		
Penetration testing		X	
Incident response		X	
Cloud security			X
Risk management			X
Forensics	X		
Other – write which one			

4.3.24 NFStream

Filled by	Stylianos Karagiannis
Organization	PDMFC
Date	18-07-2023
Contact	stylianos.karagiannis@pdmfc.com
License	O
Cost of license	
Available link to download tool	if “O” then provide link (url); if “C” then provide link(s) (url) for trial version; other
Online manual(s)	Available – provide link; if not available online, then attach a publicly available manual for the commercial tool (proprietary technology)
Online tutorial(s)	Available – provide link; (e.g. YouTube video(s))

Description

Summary
Nfstream is a Python package that offers a fast, flexible, and intuitive approach to working with network data, whether it is online or offline. With a focus on practical and real-world network data analysis, nfstream provides users with powerful data structures that simplify the process of handling and analyzing network data in Python. The package aims to be the foundational high-level building block for network data analysis, enabling users to process and analyze network traffic efficiently. nfstream's data structures are designed to be easy to use and understand, allowing users to extract valuable insights from network data without getting lost in complex implementation details. By leveraging nfstream, individuals can perform a wide range of network analysis tasks, including traffic monitoring, flow analysis, threat detection, and anomaly detection.

Assessment

The training tool has been used for

Commercial seminar (up to 2 days)	
Commercial course (up to 2 months)	
Academic Lab (accompanying cybersecurity course) / Academic course	
Cybersecurity exercise /cyber range	
Cybersecurity hackathon	
Cybersecurity game	
Certification cybersecurity course	
Specific Cybersecurity Topic(s)	
Network security control	
Penetration testing	
Incident response	
Cloud security	
Risk management	
Forensics	
Other – write which one	
Demonstration /training to Customer	
Pilot training operation	X

Other (explain in free text):	

If “Other”, then respond in free text.

Is this training tool suitable for training purposes (reach the learning objectives and knowledge areas)

Yes	X
No	

Are there any needed compute resources (CPUs, GPU, RAM, Disk space)?

Yes	
No	X

If “Yes”, then respond in free text.

What is the level of difficulty to use the training tool?

Easy	
Normal	
Medium/Standard/Average	X
Intermediate	
Hard/Expert/difficult	

Is this training tool easily adaptable to a specific training program?

Potential	X
Most likely	
Neither likely or unlikely	
Least likely	

Is this training tool easily implementable for a specific training program?

Not implementable	
Implementable with minor issues (inconsistencies)	
Implementable with major issues (inconsistencies)	
Implementable	X

Is this training tool easily scalable for a specific training program?

Not scalable	
Scalable with minor issues (inconsistencies)	
Scalable with major issues (inconsistencies)	
Scalable	X

Does this training tool cover interoperability aspects of a specific training program?

Not interoperable	
Interoperable with minor issues (inconsistencies)	
Interoperable with major issues (inconsistencies)	
Interoperable	X

Is this training tool stable while used in a specific training program?

Not stable	
Stable with minor issues (inconsistencies)	
Stable with major issues (inconsistencies)	
Stable	X

Does this training tool support the user's (trainer, trainee) privacy and security aspects?

Yes.	X
No	
Other	

If "Other", then respond in free text

What is the level of prior knowledge needed to use the training tool?

Knowledge of terms	
Knowledge of meanings	X
Integration of knowledge	
Application of knowledge	

Do the trainers/trainees find the training tool easy to use?

Yes	X
No	

Does this training tool support the trainers/trainees’ native language and/or multiple languages?

Yes	
No	X

Appropriateness of the training tool. Tool can be used for:

VG: very good, G: good, NA: not appropriate	VG	G	NA
Commercial seminar (up to 2 days)	X		
Commercial course (up to 2 months)	X		
Academic Lab (accompanying cybersecurity course) / Academic course	X		
Cybersecurity exercise /cyber range	X		
Cybersecurity hackathon	X		
Cybersecurity game		X	
Certification cybersecurity course		X	
Specific Cybersecurity Topic(s)		X	
Network security control		X	
Penetration testing		X	
Incident response	X		
Cloud security		X	
Risk management		X	
Forensics	X		
Other – write which one			

4.3.25 GPG

Filled by	Stylianos Karagiannis
Organization	PDMFC
Date	18-07-2023
Contact	stylianos.karagiannis@pdmfc.com
License	O
Cost of license	
Available link to download tool	https://gnupg.org/
Online manual(s)	https://www.gnupg.org/documentation/manuals.html
Online tutorial(s)	Online Youtube, blogs (e.g., https://www.devdungeon.com/content/gpg-tutorial)

Description

Summary
The GNU Privacy Guard (GPG or gpg) tool is a crucial security tool used for encrypting files. As part of the GNU Privacy Guard (GnuPG) suite, GPG implements the OpenPGP (Pretty Good Privacy) standard, which is widely recognized and adopted for secure communication and file encryption. By learning and utilizing GPG, individuals can enhance their understanding of file encryption techniques and strengthen their ability to protect sensitive information. With GPG, individuals can encrypt files and messages using strong cryptographic algorithms, ensuring that the content remains confidential and secure. By leveraging GPG's capabilities, learners can explore the principles and practices of encryption, including key management, digital signatures, and secure communication protocols. Through hands-on experience with GPG, individuals can gain a deeper understanding of data privacy and develop the skills necessary to implement secure file transfer and communication protocols.

Assessment

The training tool has been used for

Commercial seminar (up to 2 days)	
Commercial course (up to 2 months)	
Academic Lab (accompanying cybersecurity course) / Academic course	X
Cybersecurity exercise /cyber range	
Cybersecurity hackathon	X
Cybersecurity game	
Certification cybersecurity course	
Specific Cybersecurity Topic(s)	
Network security control	
Penetration testing	
Incident response	
Cloud security	
Risk management	
Forensics	
Other – write which one	
Demonstration /training to Customer	
Pilot training operation	

Other (explain in free text):	

If “Other”, then respond in free text.

Is this training tool suitable for training purposes (reach the learning objectives and knowledge areas)

Yes	X
No	

Are there any needed compute resources (CPUs, GPU, RAM, Disk space)?

Yes	
No	X

If “Yes”, then respond in free text.

What is the level of difficulty to use the training tool?

Easy	
Normal	X
Medium/Standard/Average	
Intermediate	
Hard/Expert/difficult	

Is this training tool easily adaptable to a specific training program?

Potential	X
Most likely	
Neither likely or unlikely	
Least likely	

Is this training tool easily implementable for a specific training program?

Not implementable	
Implementable with minor issues (inconsistencies)	
Implementable with major issues (inconsistencies)	
Implementable	X

Is this training tool easily scalable for a specific training program?

Not scalable	
Scalable with minor issues (inconsistencies)	
Scalable with major issues (inconsistencies)	
Scalable	X

Does this training tool cover interoperability aspects of a specific training program?

Not interoperable	

Interoperable with minor issues (inconsistencies)	
Interoperable with major issues (inconsistencies)	
Interoperable	X

Is this training tool stable while used in a specific training program?

Not stable	
Stable with minor issues (inconsistencies)	
Stable with major issues (inconsistencies)	
Stable	X

Does this training tool support the user’s (trainer, trainee) privacy and security aspects?

Yes.	X
No	
Other	

If “Other”, then respond in free text

What is the level of prior knowledge needed to use the training tool?

Knowledge of terms	

Knowledge of meanings	X
Integration of knowledge	
Application of knowledge	

Do the trainers/trainees find the training tool easy to use?

Yes	X
No	

Does this training tool support the trainers/trainees’ native language and/or multiple languages?

Yes	
No	X

Appropriateness of the training tool. Tool can be used for:

VG: very good, G: good, NA: not appropriate	VG	G	NA
Commercial seminar (up to 2 days)	X		
Commercial course (up to 2 months)	X		
Academic Lab (accompanying cybersecurity course) / Academic course	X		
Cybersecurity exercise /cyber range	X		
Cybersecurity hackathon	X		
Cybersecurity game			X
Certification cybersecurity course	X		
Specific Cybersecurity Topic(s)		X	
Network security control		X	
Penetration testing			X
Incident response			X
Cloud security		X	
Risk management			X
Forensics		X	
Other – write which one			

4.3.26 OpenSSL

Filled by	Stylianos Karagiannis
Organization	PDMFC
Date	18-07-2023
Contact	stylianos.karagiannis@pdmfc.com
License	O
Cost of license	
Available link to download tool	https://www.openssl.org/
Online manual(s)	https://www.openssl.org/docs/
Online tutorial(s)	Online free material from universities, blogs and Youtube (e.g., https://www.cs.toronto.edu/~arnold/427/19s/427_19S/tool/ssl/notes.pdf)

Description

Summary
OpenSSL is a powerful open-source command line tool that provides a wide range of functionalities related to SSL/TLS certificates and encryption. By learning and utilizing OpenSSL, individuals can gain a comprehensive understanding of certificate management, cryptographic operations, and secure communication protocols. This tool serves as a valuable resource for those working with SSL/TLS certificates and cryptographic operations. With OpenSSL, individuals can generate private keys, create Certificate Signing Requests (CSRs), and install SSL/TLS certificates on various platforms. By leveraging the tool's commands, learners can navigate the complex landscape of SSL/TLS certificate management and gain practical experience in securing network connections. Additionally, OpenSSL allows individuals to identify and retrieve information about certificates, facilitating certificate validation and troubleshooting.

Assessment

The training tool has been used for

Commercial seminar (up to 2 days)	
Commercial course (up to 2 months)	
Academic Lab (accompanying cybersecurity course) / Academic course	X
Cybersecurity exercise /cyber range	X
Cybersecurity hackathon	X
Cybersecurity game	
Certification cybersecurity course	
Specific Cybersecurity Topic(s)	
Network security control	
Penetration testing	
Incident response	
Cloud security	
Risk management	
Forensics	
Other – write which one	
Demonstration /training to Customer	
Pilot training operation	

Other (explain in free text):	

If “Other”, then respond in free text.

Is this training tool suitable for training purposes (reach the learning objectives and knowledge areas)

Yes	X
No	

Are there any needed compute resources (CPUs, GPU, RAM, Disk space)?

Yes	
No	X

If “Yes”, then respond in free text.

What is the level of difficulty to use the training tool?

Easy	
Normal	X
Medium/Standard/Average	
Intermediate	
Hard/Expert/difficult	

Is this training tool easily adaptable to a specific training program?

Potential	X
Most likely	
Neither likely or unlikely	
Least likely	

Is this training tool easily implementable for a specific training program?

Not implementable	
Implementable with minor issues (inconsistencies)	
Implementable with major issues (inconsistencies)	
Implementable	X

Is this training tool easily scalable for a specific training program?

Not scalable	
Scalable with minor issues (inconsistencies)	
Scalable with major issues (inconsistencies)	
Scalable	X

Does this training tool cover interoperability aspects of a specific training program?

Not interoperable	
Interoperable with minor issues (inconsistencies)	
Interoperable with major issues (inconsistencies)	
Interoperable	X

Is this training tool stable while used in a specific training program?

Not stable	
Stable with minor issues (inconsistencies)	
Stable with major issues (inconsistencies)	
Stable	X

Does this training tool support the user's (trainer, trainee) privacy and security aspects?

Yes.	X
No	
Other	

If "Other", then respond in free text

What is the level of prior knowledge needed to use the training tool?

Knowledge of terms	
Knowledge of meanings	X
Integration of knowledge	
Application of knowledge	

Do the trainers/trainees find the training tool easy to use?

Yes	X
No	

Does this training tool support the trainers/trainees' native language and/or multiple languages?

Yes	
No	X

Appropriateness of the training tool. Tool can be used for:

VG: very good, G: good, NA: not appropriate	VG	G	NA
Commercial seminar (up to 2 days)	X		
Commercial course (up to 2 months)	X		
Academic Lab (accompanying cybersecurity course) / Academic course	X		
Cybersecurity exercise /cyber range		X	
Cybersecurity hackathon	X		
Cybersecurity game		X	
Certification cybersecurity course		X	
Specific Cybersecurity Topic(s)			X
Network security control		X	
Penetration testing			X
Incident response			X
Cloud security			X
Risk management			X
Forensics			X
Other – write which one			

4.3.27 YARA

Filled by	Stylianos Karagiannis
Organization	PDMFC
Date	18-07-2023
Contact	stylianos.karagiannis@pdmfc.com
License	O
Cost of license	
Available link to download tool	https://github.com/VirusTotal/yara
Online manual(s)	https://yara.readthedocs.io/en/stable/
Online tutorial(s)	Youtube, blogs and online free tutorials (e.g., https://www.varonis.com/blog/yara-rules)

Description

Summary
YARA rules serve as a fundamental element of YARA, a powerful tool used in malware research and detection. These rules are used to define the attributes and patterns that characterize specific types or classifications of malware. By learning and utilizing YARA rules, individuals can effectively identify and scan files or memory to determine if they exhibit indicators of the specified malware characteristics. With YARA, learners can gain insights into the inner workings of malware by understanding its unique patterns, signatures, or behaviors. By creating and customizing YARA rules, individuals can define and specify the characteristics of different malware strains, enabling them to detect and analyze specific types of malicious software. YARA rules provide a flexible and comprehensive approach to malware detection, empowering users to stay one step ahead of evolving cyber threats.

Assessment

The training tool has been used for

Commercial seminar (up to 2 days)	
Commercial course (up to 2 months)	
Academic Lab (accompanying cybersecurity course) / Academic course	X
Cybersecurity exercise /cyber range	
Cybersecurity hackathon	
Cybersecurity game	
Certification cybersecurity course	
Specific Cybersecurity Topic(s)	
Network security control	
Penetration testing	
Incident response	
Cloud security	
Risk management	
Forensics	
Other – write which one	
Demonstration /training to Customer	
Pilot training operation	

Other (explain in free text):	

If “Other”, then respond in free text.

Is this training tool suitable for training purposes (reach the learning objectives and knowledge areas)

Yes	X
No	

Are there any needed compute resources (CPUs, GPU, RAM, Disk space)?

Yes	
No	X

If “Yes”, then respond in free text.

What is the level of difficulty to use the training tool?

Easy	
Normal	X
Medium/Standard/Average	
Intermediate	
Hard/Expert/difficult	

Is this training tool easily adaptable to a specific training program?

Potential	X
Most likely	
Neither likely or unlikely	
Least likely	

Is this training tool easily implementable for a specific training program?

Not implementable	
Implementable with minor issues (inconsistencies)	
Implementable with major issues (inconsistencies)	
Implementable	X

Is this training tool easily scalable for a specific training program?

Not scalable	
Scalable with minor issues (inconsistencies)	
Scalable with major issues (inconsistencies)	
Scalable	X

Does this training tool cover interoperability aspects of a specific training program?

Not interoperable	
Interoperable with minor issues (inconsistencies)	
Interoperable with major issues (inconsistencies)	
Interoperable	X

Is this training tool stable while used in a specific training program?

Not stable	
Stable with minor issues (inconsistencies)	
Stable with major issues (inconsistencies)	
Stable	X

Does this training tool support the user's (trainer, trainee) privacy and security aspects?

Yes.	X
No	
Other	

If "Other", then respond in free text

What is the level of prior knowledge needed to use the training tool?

Knowledge of terms	
Knowledge of meanings	X
Integration of knowledge	
Application of knowledge	

Do the trainers/trainees find the training tool easy to use?

Yes	X
No	

Does this training tool support the trainers/trainees’ native language and/or multiple languages?

Yes	
No	X

Appropriateness of the training tool. Tool can be used for:

VG: very good, G: good, NA: not appropriate	VG	G	NA
Commercial seminar (up to 2 days)	X		
Commercial course (up to 2 months)	X		
Academic Lab (accompanying cybersecurity course) / Academic course	X		
Cybersecurity exercise /cyber range	X		
Cybersecurity hackathon	X		
Cybersecurity game		X	
Certification cybersecurity course	X		
Specific Cybersecurity Topic(s)		X	
Network security control		X	
Penetration testing		X	
Incident response		X	
Cloud security		X	
Risk management			X
Forensics	X		
Other – write which one			
Other – write which one			

4.3.28 OpenCTI

Filled by	Stylianos Karagiannis
Organization	PDMFC
Date	18-07-2023
Contact	skaragiannis.karagiannis@pdmfc.com
License	O
Cost of license	if not “O”
Available link to download tool	if “O” then provide link (url); if “C” then provide link(s) (url) for trial version; other
Online manual(s)	Available – provide link; if not available online, then attach a publicly available manual for the commercial tool (proprietary technology)
Online tutorial(s)	Available – provide link; (e.g. YouTube video(s))

Description

Summary
OpenCTI is a powerful open-source platform designed for cyber threat intelligence analysis and management. As a Threat Intelligence Platform (TIP), OpenCTI offers a range of functionalities that facilitate knowledge management, data visualization, and contextualization of observables and indicators. By utilizing OpenCTI, individuals can structure and analyze data according to the STIX2 (Structured Threat Information Expression) standard, which enables interoperability and standardized representation of cyber threat information. With OpenCTI, learners can establish a centralized knowledge management database that aggregates and organizes various sources of threat intelligence. The platform enables the storage and analysis of diverse data types, including indicators, observables, reports, and relationships, allowing for a comprehensive understanding of cyber threats. OpenCTI's data visualization capabilities enhance the interpretation and analysis of threat intelligence data, enabling users to identify patterns, correlations, and potential threat actors or campaigns.

Assessment

The training tool has been used for

Commercial seminar (up to 2 days)	
Commercial course (up to 2 months)	
Academic Lab (accompanying cybersecurity course) / Academic course	X
Cybersecurity exercise /cyber range	
Cybersecurity hackathon	
Cybersecurity game	
Certification cybersecurity course	
Specific Cybersecurity Topic(s)	
Network security control	
Penetration testing	
Incident response	
Cloud security	
Risk management	
Forensics	
Other – write which one	
Demonstration /training to Customer	
Pilot training operation	

Other (explain in free text):	

If “Other”, then respond in free text.

Is this training tool suitable for training purposes (reach the learning objectives and knowledge areas)

Yes	X
No	

Are there any needed compute resources (CPUs, GPU, RAM, Disk space)?

Yes	X
No	

If “Yes”, then respond in free text.

6 Cores, 16GiB, >32GB SSD

Wat is the level of difficulty to use the training tool?

Easy	
Normal	X
Medium/Standard/Average	
Intermediate	
Hard/Expert/difficult	

Is this training tool easily adaptable to a specific training program?

Potential	X
Most likely	
Neither likely or unlikely	
Least likely	

Is this training tool easily implementable for a specific training program?

Not implementable	
Implementable with minor issues (inconsistencies)	
Implementable with major issues (inconsistencies)	
Implementable	X

Is this training tool easily scalable for a specific training program?

Not scalable	
Scalable with minor issues (inconsistencies)	
Scalable with major issues (inconsistencies)	
Scalable	X

Does this training tool cover interoperability aspects of a specific training program?

Not interoperable	
Interoperable with minor issues (inconsistencies)	
Interoperable with major issues (inconsistencies)	
Interoperable	X

Is this training tool stable while used in a specific training program?

Not stable	
Stable with minor issues (inconsistencies)	
Stable with major issues (inconsistencies)	
Stable	X

Does this training tool support the user's (trainer, trainee) privacy and security aspects?

Yes.	X
No	
Other	

If "Other", then respond in free text

What is the level of prior knowledge needed to use the training tool?

Knowledge of terms	
Knowledge of meanings	X
Integration of knowledge	
Application of knowledge	

Do the trainers/trainees find the training tool easy to use?

Yes	X
No	

Does this training tool support the trainers/trainees' native language and/or multiple languages?

Yes	
No	X

Appropriateness of the training tool. Tool can be used for:

VG: very good, G: good, NA: not appropriate	VG	G	NA
Commercial seminar (up to 2 days)	X		
Commercial course (up to 2 months)	X		
Academic Lab (accompanying cybersecurity course) / Academic course	X		
Cybersecurity exercise /cyber range	X		
Cybersecurity hackathon	X		
Cybersecurity game		X	
Certification cybersecurity course	X		
Specific Cybersecurity Topic(s)		X	
Network security control		X	
Penetration testing			X
Incident response		X	
Cloud security			X
Risk management			X
Forensics		X	

4.3.29 MISP

Filled by	Stylianos Karagiannis
Organization	PDMFC
Date	18-07-2023
Contact	stylianos.karagiannis@pdmfc.com
License	O
Cost of license	
Available link to download tool	https://github.com/MISP/MISP
Online manual(s)	https://www.misp-project.org/documentation/
Online tutorial(s)	https://www.circl.lu/doc/misp/ and available free on youtube and blogs

Description

Summary
MISP, which stands for Malware Information Sharing Platform and Threat Sharing, is a comprehensive platform designed to facilitate the sharing and analysis of Indicators of Compromise (IOCs) and intelligence related to malware and security incidents. At its core, MISP provides an efficient database for storing both technical and non-technical information about malware samples, incidents, attackers, and intelligence. By learning and utilizing MISP, individuals can enhance their capabilities in threat intelligence analysis, collaboration, and incident response. MISP serves as a centralized repository for storing and managing IOCs, allowing users to store and access valuable information related to malware and security incidents. It enables the collection and sharing of technical data such as hashes, network indicators, and behavioral patterns, as well as non-technical information like incident reports, threat actor profiles, and contextual details. This holistic approach to information sharing empowers organizations to collectively analyze and respond to emerging threats, enabling more effective and proactive defense measures.

Assessment

The training tool has been used for

Commercial seminar (up to 2 days)	
Commercial course (up to 2 months)	
Academic Lab (accompanying cybersecurity course) / Academic course	
Cybersecurity exercise /cyber range	
Cybersecurity hackathon	X
Cybersecurity game	
Certification cybersecurity course	
Specific Cybersecurity Topic(s)	
Network security control	
Penetration testing	
Incident response	
Cloud security	
Risk management	
Forensics	
Other – write which one	
Demonstration /training to Customer	
Pilot training operation	

Other (explain in free text):	

If “Other”, then respond in free text.

Is this training tool suitable for training purposes (reach the learning objectives and knowledge areas)

Yes	X
No	

Are there any needed compute resources (CPUs, GPU, RAM, Disk space)?

Yes	X2
No	

If “Yes”, then respond in free text.

2/4 Cores, 8GB RAM, 40GB SSD

What is the level of difficulty to use the training tool?

Easy	
Normal	X
Medium/Standard/Average	
Intermediate	
Hard/Expert/difficult	

Is this training tool easily adaptable to a specific training program?

Potential	X
Most likely	
Neither likely or unlikely	
Least likely	

Is this training tool easily implementable for a specific training program?

Not implementable	
Implementable with minor issues (inconsistencies)	
Implementable with major issues (inconsistencies)	
Implementable	X

Is this training tool easily scalable for a specific training program?

Not scalable	
Scalable with minor issues (inconsistencies)	
Scalable with major issues (inconsistencies)	
Scalable	X

Does this training tool cover interoperability aspects of a specific training program?

Not interoperable	

Interoperable with minor issues (inconsistencies)	
Interoperable with major issues (inconsistencies)	
Interoperable	X

Is this training tool stable while used in a specific training program?

Not stable	
Stable with minor issues (inconsistencies)	
Stable with major issues (inconsistencies)	
Stable	X

Does this training tool support the user’s (trainer, trainee) privacy and security aspects?

Yes.	X
No	
Other	

If “Other”, then respond in free text

What is the level of prior knowledge needed to use the training tool?

Knowledge of terms	

Knowledge of meanings	X
Integration of knowledge	
Application of knowledge	

Do the trainers/trainees find the training tool easy to use?

Yes	X
No	

Does this training tool support the trainers/trainees’ native language and/or multiple languages?

Yes	
No	X

Appropriateness of the training tool. Tool can be used for:

VG: very good, G: good, NA: not appropriate	VG	G	NA
Commercial seminar (up to 2 days)	X		
Commercial course (up to 2 months)	X		
Academic Lab (accompanying cybersecurity course) / Academic course	X		
Cybersecurity exercise /cyber range	X		
Cybersecurity hackathon	X		
Cybersecurity game		X	
Certification cybersecurity course		X	
Specific Cybersecurity Topic(s)		X	
Network security control			X
Penetration testing			X
Incident response		X	
Cloud security			X
Risk management		X	
Forensics		X	
Other – write which one			

4.3.30 RxB

Filled by	Martin Bärmann
Organization	Seriousgames Interactive A/S
Date	23-05-2023
Contact	mba@seriousgames.net
License	?
Cost of license	Under mutual agreement depending on the purpose of use and no of users
Available link to download tool	Upon provided credential, access can be granted through compatible browser
Online manual(s)	User manual as an tutorial layer within the game
Online tutorial(s)	N/A at this moment

Description

Summary
The **RxB game** is an initiative developed as part of the SPIDER [1][2] EU-funded project within the Horizon 2020 Programme. The telecommunications sector is very vulnerable to cyberattacks. Despite billions of euros invested in cybersecurity measures, cyberattack mechanisms are becoming increasingly sophisticated, pervading critical infrastructures. The virtual environment within the game will be used to help train **information security professional**s to deal with real-world incidents, test new security technologies, and support companies in making optimal **cybersecurity investment decisions**. The **RxB game** keeps training exciting and increases the **collaborative ability** in handling incidents and **defending** against **cyberattacks**. In a nutshell, the calculation models for risk estimation take under consideration several '**logical consecutive**' steps that are executed by ethical hackers (Red team) or cyber respondents (Blue team) during an attack/defence scenario. In our strategy we name these steps as **Red loop** and **Blue loop** within the deliverable. Since in the **actual calculation of a simulated scenario these actions are obscured**, SPIDER developed a game where these actions can be 'played' in the frame of **a Serious Game Security Skills Training**. The **game RxB** and intends to bridge the gap between theoretical

training and hands-on training. **RxB is a turn-based asymmetrical strategy game about cyber-attack and cybersecurity** based on the Red vs. Blue "interactions" used at hackathons, real life security simulations and company security training. Red is a hacker team trying to fulfil an objective while Blue is a cyber security team that tries to prevent this. It allows users to play on top of a **predefined asset graph** with given vulnerabilities.

RxB has been created with the following audiences in mind:

Technical people new to cyber security (e.g., cyber security students, trainees, juniors as well as operational technologist, engineers and IT professionals outside cyber security) and interested in cyber security or cyber security risk management as a career.

Cyber security managers, chief information security officers or technical specialists that want/need to understand and train cyber security strategies, cyber security management and threat prevention.

Non-cybersecurity personnel that need cyber security awareness but don't necessarily have to understand all the technicalities.

Finally, RxB could potentially be used in various contexts such as corporate security training, College and universities or individual self-training.

Main Learning Objectives & Innovation Aspects

As already mentioned, RxB aims to cover educationally several requirements of entry-level hackers. More specifically, RxB aims to deliver more awareness within the following areas to the players:

Cyber security defences require regular adjustment;

Familiarization with Hacker and Cyber defence terminology that is regularly used from exploit developers, DevSecOp engineers etc.;

Different hacker tactics and methods i.e., the way attacking surfaces are evaluated prior to engaging a target;

Prioritizing of resources during an engagement process taking under consideration the criticality of the asset and the exploitability of the existing vulnerabilities;

Selection of Cyber defence strategies that can partially mitigate or prune the available options of an attacker; Navigating through an active attack in order to promote situation awareness.

Game elements layered on top of real-life processes aim to guide, nudge and motivate users towards the desired behaviour. In a training application developed with elements of gamification, we draw on the core game elements like **mastery**, **points**, **levels**, and **achievements**. The important core of games is that the user has a strong **active role as a learner, and needs to accomplish clear goals through mastery**.

In a **turn-based game**, the user makes choices that have consequences for progression, which is clearly communicated back through points, levels and achievements. Here, the game elements are closely tied to what the user already does in the real world. It is a way to more clearly focus on the right behaviour, get feedback when he does things right, and get motivated by seeing clear progress in the form of level-ups, achievements or similar.

Since gamification is closely tied to the real world, the focus is shifted towards a more direct behavioural change. Although we can definitely create small learning elements inside a gamification experience, encouraging reflection and discussion, the user does not have the same rich learning environments as in serious games. Instead, the focus is on motivating and nudging users in the right direction.

RxB Goal

RxB is a **turn-based asymmetrical strategy game** about cyber-attack and cybersecurity based on the Red vs. Blue "games" used at hackathons, real life security simulations and company security training. Red is a hacker team member trying to fulfil an offensive objective while blue is **a cyber security team member** that tries to prevent this. However, the serious game set itself apart from other existing security training games as **no specialized technical knowledge is needed**, as it aims to deliver practical training in cyber security strategy, management, awareness and general knowledge and not in coding or tools.

Game play

A demonstration of the game play can be viewed in the following video: https://vimeo.com/600295981/c814e322a6?share=copy

The game can be played in 2 different modes:

The game is played as a hot-seat meaning that players take turns on the same computer. Hot seat also allows a single player to freely play around and try different things while controlling both the Red and Blue teams.

Single player vs. AI

As already mentioned, the head release of the game supports the **hot-seat mode human-versus-human** i.e., each counterpart has to take one decision using the turn-based approach. However, the goal is to onboard **additional playable modes** such as **single player vs. AI** towards game commercialization and exploitation.

The game is initialized based on an asset topology that imitates a telecom provider's network. As a Blue team player has to protect a network from a team of hackers (Red team). Blue has to **discover different types of vulnerabilities** and mitigate them to make sure that Red doesn't get access to the **network's sensitive resources**. Blue members also have to set up **control elements** making the road bumpy for Red and perform threat hunting and deploying intrusion detection to discover if an asset becomes compromised. Lastly, Blue will have to fix compromised assets to get the network back in working order.

One important aspect for Blue players is of course **to prioritize resources** (time, money and team members), so that the most critical aspects are taken care of. The game adapts to the players' actions, so that e.g., the Blue player must adapt its prioritization strategy depending on what the Red player does, and vice versa.

As Red team players will have to infiltrate Blues' network, **using an arsenal of offensive actions**. Red will have to work all the way **from reconnaissance through exploitation and persistency** until they reach their **objective**. Red needs to be cautious and try to trick Blue to avoid detection and being locked out of the network.

No specialised technical skill is required to play; however, it helps to know a bit about cybersecurity terminology and concepts - if not, you will learn by failing.

[1] https://cordis.europa.eu/project/id/833685

[2] https://spider-h2020.eu/

Assessment

The training tool has been used for

Commercial seminar (up to 2 days)	
Commercial course (up to 2 months)	
Academic Lab (accompanying cybersecurity course) / Academic course	
Cybersecurity exercise /cyber range	
Cybersecurity hackathon	
Cybersecurity game	**x**
Certification cybersecurity course	
Specific Cybersecurity Topic(s)	
Network security control	
Penetration testing	
Incident response	
Cloud security	
Risk management	
Forensics	
Other – write which one	
Demonstration /training to Customer	**x**
Pilot training operation	**x**
Other (explain in free text):	

*If "**Other**", then respond in free text.*

Is this training tool suitable for training purposes (reach the learning objectives and knowledge areas)

Yes	**x**
No	

Are there any needed compute resources (CPUs, GPU, RAM, Disk space)?

Yes	
No	**x**

*If "**Yes**", then respond in free text.*

What is the level of difficulty to use the training tool?

Easy	**x**
Normal	**x**
Medium/Standard/Average	
Intermediate	
Hard/Expert/difficult	

Is this training tool easily adaptable to a specific training program?

Potential	

Most likely	**x**
Neither likely or unlikely	
Least likely	

Is this training tool easily implementable for a specific training program?

Not implementable	
Implementable with minor issues (inconsistencies)	
Implementable with major issues (inconsistencies)	**x**
Implementable	

Is this training tool easily scalable for a specific training program?

Not scalable	
Scalable with minor issues (inconsistencies)	**x**
Scalable with major issues (inconsistencies)	
Scalable	

Does this training tool cover interoperability aspects of a specific training program?

Not interoperable	

Interoperable with minor issues (inconsistencies)	
Interoperable with major issues (inconsistencies)	**x**
Interoperable	

Is this training tool stable while used in a specific training program?

Not stable	
Stable with minor issues (inconsistencies)	
Stable with major issues (inconsistencies)	**x**
Stable	**xx**

Does this training tool support the user's (trainer, trainee) privacy and security aspects?

Yes.	**x**
No	
Other	

*If "**Other**", then respond in free text*

What is the level of prior knowledge needed to use the training tool?

Knowledge of terms	

Knowledge of meanings	
Integration of knowledge	**x**
Application of knowledge	**x**

Do the trainers/trainees find the training tool easy to use?

Yes	**x**
No	

Does this training tool support the trainers/trainees’ native language and/or multiple languages?

Yes	
No	**x**

Appropriateness of the training tool. Tool can be used for:

VG: very good, **G**: good, **NA**: not appropriate	**VG**	**G**	**NA**
Commercial seminar (up to 2 days)			**x**
Commercial course (up to 2 months)			**x**
Academic Lab (accompanying cybersecurity course) / Academic course			**x**
Cybersecurity exercise /cyber range			**x**
Cybersecurity hackathon		**x**	
Cybersecurity game	**x**		
Certification cybersecurity course		**x**	
Specific Cybersecurity Topic(s)		**x**	
Network security control		**x**	
Penetration testing		**x**	
Incident response		**x**	
Cloud security			**x**
Risk management			**x**
Forensics			**x**
Other – write which one			

4.3.31 Risk Assessment and Management platfrom

Filled by	Shareeful Islam
Organization	Security Lab Consulting (SLC)
Date	12-05-2023
Contact	shareeful@gmail.com
License	C
Cost of license	Under mutual agreement depending on the purpose of use and no of users
Available link to download tool	Upon provided credential, access can be granted through compatible browser
Online manual(s)	User manual available and provided upon request
Online tutorial(s)	N/A

Description

Summary
A Risk Assessment and Management Solution developed by Security Labs Consulting (SLC) aims to implement a sequential and systematic process to help organizations to understand and evaluate their individual and cascading risks and estimate the possible impacts so that informed decision can be taken. The solution is able to provide recommendations to organizations for the selection of the most appropriate control measure, indicating optimization practices, in order to minimize the expected potential loss. This unique solution relies on existing risk and security management standards, (i.e., ISO-31000/ 27001, taxonomies, (such as CVSS 3.1 (vulnerability calculation), CAPEC (threat identification), Coordinated Vulnerability Disclosure (CVD) (vulnerability identification), and suitable Machine Learning models towards achieving wider adaptability. The solution considers both textual and graphical outputs to summarize the asset, vulnerabilities, threats and risks. **Key functionalities:** *Asset Identification and Visual Representation:* Creating of an IT asset inventory of all computing and networking related devices owned, managed, or otherwise used by the organization.

Open Intelligence for Vulnerability Management: synchronizing with open-source vulnerability database to identify and assess vulnerabilities relevant to a specific system context. Asset are linked with the identified vulnerabilities.

Cyber Threat Management and Attack Scenario Generation: Identification and analysis of threats based on the vulnerability and link with the possible attack scenario. The visual scenario considers asset dependency with threats and vulnerabilities and attackers' capability and goal for the attack.

Individual and Cascading Risk Assessment and reporting: The tool assesses both individual and cascading risks and priorities the risks according to their values.

Security Control Declaration and Customization: Controls are identified and linked with the threats, vulnerabilities, and related risks. Following the assessment, most recommended controls are identified for informed decision making to minimize expected damage.

Knowledge areas

human-centric risk assessment/treatment

Asset inventory

Vulnerability and threat management

Security profiling

Assess security control

Learning Objective

The solution to equip the users/learners with the ability to assess and manage security risk and critically evaluate the protection mechanisms used to secure systems.

Skill /Competence

Demonstrate an in-depth understanding of a comprehensive risk management practice (Competence).

Analyze the existing security posture and determine cyber course of actions (Practical/Transferrable skill).

Critically evaluate assets and assess their vulnerabilities and threats (Competence).

Document and explain risk management results in a professional manner (Practical/Transferrable skill).

Assessment

The training tool has been used for

Commercial seminar (up to 2 days)	
Commercial course (up to 2 months)	
Academic Lab (accompanying cybersecurity course) / Academic course	**x**
Cybersecurity exercise /cyber range	**x**
Cybersecurity hackathon	
Cybersecurity game	
Certification cybersecurity course	
Specific Cybersecurity Topic(s)	**x**
Network security control	
Penetration testing	
Incident response	
Cloud security	
Risk management	**x**
Forensics	
Other – write which one	
Demonstration /training to Customer	
Pilot training operation	

Other (explain in free text):	

*If “**Other**”, then respond in free text.*

Is this training tool suitable for training purposes (reach the learning objectives and knowledge areas)

Yes	**x**
No	

Are there any needed compute resources (CPUs, GPU, RAM, Disk space)?

Yes	**x**
No	

*If “**Yes**”, then respond in free text.*

Internet , compatible browser

What is the level of difficulty to use the training tool?

Easy	
Normal	
Medium/Standard/Average	**x**
Intermediate	
Hard/Expert/difficult	

Is this training tool easily adaptable to a specific training program?

Potential	
Most likely	**x**
Neither likely or unlikely	
Least likely	

Is this training tool easily implementable for a specific training program?

Not implementable	
Implementable with minor issues (inconsistencies)	
Implementable with major issues (inconsistencies)	
Implementable	**x**

Is this training tool easily scalable for a specific training program?

Not scalable	
Scalable with minor issues (inconsistencies)	
Scalable with major issues (inconsistencies)	
Scalable	**x**

Does this training tool cover interoperability aspects of a specific training program?

Not interoperable	
Interoperable with minor issues (inconsistencies)	
Interoperable with major issues (inconsistencies)	
Interoperable	**x**

Is this training tool stable while used in a specific training program?

Not stable	
Stable with minor issues (inconsistencies)	
Stable with major issues (inconsistencies)	
Stable X	

Does this training tool support the user's (trainer, trainee) privacy and security aspects?

Yes.	**x**
No	
Other	

*If "**Other**", then respond in free text*

What is the level of prior knowledge needed to use the training tool?

Knowledge of terms	x
Knowledge of meanings	x
Integration of knowledge	
Application of knowledge	

Do the trainers/trainees find the training tool easy to use?

Yes	x
No	

Does this training tool support the trainers/trainees’ native language and/or multiple languages?

Yes	
No	x

Appropriateness of the training tool. Tool can be used for:

VG: very good, **G**: good, **NA**: not appropriate	**VG**	**G**	**NA**
Commercial seminar (up to 2 days)			**x**
Commercial course (up to 2 months)			**x**
Academic Lab (accompanying cybersecurity course) / Academic course	**x**		
Cybersecurity exercise /cyber range	**x**		
Cybersecurity hackathon			**x**
Cybersecurity game			**x**
Certification cybersecurity course	**x**		
Specific Cybersecurity Topic(s)			
Network security control			
Penetration testing			
Incident response			
Cloud security			
Risk management			**x**
Forensics			
Other – write which one			

4.3.32 Human-SM

Filled by	Kitty Kioskli
Organization	trustilio
Date	26-05-2023
Contact	Kitty Kioskli, kitty.kioskli@trustilio.com
License	O
Cost of license	O
Available link to download tool	N/A
Online manual(s)	N/A
Online tutorial(s)	N/A

Description

Summary
Security management package (methodologies, guidelines, interventions, trainings) developed by trustilio will be used to guide the CyberSecPro trainees in a step-by-step approach to identify and estimate the threats, vulnerabilities and risks of any enterprise; develop security reports (policies, procedures, business continuity and disaster recovery plans). Human factors and awareness raising interventions will be included in this package. This is neither a tool nor a platform, it is a methodology that trustilio uses internally when conducting consultancy on risk assessment, therefore an assessment template is not applicable.

Assessment

The training tool has been used for

Commercial seminar (up to 2 days)	**x**
Commercial course (up to 2 months)	
Academic Lab (accompanying cybersecurity course) / Academic course	**x**
Cybersecurity exercise /cyber range	**x**
Cybersecurity hackathon	
Cybersecurity game	
Certification cybersecurity course	
Specific Cybersecurity Topic(s)	
Network security control	
Penetration testing	
Incident response	**x**
Cloud security	
Risk management	**x**
Forensics	
Other – write which one	
Demonstration /training to Customer	
Pilot training operation	

Other (explain in free text):	

*If “**Other**”, then respond in free text.*

Is this training tool suitable for training purposes (reach the learning objectives and knowledge areas)

Yes	**x**
No	

Are there any needed compute resources (CPUs, GPU, RAM, Disk space)?

Yes	
No	**x**

*If “**Yes**”, then respond in free text.*

What is the level of difficulty to use the training tool?

Easy	
Normal	**x**
Medium/Standard/Average	
Intermediate	
Hard/Expert/difficult	

Is this training tool easily adaptable to a specific training program?

Potential	
Most likely	x
Neither likely or unlikely	
Least likely	

Is this training tool easily implementable for a specific training program?

Not implementable	
Implementable with minor issues (inconsistencies)	
Implementable with major issues (inconsistencies)	
Implementable	x

Is this training tool easily scalable for a specific training program?

Not scalable	
Scalable with minor issues (inconsistencies)	
Scalable with major issues (inconsistencies)	
Scalable	x

Does this training tool cover interoperability aspects of a specific training program?

Not interoperable	

Interoperable with minor issues (inconsistencies)	
Interoperable with major issues (inconsistencies)	
Interoperable	**x**

Is this training tool stable while used in a specific training program?

Not stable	
Stable with minor issues (inconsistencies)	
Stable with major issues (inconsistencies)	
Stable **x**	**x**

Does this training tool support the user's (trainer, trainee) privacy and security aspects?

Yes.	**x**
No	
Other	

*If "**Other**", then respond in free text*

What is the level of prior knowledge needed to use the training tool?

Knowledge of terms	**x**

Knowledge of meanings	
Integration of knowledge	
Application of knowledge	

Do the trainers/trainees find the training tool easy to use?

Yes	**x**
No	

Does this training tool support the trainers/trainees’ native language and/or multiple languages?

Yes	
No	**x**

Appropriateness of the training tool. Tool can be used for:

VG: very good, **G**: good, **NA**: not appropriate	**VG**	**G**	**NA**
Commercial seminar (up to 2 days)	**x**		
Commercial course (up to 2 months)			**x**
Academic Lab (accompanying cybersecurity course) / Academic course	**x**		
Cybersecurity exercise /cyber range			**x**
Cybersecurity hackathon			**x**
Cybersecurity game			**x**
Certification cybersecurity course			**x**
Specific Cybersecurity Topic(s)			
Network security control			**x**
Penetration testing			**x**
Incident response	**x**		
Cloud security			**x**
Risk management	**x**		
Forensics			**x**
Other – write which one			**x**

4.3.33 C2M-By CodeWeTrust

Filled by	Costas Voliotis
Organization	trustilio
Date	25-5-2023
Contact	costas.voliotis@codewetrust.com
License	C
Cost of license	Starts from 1100 euro/month (unlimited users)
Available link to download tool	https://www.codewetrust.com/download
Online manual(s)	https://c2m-codewetrust.gitbook.io/codewetrust/c2m-user-guide)
Online tutorial(s)	Not any

Description

Summary
CodeWeTrust's c2m is a suite of static code analysis tools assess the code quality and the security of a source code base. We believe that CodeWeTrust's c2m is unique in its ability to comprehensively assess the quality, security, and compliance of source code. It has been purpose-built from the ground up to provide a holistic evaluation of the codebase, from the initial stages of development through to the final product. CodeWeTrust sets itself apart from other approaches that focus on detecting vulnerabilities, defects, bugs, and license compliance. Instead, our tool takes a comprehensive approach to measuring quality by scanning both the source code and third-party components. By using AI-based quality analysis, we are able to provide reports that are suitable for acquisition and software development management decisions, going beyond developer-focused reporting CodeweTrust supports both On-Prem and Cloud Server Installations CodeWeTrust, with or without code sharing, automatically extracts List of licensed OSS and Commercial linked product, AI based classification and ranking by severity

Known and unknown vulnerabilities appear on your codebase or linked 3rd party components (CVE, CWE)

Aging of 3rd party OSS & Commercial libraries/components used (used vs newest version)

SBOM-SPDX

User defined quality standard

Development team productivity matrix (assuming revision history scan)

Defects, code smells, secrets, percentage and list of duplicate code blogs and more.

Assessment

The training tool has been used for

Commercial seminar (up to 2 days)	**x**
Commercial course (up to 2 months)	
Academic Lab (accompanying cybersecurity course) / Academic course	**x**
Cybersecurity exercise /cyber range	**x**
Cybersecurity hackathon	
Cybersecurity game	
Certification cybersecurity course	
Specific Cybersecurity Topic(s)	
Network security control	
Penetration testing	
Incident response	
Cloud security	

Risk management	x
Forensics	
Other – write which one	x
Demonstration /training to Customer	x
Pilot training operation	
Other (explain in free text):	

*If "**Other**", then respond in free text.*

Source Code Assessment, Static Application Security Test (SAST)

Is this training tool suitable for training purposes (reach the learning objectives and knowledge areas)

Yes	x
No	

Are there any needed compute resources (CPUs, GPU, RAM, Disk space)?

Yes	x
No	

*If "**Yes**", then respond in free text.*

What is the level of difficulty to use the training tool?

Easy	
Normal	
Medium/Standard/Average	**x**
Intermediate	
Hard/Expert/difficult	

Is this training tool easily adaptable to a specific training program?

Potential	
Most likely	**x**
Neither likely or unlikely	
Least likely	

Is this training tool easily implementable for a specific training program?

Not implementable	**x**
Implementable with minor issues (inconsistencies)	
Implementable with major issues (inconsistencies)	
Implementable	

Is this training tool easily scalable for a specific training program?

Not scalable	
Scalable with minor issues (inconsistencies)	
Scalable with major issues (inconsistencies)	
Scalable	**x**

Does this training tool cover interoperability aspects of a specific training program?

Not interoperable	
Interoperable with minor issues (inconsistencies)	
Interoperable with major issues (inconsistencies)	
Interoperable	**x**

Is this training tool stable while used in a specific training program?

Not stable	
Stable with minor issues (inconsistencies)	
Stable with major issues (inconsistencies)	
Stable	**x**

Does this training tool support the user's (trainer, trainee) privacy and security aspects?

Yes.	**x**
No	
Other	

*If “**Other**”, then respond in free text*

What is the level of prior knowledge needed to use the training tool?

Knowledge of terms	**x**
Knowledge of meanings	**x**
Integration of knowledge	
Application of knowledge	**x**

Do the trainers/trainees find the training tool easy to use?

Yes	**x**
No	

Does this training tool support the trainers/trainees’ native language and/or multiple languages?

Yes	
No	**x**

Appropriateness of the training tool. Tool can be used for:

VG: very good, **G**: good, **NA**: not appropriate	**VG**	**G**	**NA**
Commercial seminar (up to 2 days)	**x**		
Commercial course (up to 2 months)			**x**
Academic Lab (accompanying cybersecurity course) / Academic course	**x**		
Cybersecurity exercise /cyber range	**x**		
Cybersecurity hackathon			**x**
Cybersecurity game			**x**
Certification cybersecurity course			**x**
Specific Cybersecurity Topic(s)			
Network security control			
Penetration testing			
Incident response			
Cloud security			
Risk management	**x**		
Forensics			
Other – write which one			

4.3.34 SmartViz

Filled by	Stella Markopoulou
Organization	ZELUS
Date	25-05-2023
Contact	s.markopoulou@zelus.gr
License	proprietary
Cost of license	To be elaborated in the next phase
Available link to download tool	N/A (Provided upon request)
Online manual(s)	N/A
Online tutorial(s)	N/A

Description

Summary
SmartViz goes beyond data visualisation and also addresses key cybersecurity areas such as endpoint security, security training, reporting, security-focused design, detection and blocking of data manipulation. It recognizes the importance of securing endpoints, which are often targets of cyber-attacks, and provides features to monitor and protect them. The tool also offers security training capabilities, enabling users to enhance their understanding of cybersecurity practices and stay up to date with the latest threats and vulnerabilities. In terms of design, SmartViz adopts a security-focused approach, considering principles such as confidentiality, integrity, and availability. It promotes secure design practices to ensure that the tool itself is robust against potential attacks. Within CSPro, SmartViz will be used as a training tool for security analysts to be able detect incidents and analyse them to identify attacks and their origins.

Assessment

The training tool has been used for

Commercial seminar (up to 2 days)	
Commercial course (up to 2 months)	x
Academic Lab (accompanying cybersecurity course) / Academic course	
Cybersecurity exercise /cyber range	x
Cybersecurity hackathon	
Cybersecurity game	
Certification cybersecurity course	
Specific Cybersecurity Topic(s)	
Network security control	
Penetration testing	x
Incident response	x
Cloud security	
Risk management	x
Forensics	x
Other – write which one	
Demonstration /training to Customer	x
Pilot training operation	x

Other (explain in free text):	

*If “**Other**”, then respond in free text.*

Is this training tool suitable for training purposes (reach the learning objectives and knowledge areas)

Yes	**x**
No	

Are there any needed compute resources (CPUs, GPU, RAM, Disk space)?

Yes	
No	**x**

*If “**Yes**”, then respond in free text.*

What is the level of difficulty to use the training tool?

Easy	
Normal	
Medium/Standard/Average	**x**
Intermediate	
Hard/Expert/difficult	

Is this training tool easily adaptable to a specific training program?

Potential	
Most likely	**x**
Neither likely or unlikely	
Least likely	

Is this training tool easily implementable for a specific training program?

Not implementable	
Implementable with minor issues (inconsistencies)	**x**
Implementable with major issues (inconsistencies)	
Implementable	

Is this training tool easily scalable for a specific training program?

Not scalable	
Scalable with minor issues (inconsistencies)	**x**
Scalable with major issues (inconsistencies)	
Scalable	

Does this training tool cover interoperability aspects of a specific training program?

Not interoperable	

Interoperable with minor issues (inconsistencies)	x
Interoperable with major issues (inconsistencies)	
Interoperable	

Is this training tool stable while used in a specific training program?

Not stable	
Stable with minor issues (inconsistencies)	
Stable with major issues (inconsistencies)	
Stable	x

Does this training tool support the user's (trainer, trainee) privacy and security aspects?

Yes.	x
No	
Other	

*If "**Other**", then respond in free text*

What is the level of prior knowledge needed to use the training tool?

Knowledge of terms	

Knowledge of meanings	
Integration of knowledge	**x**
Application of knowledge	

Do the trainers/trainees find the training tool easy to use?

Yes	**x**
No	

Does this training tool support the trainers/trainees’ native language and/or multiple languages?

Yes	
No	**x**

Appropriateness of the training tool. Tool can be used for:

VG: very good, **G**: good, **NA**: not appropriate	**VG**	**G**	**NA**
Commercial seminar (up to 2 days)			**x**
Commercial course (up to 2 months)	**x**		
Academic Lab (accompanying cybersecurity course) / Academic course		**x**	
Cybersecurity exercise /cyber range		**x**	
Cybersecurity hackathon			**x**
Cybersecurity game			**x**
Certification cybersecurity course			**x**
Specific Cybersecurity Topic(s)			
Network security control		**x**	
Penetration testing			**x**
Incident response	**x**		
Cloud security		**x**	
Risk management		**x**	
Forensics	**x**		
Other – write which one			

4.3.35 AIT Cyber Range

Filled by	Gregor Langner
Organization	AIT Austrian Institute of Technology GmbH
Date	11-05-2023
Contact	gregor.langner@ait.a.cat
License	C
Cost of license	No individual licences are offered for sale
Available link to download tool	-
Online manual(s)	
Online tutorial(s)	

Description

Summary
The AIT Austrian Institute of Technology has designed a unique digital and hybrid simulation platform and operates a training center at its premises in Vienna – the AIT Cyber Range. The facility can accommodate up to twenty-four in-presence participants (depending on social distancing requirements). In the training room, participants can access the AIT Cyber Range using high-quality computing equipment. Additionally, practical hands-on exercises can be conducted in the training room, using industrial control systems equipment. The advanced audio-video setup in the training room allows participants to engage flexibly with each other, e.g., participants can share their screen with the entire class on large projector screens. This can be used to facilitate group discussions. Reflecting the need to accommodate online events and participants, the training room includes facilities to live stream video and audio to the Internet. Co-located with the main training room are a multitude of other breakout rooms and space to host refreshments and social events. Our goal is to provide a flexible, professional and welcoming environment for our training course and exercise participants.

Assessment

The training tool has been used for

Commercial seminar (up to 2 days)	x
Commercial course (up to 2 months)	x
Academic Lab (accompanying cybersecurity course) / Academic course	x
Cybersecurity exercise /cyber range	x
Cybersecurity hackathon	x
Cybersecurity game	x
Certification cybersecurity course	
Specific Cybersecurity Topic(s)	
Network security control	
Penetration testing	
Incident response	x
Cloud security	x
Risk management	x
Forensics	x
Other – write which one	
Demonstration /training to Customer	x
Pilot training operation	x

Other (explain in free text):	

*If “**Other**”, then respond in free text.*

Is this training tool suitable for training purposes (reach the learning objectives and knowledge areas)

Yes	**x**
No	

Are there any needed compute resources (CPUs, GPU, RAM, Disk space)?

Yes	**x**
No	

*If “**Yes**”, then respond in free text.*

A computer with a current browser is required to participate in the exercise.

What is the level of difficulty to use the training tool?

Easy	
Normal	**x**
Medium/Standard/Average	**x**
Intermediate	**x**
Hard/Expert/difficult	**x**

Is this training tool easily adaptable to a specific training program?

Potential	
Most likely	x
Neither likely or unlikely	
Least likely	

Is this training tool easily implementable for a specific training program?

Not implementable	
Implementable with minor issues (inconsistencies)	
Implementable with major issues (inconsistencies)	
Implementable	x

Is this training tool easily scalable for a specific training program?

Not scalable	
Scalable with minor issues (inconsistencies)	
Scalable with major issues (inconsistencies)	
Scalable	x

Does this training tool cover interoperability aspects of a specific training program?

Not interoperable	
Interoperable with minor issues (inconsistencies)	
Interoperable with major issues (inconsistencies)	
Interoperable	**x**

Is this training tool stable while used in a specific training program?

Not stable	
Stable with minor issues (inconsistencies)	
Stable with major issues (inconsistencies)	
Stable **X**	**x**

Does this training tool support the user's (trainer, trainee) privacy and security aspects?

Yes.	
No	
Other	**x**

*If "**Other**", then respond in free text*

There is log data for each activity, but this data cannot be attributed to individual users as they have roles in the exercise and are not linked to the individual users in the environment.

What is the level of prior knowledge needed to use the training tool?

Knowledge of terms	**x**
Knowledge of meanings	**x**
Integration of knowledge	**x**
Application of knowledge	**x**

Do the trainers/trainees find the training tool easy to use?

Yes	**x**
No	

Does this training tool support the trainers/trainees’ native language and/or multiple languages?

Yes	**x**
No	

Appropriateness of the training tool. Tool can be used for:

VG: very good, **G**: good, **NA**: not appropriate	**VG**	**G**	**NA**
Commercial seminar (up to 2 days)	x		
Commercial course (up to 2 months)	x		
Academic Lab (accompanying cybersecurity course) / Academic course	x		
Cybersecurity exercise /cyber range	x		
Cybersecurity hackathon	x		
Cybersecurity game	x		
Certification cybersecurity course		x	
Specific Cybersecurity Topic(s)			
Network security control	x		
Penetration testing		x	
Incident response	x		
Cloud security		x	
Risk management	x		
Forensics	x		
Other – write which one			

4.3.36 Security Infusion

Filled by	Nikos Nikolaou
Organization	ITML
Date	12-05-2023
Contact	nikolaou@itml.gr
License	C
Cost of license	if not "O"
Available link to download tool	To schedule an online demo https://security-infusion.com/#ContactUs
Online manual(s)	https://security-infusion.com/documentation
Online tutorial(s)	YouTube - Security Infusion: Tutorial Series (playlist of 4 videos) https://www.youtube.com/playlist?list=PLvOnVzMrm7PyVjpfF5I5WOZ0xVY5-6p0W

Description

Summary
Security Infusion (**SI**) is an agent-based software that collects, analyses, visualises, and presents real time data that concern the operation and security status of an organization's IT resources during their day-to-day operations, along with storing historical data from past logs and events to be used and analysed later. The overall solution comprises a cloud-based manager that collects data from different resources and a set of light-weight agents that run on those resources and collect operational data. The agents can be installed within the user's OS, while the managers reside in the cloud. There are two types of agents, the master agent is the one responsible for data streams, port scans, vulnerability assessments, and containing log servers; whereas the data agents explicitly collect data. The infusion manager is responsible for a multitude of operations including data reduction, threat management, and anomaly detection reasoner. **SI** functions as a SIEM (Security Information and Event Management), monitoring and IDS (Intrusion Detection System) service. The collected data from the underlying IT infrastructure are related with performance, services, network, and computing events. They are monitored, collected,

and analysed in real time, with the capability of further storage for the purposes of incident investigation and forensic analysis. The software is mainly a cloud native application with an edge deployment option, if required. Security Infusion was designed based on ITML's experience of managing IT resources and operational risk. The service's main aim is efficiency and simplicity for the end user, without compromising performance or accuracy of the data and information it collects and processes. Security Infusion also delivers thorough vulnerability assessments and port scans to assess certain future issues and prepare administrators to avoid and/or resolve them.

Security Infusion contains a friendly UI, which contains the following features: (i) Dashboard, , (ii) Event Analyser, (iii) Monitoring, (iv) Vulnerability and Port Scan, (v) Reporting, (vi) Admin panel. **Security Infusion** processes the following data: (1) Inputs system data, (2) OS data, (3) Setwork data, (4) Syslog events

Assessment

The training tool has been used for

Commercial seminar (up to 2 days)	
Commercial course (up to 2 months)	
Academic Lab (accompanying cybersecurity course) / Academic course	
Cybersecurity exercise /cyber range	
Cybersecurity hackathon	
Cybersecurity game	
Certification cybersecurity course	
Specific Cybersecurity Topic(s)	
Network security control	**X**
Penetration testing	
Incident response	**X**

Cloud security	
Risk management	X
Forensics	X
Other – write which one	
Demonstration /training to Customer	X
Pilot training operation	
Other (explain in free text):	

*If "**Other**", then respond in free text.*

Is this training tool suitable for training purposes (reach the learning objectives and knowledge areas)

Yes	x
No	

Are there any needed compute resources (CPUs, GPU, RAM, Disk space)?

Yes	**x**
No	

*If "**Yes**", then respond in free text.*

The requirements differ depending on the OS type:

For the windows agent, a minimum of windows 7 OS, a 32/64bit, an intel i3-i5, and a 3GB-4GB memory are required.

For the Linux agent, a centos or Ubuntu 18.04 OS, a 32/64bit, a JRE 1.8, an intel i3-i5, and a 3GB-4GB memory are required.

What is the level of difficulty to use the training tool?

Easy	
Normal	**X**
Medium/Standard/Average	
Intermediate	
Hard/Expert/difficult	

Is this training tool easily adaptable to a specific training program?

Potential	
Most likely	
Neither likely or unlikely	**X**
Least likely	

Is this training tool easily implementable for a specific training program?

Not implementable	
Implementable with minor issues (inconsistencies)	
Implementable with major issues (inconsistencies)	**X**
Implementable	

Is this training tool easily scalable for a specific training program?

Not scalable	
Scalable with minor issues (inconsistencies)	**X**
Scalable with major issues (inconsistencies)	
Scalable	

Does this training tool cover interoperability aspects of a specific training program?

Not interoperable	
Interoperable with minor issues (inconsistencies)	
Interoperable with major issues (inconsistencies)	**X**
Interoperable	

Is this training tool stable while used in a specific training program?

Not stable	
Stable with minor issues (inconsistencies)	
Stable with major issues (inconsistencies)	
Stable **X**	**XX**

Does this training tool support the user's (trainer, trainee) privacy and security aspects?

Yes.	**X**
No	
Other	

*If "**Other**", then respond in free text*

What is the level of prior knowledge needed to use the training tool?

Knowledge of terms	X
Knowledge of meanings	X
Integration of knowledge	X
Application of knowledge	X

Do the trainers/trainees find the training tool easy to use?

Yes	X
No	

Does this training tool support the trainers/trainees’ native language and/or multiple languages?

Yes	
No	X

Appropriateness of the training tool. Tool can be used for:

VG: very good, **G**: good, **NA**: not appropriate	**VG**	**G**	**NA**
Commercial seminar (up to 2 days)			
Commercial course (up to 2 months)			
Academic Lab (accompanying cybersecurity course) / Academic course			
Cybersecurity exercise /cyber range			
Cybersecurity hackathon			
Cybersecurity game			
Certification cybersecurity course			
Specific Cybersecurity Topic(s)			
Network security control		**X**	
Penetration testing			
Incident response		**X**	
Cloud security			
Risk management		**X**	
Forensics		**X**	
Other – write which one			

4.3.37 Be Cyber Aware

Filled by	Nikos NIKOLAOU
Organization	ITML
Date	12-05-2023
Contact	nikolaou@itml.gr
License	O
Cost of license	
Available link to download tool	Tool is available online (not to download, only use) - https://becyberaware.eu/
Online manual(s)	Guidelines available online - - https://becyberaware.eu/
Online tutorial(s)	https://www.youtube.com/@becyberaware8498/featured

Description

Summary
Be Cyber Aware is an initiative developed as part of the ENSURESEC [1][2] EU-funded project within the Horizon 2020 Programme[3]. **Be Cyber Aware** provides free Cyber Security Awareness training content as well as in person assessments on Cybersecurity Awareness as well as an option to register for a series of simulated (fake) scams to test the end-user vulnerability. Via addressing cyber and physical threats for e-commerce, **Be Cyber Aware** is available as a website that aims to improve the European vision of a reliable and trusted digital single market. In order to address the challenge of delivery of security awareness specific to e-commerce, the **Be Cyber Aware** initiative provides security awareness content which includes, security awareness videos, downloadable and printable security awareness supplementary material and self-assessment questionnaires. In addition, a separate YouTube channel was set up[4]. This channel contains all security awareness videos. **Be Cyber Aware** initiative stands as online cybersecurity training tool which provides training material and techniques in order to address six (6) attack techniques grouped in two (2) broad categories – (1) social engineering practice and (2) deception in marketing practices. The selected attack techniques in which the **Be Cyber Aware** initiative provides online cybersecurity

awareness training are: (1) Phishing, (2) QRishing, (3) Strike Through Pricing, (4) Smishing, (5) Equivocation and Manipulation and (6) Fake Reviews.

For each one of the cybersecurity awareness trainings, **Be Cyber Aware** includes a short introduction to the attack techniques; the description and consequences of the attack technique; the reasons we fall for the attack technique; the prevention and detection measures (not to fall for attack technique); and the appropriate reaction to the attack technique. For each one of the cybersecurity awareness trainings, **Be Cyber Aware** provides also a short 3-minute security awareness video (available also on YouTube), a downloadable and printable security awareness poster, short awareness tutorial and a self-assessment questionnaire. Regarding the self-assessment questions as part of the cybersecurity awareness training, for each one of the six (6) attack techniques, a set of security awareness quizzes are available to assess the level of awareness of trainees prior to and after the delivery of the cybersecurity awareness training. In addition, an extra (optional – sign-up/registration needed) assessment mechanism is available and provides experimental attack simulation. The target audience of **Be Cyber Aware** initiative for each one of the attack techniques can be users of various demographic characteristics (level of education, social and economic status) and individual states (low/medium level of risk awareness, high/medium curiosity, low/medium technological expertise, overconfidence in internet/smartphones/tablets usage). The entire content of **Be Cyber Aware** initiative, as cybersecurity awareness tool, is available into six languages (English, Greek, Romanian, Spanish, Italian, and German).

[1] https://www.ensuresec.eu/

[2] https://cordis.europa.eu/project/id/883242

[3] https://research-and-innovation.ec.europa.eu/funding/funding-opportunities/funding-programmes-and-open-calls/horizon-2020_en

[4] https://www.youtube.com/channel/UCSAcOdvaGAU3q4PffI1lYDQ

Assessment

The training tool has been used for

Commercial seminar (up to 2 days)	
Commercial course (up to 2 months)	
Academic Lab (accompanying cybersecurity course) / Academic course	
Cybersecurity exercise /cyber range	**X**
Cybersecurity hackathon	

Cybersecurity game	**X**
Certification cybersecurity course	
Specific Cybersecurity Topic(s)	
Network security control	
Penetration testing	
Incident response	
Cloud security	
Risk management	
Forensics	
Other – write which one	**X**
Demonstration /training to Customer	
Pilot training operation	
Other (explain in free text):	

*If "**Other**", then respond in free text.*

Cybersecurity awareness training about: (1) Phishing, (2) QRishing, (3) Strike Through Pricing, (4) Smishing, (5) Equivocation and Manipulation and (6) Fake Reviews

Is this training tool suitable for training purposes (reach the learning objectives and knowledge areas)

Yes	**X**
No	

Are there any needed compute resources (CPUs, GPU, RAM, Disk space)?

Yes	
No	**X**

*If "**Yes**", then respond in free text.*

What is the level of difficulty to use the training tool?

Easy	**X**
Normal	
Medium/Standard/Average	
Intermediate	
Hard/Expert/difficult	

Is this training tool easily adaptable to a specific training program?

Potential	
Most likely	**X**
Neither likely or unlikely	
Least likely	

Is this training tool easily implementable for a specific training program?

Not implementable	
Implementable with minor issues (inconsistencies)	
Implementable with major issues (inconsistencies)	
Implementable	**X**

Is this training tool easily scalable for a specific training program?

Not scalable	**X**
Scalable with minor issues (inconsistencies)	
Scalable with major issues (inconsistencies)	
Scalable	

Does this training tool cover interoperability aspects of a specific training program?

Not interoperable	**X**
Interoperable with minor issues (inconsistencies)	
Interoperable with major issues (inconsistencies)	
Interoperable	

Is this training tool stable while used in a specific training program?

Not stable	
Stable with minor issues (inconsistencies)	
Stable with major issues (inconsistencies)	
Stable	**X**

Does this training tool support the user's (trainer, trainee) privacy and security aspects?

Yes.	**X**
No	
Other	

*If "**Other**", then respond in free text*

What is the level of prior knowledge needed to use the training tool?

Knowledge of terms	X
Knowledge of meanings	X
Integration of knowledge	
Application of knowledge	

Do the trainers/trainees find the training tool easy to use?

Yes	X
No	

Does this training tool support the trainers/trainees' native language and/or multiple languages?

Yes	X
No	

Appropriateness of the training tool. Tool can be used for:

VG: very good, **G**: good, **NA**: not appropriate	**VG**	**G**	**NA**
Commercial seminar (up to 2 days)			
Commercial course (up to 2 months)			
Academic Lab (accompanying cybersecurity course) / Academic course			
Cybersecurity exercise /cyber range	**X**		
Cybersecurity hackathon			
Cybersecurity game	**X**		
Certification cybersecurity course			
Specific Cybersecurity Topic(s)			
Network security control			
Penetration testing			
Incident response			
Cloud security			
Risk management			
Forensics			
Other – write which one	**X**		

*If "**Other**", then respond in free text*

Cybersecurity awareness training about: (1) Phishing, (2) QRishing, (3) Strike Through Pricing, (4) Smishing, (5) Equivocation and Manipulation and (6) Fake Reviews

5 CSP Blended Tools

5.1 Knowledge areas as per market demand from D2.1

Previously, CyberSecPro conducted a market-driven professional cybersecurity programme analysis. The market analysis focused on cybersecurity knowledge areas and hands-on skills needed in the market and within the EU cybersecurity ecosystem. Table 2 presents a summary of knowledge areas elicited from the market analysis.

Table 2: Market Analysis Identified Knowledge Areas

S/N	Cybersecurity Knowledge
1	Cybersecurity Tools and Technologies
2	Cybersecurity Management Systems (CSMS)
3	Ethical Hacking and Penetration Testing
4	Cybersecurity Threat Management / Security Operations Center (SOC)
5	Cybersecurity for Artificial Intelligence and Machine Learning
6	Cybersecurity Risk Management
7	Cybersecurity Policy, Process and Compliance
8	Cybersecurity Education and Training
9	Network and Communications Security
10	Programming Skills and Software Security
11	Cybersecurity Forensics
12	Cloud Security
13	Soft and Transferable Skills
14	Systems Security / Systems Administrations and Security
15	Cybersecurity Law and Auditing
16	Cybersecurity Architecture
17	Cybersecurity Engineering
18	Data Protection and Security

5.2 Analysis prioritisation of knowledge areas of CSP Course offerings

Given the market-driven demand for cybersecurity knowledge areas and the need to address the cybersecurity workforce skills shortage in the EU, this section prioritises the knowledge areas presented in the previous section. Prioritisation of knowledge areas was performed based on market survey responses (see D2.1) as well as on the knowledge areas the CSP partner courses covered presented here (Table 3). A total of 81 courses are currently available from CSP higher education institutions (67) and private companies (14) where 42 (52%) courses are at undergraduate levels (BSc.),16 (20%) courses offered at the graduate level (MSc.), 7 (9%) summer school courses, and 15 (19%) professional training courses (See Appendix A for courses offered by CSP partners). While CSP HEI's may offer similar courses, we recommend referring to course descriptions in Section 3 for information on European Credit Transfer and Accumulation System (ECTS) course hour requirements or costs as these may vary between courses and institutions.

Table 3: Knowledge areas the CSP partner courses

Knowledge Areas from CSP Course Offerings	Course offered by	Course Name	Department	Knowledge Area in the course offered
Applied Cryptography	UPRC	Cryptography	Department of Informatics	Applied Cryptography
	UPRC	Applied Cryptography, MSc	Department of Informatics	Applied Cryptography
	PDMFC	Applied Cryptography	R&D	Applied Cryptography
	UCY	Systems Security	Computer Science	Applied Cryptography
	UCY	Data Security	Computer Science, MSc	Applied Cryptography
	UMA	Security Services and Applications	Computer Science	Applied Cryptography
	UMA	Information Security	Computer Science	Applied Cryptography
	UMA	Foundations of Cybersecurity	Computer Science	Applied Cryptography
				TOTAL = 8
Risk Management and governance	UPRC	Security Governance	Department of Informatics	Risk Management & Governance Security Operations & Incident Management Forensics
	UPRC	Security Policies and Security Management	Department of Digital Systems	Risk Management & Governance
	UPRC	Operational Research	Department of Business Administration	Risk Management & Governance

	UPRC	Information Security Governance, MSc	Department of Informatics	Risk Management, Governance & Compliance Security Auditing
	UPRC	CyberHot		Risk Management & Governance Malware & Attack Technologies
	UPRC	Cybersecurity Policies and Practices in the EU - for non-IT Experts		Risk Management & Governance Law & Regulation
	LAU	Information Security Management	ICT & Cybersecurity	Risk Management & Governance
	LAU	Risk Management		Risk Management & Governance
	PDMFC	Introduction to Risk Management using Eramba or Simple Risk Open Source Software	R&D	Risk Management & Governance
	PDMFC	ISO 27001	R&D	Risk Management, Governance & Compliance Security Auditing
	FCT	Globalisation and Security Risks	NOVA Information Management Schools	Risk Management & Governance
	MAG	Cyber Security Specialist	Maggioli Academy	Risk Management & Governance
	MAG	Project Management	Maggioli Academy	Risk Management & Governance
	Trustilio	ISO 27001		Risk Management & Governance
				TOTAL = 14
Security Operations & Incident Management	LAU	Management of Cyber security	ICT & Cybersecurity	Security Operations & Incident Management
	TalTech	Cyber Incident Handling	Department of Software Sciences, MSc	Security Operations & Incident Management
	PDMFC	Incident Response & Network Intrusion Detection Systems	R&D	Security Operations & Incident Management
				TOTAL = 3
Forensics	UPRC	Digital Forensics, MSc	Department of Informatics	Forensics
	UMA	Information Security and Computer Forensics	Computer Science	Forensics

	UMA	Computer Forensics	Computer Science, MSc	Forensics
				TOTAL = 3
Malware & Attack Technologies	UPRC	Information Systems Security	Department of Informatics	Malware & Attack Technologies
	UPRC	Malware Analysis, MSc	Department of Informatics	Malware & Attack Technologies
	LAU	Enterprice Security and Practitioners	ICT & Cybersecurity	Malware & Attack Technologies
	TalTech	Cyber Defense Monitoring Solutions	Department of Software Sciences, MSc	Malware & Attack Technologies
	PDMFC	Vulnerability Assessment & Management	R&D	Malware & Attack Technologies
	PDMFC	Penetration Testing	R&D	Malware & Attack Technologies
	UMA	Malware Analysis	Computer Science, MSc	Malware & Attack Technologies
	Focal Point	Penetration Testing		Malware & Attack Technologies
				TOTAL = 8
Maritime Informatics	UPRC	Maritime ICT Systems	Department of Informatics	Maritime Informatics
	UPRC	Maritime Information Systems	Department of Maritime Studies	Maritime Informatics
	UPRC	Maritime Informatics, MSc	Department of Informatics	Maritime Informatics
	TalTech	Introduction to Cyber Security (Maritime)	Estonian Maritime Academy	Maritime Informatics
	Focal Point	Cyber Defense exercise for Navy		Maritime Informatics
				TOTAL = 5
Network Security	UPRC	Network Security	Department of Informatics	Network Security
	UPRC	Mobile and Wireless Communications Security	Department of Digital Systems	Network Security
	UPRC	Network Security	Hellenic Air Force Academy	Network Security
	UPRC	Network and Communications Security, MSc	Department of Informatics	Network Security

	LAU	Internet Infrastructure and Security	ICT & Cybersecurity	Network Security
	LAU	Network and Applications Security	ICT & Cybersecurity	Network Security
	UMA	Information Security	Computer Science	Network Security
	UMA	Design and Configuration of Secure Network Systems	Computer Science, MSc	Network Security
	FCT	Network and Computer Systems Security	Department of Informatics	Network Security
				TOTAL = 9
Formal Methods for Security	UPRC	Internet Protocols	Department of Digital Systems	Formal Methods for Security
				TOTAL = 1
Privacy & Online Rights	UPRC	Privacy on the Internet	Department of Digital Systems	Privacy & Online Rights
	UPRC	Security of Information and Network Systems - GDPR	Department of Informatics, MSc	Privacy & Online Rights
	PDMFC	GDPR	R&D	Privacy & Online Rights
	FCT	GDPR: Governance, Implementation, Maintenance and Control	NOVA Information Management Schools	Privacy & Online Rights
	UMA	Digital Identity and Privacy	Computer Science	Digital Identity and Privacy
	UMA	Security and Privacy in Application Environments	Computer Science, MSc	Privacy
				TOTAL 6
e-Commerce	UPRC	e-Business and Innovation	Department of Informatics	e-Commerce
	UPRC	e-Commerce	Department of Business Administration	e-Commerce
				TOTAL = 2
Software Security	UPRC	Software Security	Department of Informatics, MSc	Software Security
	LAU	Fundamentals of Programming	ICT & Cybersecurity	Software Security

	UCY	Software Analysis	Computer Science	Software Security
	FCT	Software Security	Department of Informatics	Software Security
	UMA	Secure Coding	Computer Science, MSc	Software Security
				TOTAL = 5
Web & Mobile Security	UPRC	Mobile Internet Security	Department of Digital Systems, MSc	Web & Mobile Security
	GUF	Mobile Business	Economics & Business	Web & Mobile Security
				TOTAL = 2
Cloud Computing	UPRC	Distributed Systems & Cloud Computing	Department of Informatics, MSc	Cloud Computing
	MAG	Junior Full Stack Development	Maggioli Academy	Cloud Computing
				TOTAL = 2
Business Informatics	GUF	Wirtschaftsinformatik II (PWIN) (Business Informatics II)	Economics & Business	Business Informatics
				TOTAL = 1
Authentication, Authorisation and Accountability	GUF	Information & Communication Security	Economics & Business	Authentication, Authorisation & Accountability Cryptography Network Security
	UMA	Digital Identity and Privacy	Computer Science	Authentication, Access control
	UMA	Security in Services and Applications	Computer Science	Access control
	UMA	Information Security	Computer Science	Access control
				TOTAL = 4
Operating Systems & Virtualisation Security	LAU	Data Networks and Information Security	ICT & Cybersecurity	Operating Systems & Virtualisation Security
	LAU	Information Management and Databases	ICT & Cybersecurity	Operating Systems & Virtualisation Security
	UMA	Design and Configuration of Secure Network Systems	Computer Science	Operating Systems
				TOTAL = 3

AI Threat Detection	PDMFC	AI & Cybersecurity	R&D	AI Threat Detection
				TOTAL = 1
Cyber-Physical Systems Security	UMA	Security in Industrial and Cyber-Physical Systems	Computer Science, MSc	Cyber-Physical Systems Security
				TOTAL = 1
Law & Regulation	FCT	Cybercrime	NOVA School of Law	Law & Regulation Forensics
				TOTAL = 1
Social Network	FCT	Social Network Intelligence	NOVA Information Management Schools	Social Network
				TOTAL = 1
Data Analysis	MAG	Data Science	Maggioli Academy	Data Analysis
				TOTAL = 1

5.3 Courses Matching the Knowledge Areas

The market analysis focus was to elicit cybersecurity in demand knowledge areas. Based on D2.1 (Table 22), knowledge areas are prioritised in two categories: in-demand and high-demand.

To match the knowledge areas (KA) from the market analysis to the KA's of the CSP partner course offerings, the initial phase was comprehending the specific subjects and concepts that were handled by each knowledge area and domain. Then, the knowledge areas were subsequently categorized based on their thematic alignment with one another. An example of this is the domain of "Penetration Testing," which is primarily concerned with the identification and exploitation of security vulnerabilities. This domain was associated with other domains that address various aspects of attacks, vulnerabilities, and security issues, such as "Web & Mobile Security" or "Malware and attack technologies." To consider the existence of overlaps it is important to acknowledge that certain fields of knowledge inherently encompass other domains of knowledge. For example, the concept of "Risk Management and Governance" encompasses both "Risk Assessment and Risk Management" and "Cybersecurity Management Systems and Processes." Also, the inclusion of other knowledge fields, such as "Business Informatics," involved a thorough assessment of their thematic importance and subsequent alignment with the most appropriate knowledge domain(s). The field of "Business Informatics" has been associated with risk management and regulatory problems due to its emphasis on corporate hazards and compliance. In order to enhance the accuracy and relevance of the matching process, the mapping underwent improvements in each iteration, taking into account any additions or alterations made to the list of knowledge areas and domains. To effectively encompass the overarching concepts of cybersecurity, a thorough and all-encompassing approach was adopted during the course of the analysis. The comprehensive nature of this method facilitated a more exact and refined matching of domains and places. Prior background knowledge of cybersecurity domains helped the mapping process. For example, although the domain of "e_Commerce" covers various aspects of cybersecurity, it has been associated with "Penetration Testing" mostly owing to the common association with security vulnerabilities in online retail platforms.

The final outcome consisted of a systematic arrangement of knowledge areas aligned with domains, ensuring that each area was appropriately situated inside the domains that were most relevant to its thematic content as identified by the market analysis, knowledge areas from course offerings and the ECSF.

Table 4: Mapped Knowledge Areas from Courses and Market Analysis

Knowledge Areas of CSP Partners Course Offerings	Knowledge Areas Market Analysis
Risk Management and Governance	Cybersecurity Threat Management, Risk Assessment and Risk Management Cybersecurity Management Systems and Processes
Network Security	Cybersecurity Tools/Technologies Communications and Network Security
Forensics	Incident Response Cybersecurity Forensics
Applied Cyrptogaphy	Cybersecurity Tools/Technologies
Maritime Informatics	Emerging Technologies
Privacy & Online Rights	Data Protection and Security Cybersecurity Regulations and Compliance
Software Security	Cybersecurity Engineering, Penetration testing
Security Operations and Incidence Management	Cybersecurity Threat Management Cybersecurity Management Systems and Processes Incident Response
E_Commerce	Penetration Testing Cybersecurity Regulations and Compliance Data Protection and Security

Web & Mobile Security	Penetration Testing
Cloud Computing	Emerging Technologies Cloud Security
Operating Systems & Virtual Security	Cybersecurity Architecture Cybersecurity Tools/Technologies
Cyber-Physical Systems Security	Emerging Technologies Cybersecurity Engineering Cybersecurity Architecture
Authentication, Authorisation and Accountability	Cybersecurity Management Systems and Processes Cybersecurity Architecture Cybersecurity Tools/Technologies
Malware and Attack technologies	Cybersecurity Threat Management, Penetration testing Cybersecurity Tools/Technologies
AI Threat Detection	Cybersecurity Threat Management Cybersecurity for Artificial Intelligence and Machine Learning
Adversrial Behaviour	Cybersecurity Threat Management
Law & Regulation	Cybersecurity Regulations and Compliance
Business Informatics	Risk Assessment and Risk Management Cybersecurity Regulations and Compliance
Social Network	Communications and Network Security Emerging Technologies

An analysis of the knowledge areas derived from the market analysis and from the courses offered through CSP partners was performed (see Table 3). From the Market Analysis, “High Demand” was identified in 7 knowledge areas (penetration testing, cybersecurity tools/technologies, cybersecurity threat management, cybersecurity management systems, risk assessment and risk management, emerging technologies, and cybersecurity regulations and compliance) across 3 domains (Maritime, ICT, Other) where penetration testing was in demand across all three, and Cybersecurity tools/technologies and Cybersecurity Management Systems was identified as High Demand in ICT and Other categories. When combining the knowledge areas from the Market Demand analysis and the CSP partner course offerings, all High Demand knowledge areas identified are covered via multiple courses (see Table 5).

Table 5: High Demand KA's and Number of Courses Offered

Knowledge Areas in High Demand	Number of CSP courses offered
Penetration Testing	12
Cybersecurity Tools/Technologies	23
Cybersecurity Threat Management	27
Cybersecurity Management Systems: CS Management and Processes	21
Risk Assessment and Risk Management	15
Emerging Technologies	8
Cybersecurity Regulations and Compliance	9

Currently, CSP partners have several offers that cover the high in-demand knowledge areas that were identified in the market analysis for al demands.

5.4 CSP Knowledge Areas and the European Cybersecurity Framework

CSP is also using the ECSF as a steering framework for knowledge areas that are defined for the 12 ENISA roles in cybersecurity. The market analysis recommended mapping the CSP course knowledge areas to the ECSF framework definitions and knowledge areas (see ENISA [26] for roles knowledge and skills descriptions). CSP courses were mapped onto the ECSF roles, and the knowledge areas associated with each role (see Tables 6-17). The following tables show the which courses best fit each ENISA role. The number beside the role name indicates the number of knowledge areas defined by the ECSF. Please note that for each role, only the top courses offered from CSP partners in terms of matched knowledge areas are reported.

Table 6: Chief Information Security Officer, (11)

HEI/Partner	Level	Course Name	KA & Skills
UPRC	MSc	Information Security Governance	6

UPRC	BSc	Security Policies and Security Management	5
Trustilio		ISO27001	5
UNINOVA	Exec Master	Strategic Leadership and Governance:	4
Laurea	Professional training	Risk Manager	3
NOVA FCT	Other	Cybersecurity	3
UPRC	BSc	Security governance	3
UPRC	BSc	Maritime ICT Systems	3
UPRC	MSc Summer School	Cybersecurity Policies and Practices in the EU – for non-IT experts	3

Table 7: Cyber Incident Responder, (13)

HEI/Partner	Level	Course Name	KA & Skills
UNINOVA	Exec Master	Incident Response and Risk Management	8
UNINOVA	Exec Master	Strategic Leadership and Governance:	5
UMA	MSc	Design and Configuration of Secure Networked Systems	5
Laurea	BIT	Enterprise Security and Practitioners	4
Laurea	BIT	Cybersecurity Analyst	4
UPRC	BIT	Security governance	4
UPRC, UCy & HAFA	MSc	Cybersecurity	4
UPRC	MSc Summer School	CyberHoT	4
Focal Point		FP_CDX	4

Table 8: Cyber Legal, Policy and Compliance Officer, (5)

HEI/Partner	Level	Course Name	KA & Skills
UNINOVA	Exec Master	Emerging Trends and Collaboration	5
UPRC	BSc	Security governance	5
UPRC	BSc	Privacy on the Internet	5

Trustilio		ISO27001	5
UPRC	BSc	Security Policies and Security Management	4

Table 9: Cyber Threat Intelligence Specialist, (13)

HEI/Partner	Level	Course Name	KA & Skills
UPRC	MSc Summer School	CyberHoT	6
Laurea	Professional training	Risk Manager	5
UMA	MSc	Design and Configuration of Secure Networked Systems	5
UPRC, UCy & HAFA	MSc	Cybersecurity	5
Laurea	BIT	Enterprise Security and Practitioners	4
UPRC	BSc	Maritime ICT Systems	4
Zelus	Professional training	Threat Intelligence Analysis	4

Table 10: Cybersecurity Architect, (15)

HEI/Partner	Level	Course Name	KA & Skills
UMA	MSc	Security in Industrial and Cyber-Physical systems	5
NOVA FCT	Other	How to implement an Information Security Management System with ISO/IEC 27001	5
GUF	BSc	Business Informatics II	4
Laurea	BIT	Data Networks and Information Security	4
Laurea	BIT	Enterprise Security and Practitioners	3
Laurea	Prof	Risk Manager	3
UMA	MSc	Security and Privacy in Application Environments	3
UPRC	BSc	Information Systems Security	3
UPRC	BSc	Maritime ICT Systems	3
UPRC	MSc Summer School	CyberHoT	3
Trustilio		ISO27001	3

Table 11: Cybersecurity Auditor, (8)

HEI/Partner	Level	Course Name	KA & Skills
Trustilio		ISO27001	6
UPRC	BSc	Security governance	5
UPRC	MSc	Information Security Governance	4

Table 12: Cybersecurity Educator, (8)

HEI/Partner	Level	Course Name	KA & Skills
UCy	BSc	System Security	3
Laurea	BIT	Enterprise Security and Practitioners	2
UMA	MSc	Security and Privacy in Application Environments	2
NOVA FCT	MSc	Cybercrime	2

Table 13: Cybersecurity Implementer (11)

HEI/Partner	Level	Course Name	KA & Skills
UPRC, UCy & HAFA	MSc	Cybersecurity	4
Laurea	BIT	Fundamentals of Programming	3
Laurea	BIT	Enterprise Security and Practitioners	3
Laurea	BIT	Systems security	3
UMA	MSc	Design and Configuration of Secure Networked Systems	3
NOVA FCT	BSc	Networks and Computer Systems Security	3
UPRC	BSc	Information Systems Security	3

Table 14: Cybersecurity Researcher, (5)

HEI/Partner	Level	Course Name	KA & Skills
UPRC	BSc	Security governance	4
Laurea	BIT	Cybersecurity Project	3
Laurea	BIT	Cybersecurity Hackathon Project	3
UMA	MSc	Security and Privacy in Application Environments	3

Table 15: Cybersecurity Risk Manager, (10)

HEI/Partner	Level	Course Name	KA & Skills
Laurea	BIT	Enterprise Security and Practitioners	7
Laurea	BIT	Introduction to Information Security	6
UPRC	BSc	Maritime ICT Systems	6
UNINOVA	Exec Master	Strategic Leadership and Governance:	5
UMA	MSc	Design and Configuration of Secure Networked Systems	5

Table 16: Digital Forensics Investigator, (13)

HEI/Partner	Level	Course Name	KA & Skills
UPRC	BSc	Security governance	6
UPRC, UCy & HAFA	MSc	Cybersecurity	6
Laurea	BIT	Cybersecurity Analyst	5
UMA	MSc	Design and Configuration of Secure Networked Systems	5

Table 17: Penetration Tester. (12)

HEI/Partner	Level	Course Name	KA & Skills
UPRC, Ucy & HAFA	MSc	Cybersecurity	7
Laurea	BIT	Network and Application Security	6
UMA	MSc	Design and Configuration of Secure Networked Systems	5
UPRC	BSc	Security governance	5
UPRC	BSc	Maritime ICT Systems	4
UPRC	MSc	Penetration Testng	4
Trustilio		Code Auditing	4
Zelus		Penetraton testing or Ethical Hacking	4

Based on the ECSF framework, CSP course offerings have varied overlap with the defined ECSF framework. The Cyber, Legal, Policy and Compliance Officer role is covered 100% by 4 course offerings and at different levels (Bachelor's, Masters's). CSP course offerings also have good coverage for Cybersecurity Researcher (80%), Cybersecurity Risk Manager (70%), Cyber Incident Responder (67%), and Cybersecurity Auditor (67%) roles. Penetration Tester (58%), Chief Information Security Officer (55%), Cyber Threat Intelligence Specialist (46%) have adequate knowledge areas covered, while, Cybersecurity Educator (38%), Cybersecurity Implementer (36%), and Cybersecurity Architect (33%) roles have few knowledge areas covered.

Some courses offered by CSP partners cover multiple KA's in the ECSF and this would also be of interest as courses may have a wide range of topics that are not necessarily constrained to single knowledge areas. The following table shows mappings of courses overall ECSF knowledge areas (total 124; Table 18). Please note, only the top 10 courses are presented.

Table 18: Top CSP Course Offerings Coverage of ECSF Knowledge Areas

HEI/ Partner	Level	Course Name	Number of KA's identified over all ENISA Roles (Total KA's: 124)	Percent Coverage
UPRC	BSc	Security governance	43	34,68
UMA	MSc	Design and Configuration of Secure Networked Systems	35	28,23
UPRC	BSc	Maritime ICT Systems	34	27,42
Laurea	BIT	Enterprise Security and Practitioners	31	25,00
UPRC, UCy & HAFA	MSc	Cybersecurity	31	25,00
Trustilio		ISO27001	31	25,00
Laurea	Prof	Risk Manager	29	23,39
UPRC	MSc Summer School	CyberHoT	28	22,58
UPRC	BSc	Information Systems Security	22	17,74
UPRC	MSc	Information Security Governance	22	17,74
Laurea	BIT	Introduction to Information Security	21	16,94

The courses presented in Table 18 may have some advantages in covering knowledge areas across different roles and could be used to support needed education. For example, The UPRC (together with UCy and HAFA) course covers multiple KA's from the market analysis and the ECSF. Also, the UPRC course in 'Security Governance' has good knowledge area coverage in the ESCF framework. The 'CyberHot' summer school is also another CSP offering that is relevant in covering multiple knowledge areas from the market analysis and the ECSF frameworks. Appendix E shows all courses mapped on the ECSF roles framework.

5.5 CSP Tools Matching the Knowledge Areas

A total of 66 (Appendix B) tools are currently offered to the CSP program from higher education institutions (28) and partners (38). While most tools offered from HEI's are academic labs (see Table19), CSP partners complement HEI institutions by offering a more varied offering of tools.

Table 19: Couse Type Offered at CSP Partners

Type of course offering	CSP HEI	CSP Partner
Commercial seminar (up to 2 days)	2	9
Commercial course (up to 2 months)	0	6
Academic Lab (accompanying cybersecurity course) / Academic course	27	21
Cybersecurity exercise /cyber range	4	19
Cybersecurity hackathon	2	22
Cybersecurity game	2	8
Certification cybersecurity course	1	5

The knowledge areas covered by the tools do correspond with several KA's identified in the market demand analysis but are limited in their specific scope. But the tools are also evaluated by CSP contributors who have expertise in their field and do give suggestions for their adaptability, for example how the tools can cover other knowledge areas, or how the tools can be adapted to different offerings. For example, other reported knowledge areas the tools covered as reported by partners include malware analysis, vulnerabilities code, and cryptography and authentication.

Table 20: CSP Tool Offerings Knowledge Areas

Tool Knowledge Area	CSP HEI	CSP Partner
Network security control	8	12
Penetration testing	9	7
Incident response	1	15
Cloud security	0	9
Risk management	5	12
Forensics	5	13
Other – write which one	11	12

More than half of the tool's use was reported as easy (12%) or normal (48%) in difficulty, while some tools had medium (18%), intermediate (11%) or difficult/expert (11%) levels.

Only one HEI tool (Nessus) gave users the possibility for certification, whereas five private tool offerings (HtB Enterprise Labs, IDPS, Wazuh, Lynis, LIDDUN) offered certification possibilities. Please refer to the tool description in Section 4.2 for any information on cost or licensing for certifications. Most tools were reported as easy (80%) to learn, and 16 of the tools offered the possibility of learning the tool in different languages. Again, please refer to the tool descriptions in Section 4.2 for more information.

Per October 15, 2023 the CSP consortium has already begun training partners in tool use (Appendix C). Ten physical courses and seven online courses have been delivered to partners for training with the tools offered by CSP partners. Please see Appendix E for oversight of all courses and the evaluations by the course providers (Appendix F). Appendix G contains a template for the evaluation of participants experiences of the courses. These will be used in future course deliveries to evaluate the courses and the tools.

5.6 Conclusion of CSP Course, Tools, and Platform Offerings

The market-driven analysis of professional cybersecurity programs undertaken by CyberSecPro had the primary objective to identify the essential knowledge areas and proficiencies necessary in the cybersecurity field, specifically within the European Union's cybersecurity industry. CSP partner courses and tools that are currently delivered and available to the CyberSecPro program. The prioritization of knowledge categories was determined by the analysis of market surveys and the evaluation of cybersecurity courses and tools provided by CSP partners. A total of 81 courses offered, distributed across several academic levels. Among these, 52% were categorized as undergraduate courses, 20% were classified as graduate courses, 9% were designated as summer school courses, and the remaining 19% were categorized as professional training courses.

The investigation classified knowledge domains into categories of in-demand and high-demand, taking into consideration market demand. The areas were aligned with CSP partner course offerings, taking into account thematic congruence. The inclusion of intersecting knowledge domains was taken into account, hence providing a high level of accuracy in the alignment. In addition, this chapter analysis also included evaluations of cybersecurity tools offered by CSP partners. Although the knowledge areas and subjects these tools addressed were diverse, their range was fairly restricted, but these tools can be adaptable and flexible of knowledge areas coverage for these instruments.

The level of difficulty and the available certification alternatives for both the courses and the tools offered by CSP partners exhibited variability that can be matched to several of the knowledge areas defined by the market analysis.

The analysis also compared CSP partner course offerings to the ECSF to delineate the knowledge domains associated with the defined ENISA roles. While certain roles were adequately addressed in CSP courses, others had limited coverage of knowledge domains. Certain courses did encompass various knowledge areas under the ECSF, meaning that specific course meet both the market demand and established frameworks like the ECSF.

Conclusions

Based on the analysis from the market demand and from the CSP course and tool analysis, the following recommendations are proposed:

- Increase course variety in the CyberSecPro program to provide a more inclusive learning environment. There are already many cybersecurity courses, but expanding the variety might target more particular domains and accommodate more learners. Additional courses or resources to address these weaknesses can improve program participants' education.
- Promote Adaptable Tools: Work with Certified Security Professionals (CSP) to build cybersecurity tools with greater adaptability and knowledge area coverage. This ensures these tools remain relevant in a fast-changing field.
- Standardize course and tool certification. This gives students clear ways to demonstrate their expertise in specific fields, advancing their careers.
- Align the CyberSecPro program with the ECSF. The curriculum must give students the skills and knowledge needed for professional jobs as specified by ENISA. The program's alignment may increase its legitimacy and significance in EU cybersecurity.
- Interdisciplinary courses that bridge technical and human aspects of cybersecurity could improve education. These courses cover the role of cybersecurity in across institutions and organizations and solve actual problems.
- Networking Opportunities: The program needs to encourage participants to network with industry professionals to collaborate and apply program expertise. CSP should develop possible internship or practical placement courses due to their close links to achieving learning outcomes
- Ensuring material accessibility: Program participants must have easy access to learning materials such as textbooks, research articles, and knowledge-sharing internet forums. This will ensure that trainee will have up-to-date scientific findings and market knowledge.

Due to industry changes and new technologies, the program's course content and tools need to be updated constantly. In cybersecurity, keeping up with industry changes is crucial, therefore, programme participants, CSP partners, and industry experts must form a feedback loop to evaluate courses and tools. Integrate user suggestions for software improvements. These proposals can help the CyberSecPro program stay competitive and adapt to EU cybersecurity industry changes.

References

[1] Flatiron School. 2022. Flatiron School. Retrieved from https://flatironschool.com/

[2] Fullstack Academy. 2023. About Fullstack Academy. Retrieved from https://www.fullstackacademy.com/

[3] Australian Computer Society. 2023. Australian Computer Society (ACS). Retrieved from https://www.acs.org.au/

[4] The Offensive Security Certified Professional. 2023. Elevating Cyber Workforce and Professional Development. Retrieved from https://www.offsec.com/

[5] ENISA. 2023. Training Courses. Retrieved from https://www.enisa.europa.eu/topics/training-and-exercises/trainings-for-cybersecurity-specialists/training-courses .

[6] European Cybersecurity Competence Centre and Network (ECCC). 2023. ECCC. Retrieved from https://cybersecurity-centre.europa.eu/index_en

[7] ESDC. 2023a. European Security and Defense College. Retrieved from https://esdc.europa.eu/

[8] ESDC. 2023b. EAB.Cyber. Retrieved from https://esdc.europa.eu/eab-cyber/

[9] CERT-EU. 2023. CERT-EU. Retrieved from https://cert.europa.eu/

[10] European Cyberdefence Agency. 2019. EDA. Retrieved from https://eda.europa.eu/news-and-events/news/2019/11/07/eda-cyber-ranges-federation-project-showcased-at-demo-exercise-in-finland

[11] EDA. 2019. EDA Cyber Ranges Federation project showcased at demo exercise in Finland. Retrieved from https://eda.europa.eu/news-and-events/news/2019/11/07/eda-cyber-ranges-federation-project-showcased-at-demo-exercise-in-finland

[12] European Commission. 2022a Digital skills and jobs coalition. Retrieved from https://digital-strategy.ec.europa.eu/en/policies/digital-skills-coalition

[13] European Commission. 2022b. National coalitions for digital skills and jobs. Retrieved from https://digital-strategy.ec.europa.eu/en/policies/national-coalitions

[14] European Commission. 2018. Employment, Social Affairs & Inclusion. Retrieved from https://ec.europa.eu/social/main.jsp?catId=1415&langId=en

[15] European Commission. 2023a. DigComp Framework. Retrieved from https://ec.europa.eu/jrc/en/digcomp/digital-competence-framework.

[16] European Commission. 2020. European Skills/Competences, Qualifications and Occupations (ESCO). Retrieved from https://ec.europa.eu/social/main.jsp?catId=1326&langId=en

[17] European Commission. 2023b. DIRECTORATE-GENERALGROW: Internal Market, Industry, Entrepreneurship and SMEs. Retrieved from https://commission.europa.eu/about-european-commission/departments-and-executive-agencies/internal-market-industry-entrepreneurship-and-smes_en

[18] EU Science Hub. 2023. JRC science and knowledge activities. Retrieved from https://joint-research-centre.ec.europa.eu/jrc-science-and-knowledge-activities_en

[19] European Commission. 2023c. DIRECTORATE-GENERALMOVE: Mobility and Transport. Retrieved from https://commission.europa.eu/about-european-commission/departments-and-executive-agencies/mobility-and-transport_en

[20] European Commission. 2023d. Closing the cybersecurity talent gap to boost the EU's competitiveness, growth and resilience ('The Cybersecurity Skills Academy'). Retrieved from https://digital-strategy.ec.europa.eu/en/library/communication-cybersecurity-skills-academy

[21] Cepol. 2023. Cepol. Retrieved from https://www.cepol.europa.eu/training-education

[22] NATO. 2023. NATO School: Cooperative Security Department (COSEC). Retrieved from https://www.natoschool.nato.int/Academics/COSEC

[23] European Network for Cyber Security (ENCS). 2023. ENCS. Retrieved from https://encs.eu

[24] GIAC. 2023. GIAC Certifications. Retrieved from https://www.giac.org

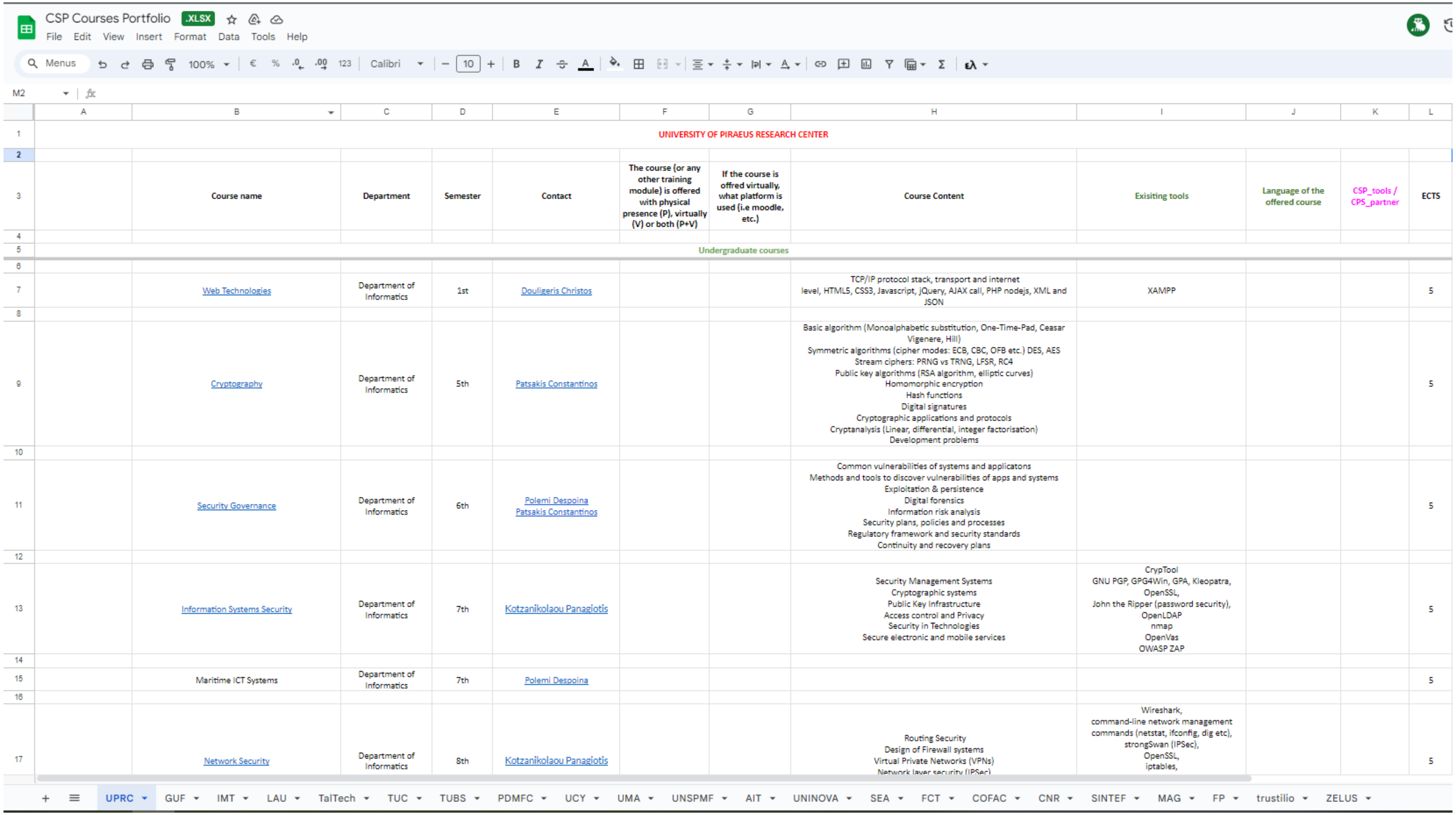
[25] CompTIA. 2023. CompTIA Security+. Retrieved from https://www.comptia.org/certifications/security

[26] ENISA. 2022. European Cybersecurity Skills Framework Role Profiles. Retrieved from https://www.enisa.europa.eu/publications/european-cybersecurity-skills-framework-role-profiles

Annex A: Catalogue to Courses

The course catalogue can be viewed at the following address:

https://docs.google.com/spreadsheets/d/1UzIkxWmZbt1gavOuSlpME4f_xiDaZeYu/edit?usp=sharing&rtpof=true&sd=true

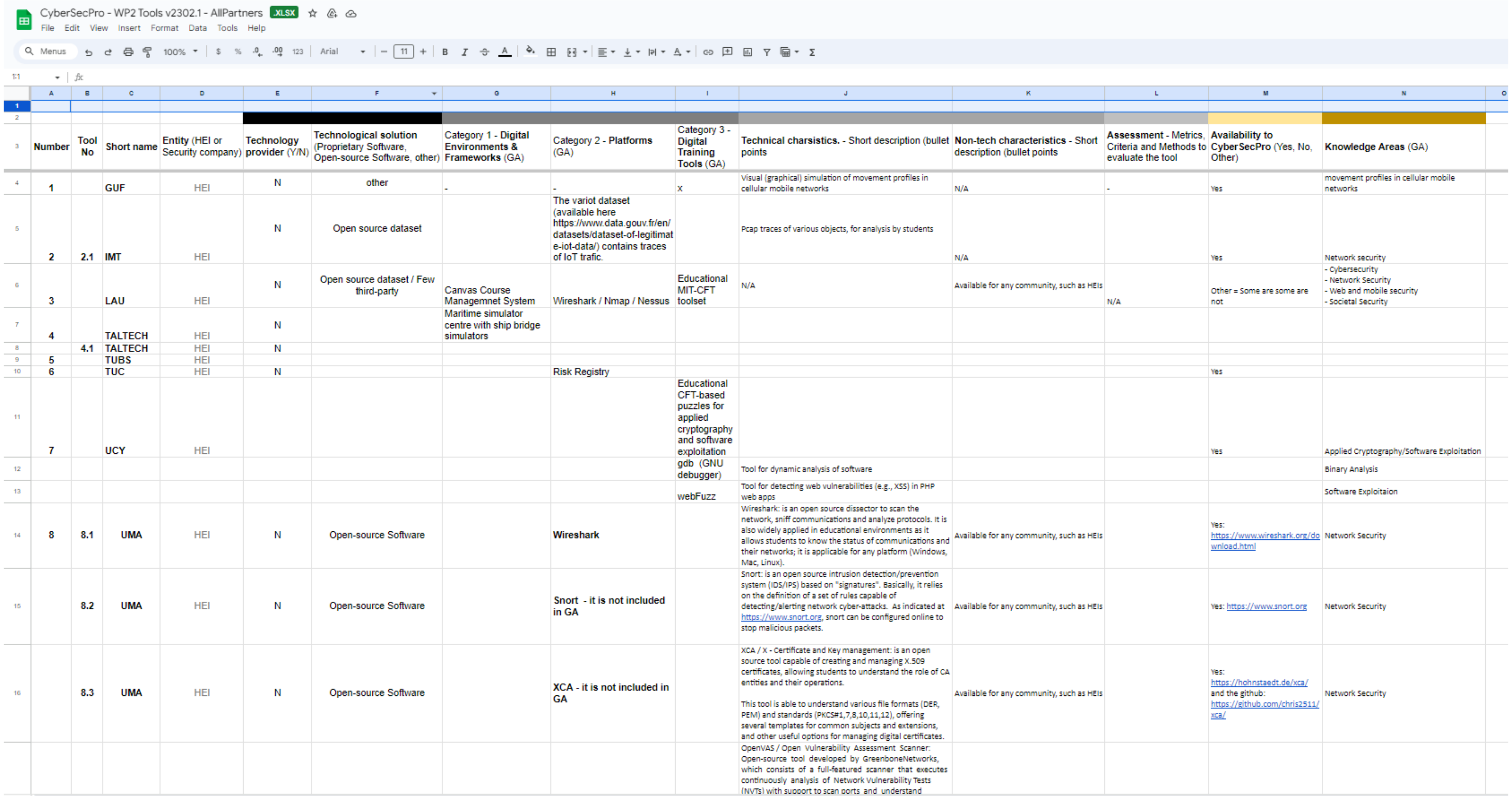


	A	B	C	D	E	F	G	H	I	J	K	L
1						UNIVERSITY OF PIRAEUS RESEARCH CENTER						
2												
3		Course name	Department	Semester	Contact	The course (or any other training module) is offered with physical presence (P), virtually (V) or both (P+V)	If the course is offred virtually, what platform is used (i.e moodle, etc.)	Course Content	Exisiting tools	Language of the offered course	CSP_tools / CPS_partner	ECTS
4												
5						Undergraduate courses						
6												
7		Web Technologies	Department of Informatics	1st	Douligeris Christos			TCP/IP protocol stack, transport and internet level, HTML5, CSS3, Javascript, jQuery, AJAX call, PHP nodejs, XML and JSON	XAMPP			5
8												
9		Cryptography	Department of Informatics	5th	Patsakis Constantinos			Basic algorithm (Monoalphabetic substitution, One-Time-Pad, Ceasar Vigenere, Hill) Symmetric algorithms (cipher modes: ECB, CBC, OFB etc.) DES, AES Stream ciphers: PRNG vs TRNG, LFSR, RC4 Public key algorithms (RSA algorithm, elliptic curves) Homomorphic encryption Hash functions Digital signatures Cryptographic applications and protocols Cryptanalysis (Linear, differential, integer factorisation) Development problems				5
10												
11		Security Governance	Department of Informatics	6th	Polemi Despoina Patsakis Constantinos			Common vulnerabilities of systems and applicatons Methods and tools to discover vulnerabilities of apps and systems Exploitation & persistence Digital forensics Information risk analysis Security plans, policies and processes Regulatory framework and security standards Continuity and recovery plans				5
12												
13		Information Systems Security	Department of Informatics	7th	Kotzanikolaou Panagiotis			Security Management Systems Cryptographic systems Public Key Infrastructure Access control and Privacy Security in Technologies Secure electronic and mobile services	CrypTool GNU PGP, GPG4Win, GPA, Kleopatra, OpenSSL, John the Ripper (password security), OpenLDAP nmap OpenVas OWASP ZAP			5
14												
15		Maritime ICT Systems	Department of Informatics	7th	Polemi Despoina							5
16												
17		Network Security	Department of Informatics	8th	Kotzanikolaou Panagiotis			Routing Security Design of Firewall systems Virtual Private Networks (VPNs) Network layer security (IPSec)	Wireshark, command-line network management commands (netstat, ifconfig, dig etc), strongSwan (IPSec), OpenSSL, iptables,			5

Annex B: Catalogue of Tools used by the partners

The tool catalogue can be viewed at the following address:

https://docs.google.com/spreadsheets/d/13h-apt-jJ8al-g0xjF_8BcPVzTiHdkI9/edit?usp=sharing&ouid=114503703144570504070&rtpof=true&sd=true


CyberSecPro - WP2 Tools v2302.1 - AllPartners .XLSX
File Edit View Insert Format Data Tools Help
Menus 100% Arial 11

Number	Tool No	Short name	Entity (HEI or Security company)	Technology provider (Y/N)	Technological solution (Proprietary Software, Open-source Software, other)	Category 1 - Digital Environments & Frameworks (GA)	Category 2 - Platforms (GA)	Category 3 - Digital Training Tools (GA)	Technical charsistics. - Short description (bullet points	Non-tech characteristics - Short description (bullet points	Assessment - Metrics, Criteria and Methods to evaluate the tool	Availability to CyberSecPro (Yes, No, Other)	Knowledge Areas (GA)
1		GUF	HEI	N	other	-	-	x	Visual (graphical) simulation of movement profiles in cellular mobile networks	N/A	-	Yes	movement profiles in cellular mobile networks
2	2.1	IMT	HEI	N	Open source dataset		The variot dataset (available here https://www.data.gouv.fr/en/datasets/dataset-of-legitimate-iot-data/) contains traces of IoT trafic.		Pcap traces of various objects, for analysis by students	N/A		Yes	Network security
3		LAU	HEI	N	Open source dataset / Few third-party	Canvas Course Managemnet System	Wireshark / Nmap / Nessus	Educational MIT-CFT toolset	N/A	Available for any community, such as HEIs	N/A	Other = Some are some are not	- Cybersecurity - Network Security - Web and mobile security - Societal Security
4		TALTECH	HEI	N		Maritime simulator centre with ship bridge simulators							
	4.1	TALTECH	HEI	N									
5		TUBS	HEI										
6		TUC	HEI	N			Risk Registry					Yes	
7		UCY	HEI					Educational CFT-based puzzles for applied cryptography and software exploitation				Yes	Applied Cryptography/Software Exploitation
								gdb (GNU debugger)	Tool for dynamic analysis of software				Binary Analysis
								webFuzz	Tool for detecting web vulnerabilities (e.g., XSS) in PHP web apps				Software Exploitaion
8	8.1	UMA	HEI	N	Open-source Software		Wireshark		Wireshark: is an open source dissector to scan the network, sniff communications and analyze protocols. It is also widely applied in educational environments as it allows students to know the status of communications and their networks; it is applicable for any platform (Windows, Mac, Linux).	Available for any community, such as HEIs		Yes: https://www.wireshark.org/download.html	Network Security
	8.2	UMA	HEI	N	Open-source Software		Snort - it is not included in GA		Snort: is an open source intrusion detection/prevention system (IDS/IPS) based on "signatures". Basically, it relies on the definition of a set of rules capable of detecting/alerting network cyber-attacks. As indicated at https://www.snort.org, snort can be configured online to stop malicious packets.	Available for any community, such as HEIs		Yes: https://www.snort.org	Network Security
	8.3	UMA	HEI	N	Open-source Software		XCA - it is not included in GA		XCA / X - Certificate and Key management: is an open source tool capable of creating and managing X.509 certificates, allowing students to understand the role of CA entities and their operations. This tool is able to understand various file formats (DER, PEM) and standards (PKCS#1,7,8,10,11,12), offering several templates for common subjects and extensions, and other useful options for managing digital certificates.	Available for any community, such as HEIs		Yes: https://hohnstaedt.de/xca/ and the github: https://github.com/chris2511/xca/	Network Security
									OpenVAS / Open Vulnerability Assessment Scanner: Open-source tool developed by GreenboneNetworks, which consists of a full-featured scanner that executes continuously analysis of Network Vulnerability Tests (NVTs) with support to scan ports and understand				

Annex C: CSP Partner Delivered Training Schedule

CyberSecPro Training Program Analysis - Physical Training Sessions

CSP training program analysis - physical training sessions | 26-Sep-2023 @ Chania, GR						
	Tool(s)	**Organization**	**Trainer(s)**	**Learning objectives**	**Duration of session**	**Prior knowledge and tools needed by *trainees***
1	XCA	UMA	Cristina Alcaraz	To learn how to manage certificates from the point of view of the certification authority, as an end user.	60min	No previous knowledge of other tools is required
2	netcat-nmap	UPRC	Dimitris Koutras	basic use of netcat - real case scenarios handling with nmap	60min	No previous knowledge of other tools is required
3	Security Infusion	ITML	TBD	Demonstration - Monitoring, alerting, reporting and analyis on security incidents	60 min	No prior knowledge and tools are required
4	gdb (internals)	UCY	Elias Athanasopoulos	How software breakpoints work	60 min	Basic background of Operating Systems

5	AIS jamming and Spoofing demonstrator	C2B	Bruno Bender	Apprehend the functionalities and potential threats on Automatic Identification System for mariners in its daily use	60 min	No prior knowledge and tools are required
6	Risk Assessment and Managment platfrom	SLC	Shareeful Islam	Demonstrate an in-depth understanding of a comprehensive risk management practice; ability to assess and manage security risk; Visually model the asset and risk management activities	60 min	Background of Basic Risk Management
7	Cyber-Defense Exercises	FP	Christos Grigoriadis- Christos Lazaridis	Firewall and SIEM implementations for the monitoring of a cyber-range environment throughout a series of attacks.	60 min	Background in Active directory, firewalls, monitoring, and log processing
8	SmartViz	ZELUS	Stella Markopoulou	Monitoring, reporting, visualising and analysing security incidents and events	60min	No previous knowledge of other tools is required
9	RxB	SGI	Martin Bärmann	RxB is an asymmetrical strategy game about cyber-attacks and defense. As Red you will attack a system in order to get access to vulnerable assets, and as Blue you will defend your system against potential threats. Each player has unique win conditions, and each play type gives a unique perspective into	60min	No previous knowledge of other tools is required

				modern real-world cyber threat landscape and threat mitigations.		
10	C2M	trustillio	C. Voliotis - K. Kioskli	SAST	60min	No previous knowledge of other tools is required

CyberSecPro Training Program Analysis - Online Training Sessions

CSP training program analysis - online training sessions

No	Date	Tool(s)	Organization	Trainer(s)	Learning objectives	Duration of session	Prior knowledge and tools needed by *trainees*	Language	Online access (link)
1	13/06/2023	C2M	**trustilio**	COSTAS VOLIOTIS	SAST	18.30-19.30	GIT - basic	English	link to training
2	16/05/2023	objdump - gdb	**UPRC**	DIMITRIS KOUTRAS	binary debugging DEMONSTRATION	18.30-20.30 CET+1	Assembly-Good Knowledge	Greek	hlink to training
3	24/05/2023	Snort	**UPRC**	DIMITRIS KOUTRAS	IDS	14.30-17.00 CET+1	IDS - basic Knowledge	Greek	https://join.skype.com/FlJBE6HgGw8p
4	03.07.2023	Penetration Testing-HtB	**FP-UPRC**	GRIGORIADIS CHRISTOS	Red Teaming	18:00-21:00 CET+1	Penetration Testing-Easy to intermediate	English	link to training
5	31/07/2023	Attack and Defense (Wazuh + Suricata)	**PDM**	S. Karagiannis	Red and Blue Teaming	17:00-20:00 CET	Easy to intermediate - Fundamental knowledge on networks and operating systems (Linux/Unix)	English	link to training
6	14/9/23-31/9/23	Cybersecurity training (TTT,	**AIT-UPRC**	NINETA POLEMI	Overview on International Ship and Port Facility Security (ISPS) Code, International Safety Management (ISM)	8 days		English	

		Shadowing, Coaching)			Code, Ships and Marine Technology (ISO 20858) standard, IMO Guidelines on maritime cyber risk management, IMO Guidelines and Djibouti Code of Conduct (DCoC) against piracy and armed robbery; presentation of physical and cyber threats in maritime port infrastructures; discussion of novel threat trends for seaport operators; examine potential mitigation strategies for those threats; characterizing and assessing interdependencies within maritime port infrastructures; security aspects integrating the physical and cyber domain; identifying cascading effects in port infrastructures; concepts towards an Hybrid Situational					
7	16/10/23	Training on cyber security risk management platform Provider	Security Lab Consulting(SLC)	Dr. Shareeful Islam	training session on cyber security and risk management platform	12:00 - 13:00 CET	None		English	link to training

Annex D: CSP Partner Courses and ECSF Roles Framework Mapping

HEI/Partner	Level	Course Name	Number of KA's identified over all ENISA Roles (Total KA's: 124)	Percent Coverage
UPRC	BSc	Security governance	43	34,68
UMA	MSc	Design and Configuration of Secure Networked Systems	35	28,23
UPRC	BSc	Maritime ICT Systems	34	27,42
Laurea	BIT	Enterprise Security and Practitioners	31	25,00
UPRC Ucy & HAFA	MSc	Cybersecurity	31	25,00
Trustilio		ISO27001	31	25,00
Laurea	Prof	Risk Manager	29	23,39
UPRC	MSc Summerschool	CyberHoT	28	22,58
UPRC	BSc	Information Systems Security	22	17,74
UPRC	MSc	Information Security Governance	22	17,74
Laurea	BIT	Introduction to Information Security	21	16,94
UMA	MSc	Security and Privacy in Application Environments	20	16,13
UPRC	BSc	Security Policies and Security Management	20	16,13
Laurea	BIT	Cybersecurity Analyst	18	14,52
NOVA FCT	BSc	Networks and Computer Systems Security	18	14,52
Trustilio		Code Auditing	18	14,52

UNINOVA	Exec Master	Strategic Leadership and Governance:	17	13,71
Laurea	BIT	Systems security	17	13,71
UMA	MSc	Security in Industrial and Cyber-Physical systems	17	13,71
Laurea	BIT	Cybersecurity Project	16	12,90
Ucy	BSc	System Security	15	12,10
NOVA FCT	Other	Cybersecurity	15	12,10
Zelus		Threat Intelligence Analysis	15	12,10
Zelus		Penetraton testing or Ethical Hacking	14	11,29
Laurea	BIT	Data Networks and Information Security	13	10,48
Focal Point		FP_CDX	13	10,48
UNINOVA	Exec Master	Incident Response and Risk Management	12	9,68
Laurea	BIT	Internet Infrastructure and Security	12	9,68
Laurea	BIT	Fundamentals of Programming	12	9,68
Laurea	MSc	Cybersecurity Management	12	9,68
UPRC	BSc	Information Systems Security	12	9,68
Sintef	Msc	Introduction to Cyber Security: Risk Management	12	9,68
Laurea	BIT	Information Security Management	11	8,87
UNINOVA	Exec Master	Emerging Trends and Collaboration	10	8,06
UMA	BSc	Foundations of Cybersecurity	10	8,06

UPRC	MSc	Network and Communications Security	10	8,06
UPRC	MSc	Network Security	10	8,06
APIROPLUS		ISO27001/ Lead Auditor Course IRCA approved	10	8,06
Laurea	BIT	The ICT Environment and Infrastructure	9	7,26
Laurea	BIT	Cybersecurity Hackathon Project	9	7,26
UPRC	MSc Summerschol	Cybersecurity Policies and Practices in the EU – for non-IT experts	9	7,26
UPRC	BSc	Operational Research	8	6,45
GUF	MSc	Information & Communication Security	7	5,65
UPRC	W West macedonia	Security of Information and Network Systems – GDPR	7	5,65
Laurea	BIT	Network Applications	6	4,84
Laurea	BIT	Network and Application Security	6	4,84
UPRC	HAFA BSc	Computer Networks & Network Security (Introduction)	6	4,84
UPRC	MSc	Cryptography	6	4,84
UPRC	MSc	Maritime Informatics	6	4,84
UNSPMF	BSc	Computer Networks	5	4,03
NOVA FCT	MSc	Cybersecurity and Governance	5	4,03
NOVA FCT	MSc	Cybercrime	5	4,03
NOVA FCT	Other	Globalisation and Security Risks	5	4,03
NOVA FCT	Other	How to implement an Information Security	5	4,03

		Management System with ISO/IEC 27001		
UPRC	BSc	Network Security	5	4,03
UPRC	BSc	Network Security	5	4,03
UPRC	BSc	Privacy on the Internet	5	4,03
UPRC	BSc	Information Systems	5	4,03
UPRC	MSc	Digital Forensics	5	4,03
UPRC	MSc Summerschol	CCNA Security V1.0	5	4,03
GUF	BSc	Business Informatics II	4	3,23
GUF	MSc	Mobile Business II - Technology, Markets, Platforms, and Business Models	4	3,23
Laurea	BIT	Information and Cyber Security Management	4	3,23
TUC	BSc	Security of Systems and Services	4	3,23
UMA	BSc	Digital Identity and Privacy	4	3,23
NOVA FCT	Other	Economic and Competitive Intelligence	4	3,23
UPRC	MSc	Penetration Testng	4	3,23
Focal Point		Table Top Exercise	4	3,23
Focal Point		FP_Training Lab	4	3,23
Maggioli	Seminar	Cybersecurity Specialist	4	3,23
Trustilio		CyberHOT	4	3,23
Zelus		SmrtViz	4	3,23
GUF	MSc	Mobile Business I - Technology, Markets, Platforms, and Business Models	3	2,42

Laurea	BIT	Information and Cybersecurity	3	2,42
NOVA FCT	BSc	Software Security	3	2,42
NOVA FCT	Other	Cybersecurity, IT Asset Management, and Governance	3	2,42
NOVA FCT	Other	GDPR: Governance, Implementation, Maintenance and Control: Governance, Implementation, Maintenance and Control	3	2,42
NOVA FCT	Other	Cybercrime - Prevention and Forensic Techniques	3	2,42
UPRC	BSc	Privacy Enhancing Technologies	3	2,42
UPRC	BSc	Mobile and Wireless Communications Security	3	2,42
UPRC	BSc	Management Information Systems	3	2,42
Zelus		Defensive analysis	3	2,42
UMA	MSc	Computer Forensics	2	1,61
UMA	MSc	Secure Coding	2	1,61
UMA	BSc	Security in Information Systems	2	1,61
NOVA FCT	MSc	Data Protection and Management Law	2	1,61
NOVA FCT	Other	Structured Analytical Techniques for Information Analysis	2	1,61
NOVA FCT	Other	The Legal Framework of the Digital Ecosystem - Telecommunications, Media and Information Technology (TMT)	2	1,61
UPRC	BSc	E-Commerce	2	1,61

Focal Point		HtB_Enterprise_Labs: Introduction To Penetration Testing	2	1,61
Sintef	Seminar	Thinking like an attacker	2	1,61
Trustilio		Lean Business Canvas Model	2	1,61
UMA	MSc	Malware analysis	1	0,81
UMA	BSc	Information Security and Computer Forensics	1	0,81
NOVA FCT	Other	Intelligence Services and Political Regimes	1	0,81
NOVA FCT	Other	Social Network Intelligence	1	0,81
NOVA FCT	Other	Digital Transformation in a Cybersecurity context	1	0,81
NOVA FCT	Other	Competitive and Counter Intelligence	1	0,81
UPRC	MSc	Malware Analysis	1	0,81
Laurea	BIT	Information Management and Databases	0	0,00
Laurea	BIT	Foundations of Web Development	0	0,00
Laurea	BIT	Cybersecurity Working Life Practices	0	0,00
TUC	BSc	Computer organization	0	0,00
TUC	Msc	Advantage computer Architecture	0	0,00
UMA	BSc	Security in Services and Applications	0	0,00
Ucy	BSc	Software Analysis	0	0,00
Ucy	MSc	Data Security	0	0,00
UNSPMF	BSc	Development of information systems	0	0,00

UNSPMF	MSc	Deep Learning	0	0,00
UNSPMF	MSc	Distributed Deep Learning	0	0,00
UNSPMF	MSc	Distributed optimization with applications	0	0,00
NOVA FCT	Other	Regional Dynamics of Security and Defense	0	0,00
NOVA FCT	Other	Methodology and Techniques for Analysis and Prospection	0	0,00
UPRC	BSc	Web technologies	0	0,00
UPRC	BSc	Cryptography	0	0,00
UPRC	BSc	Internet Protocols	0	0,00
UPRC	BSc	Cryptography	0	0,00
UPRC	BSc	E-Business and Innovation	0	0,00
UPRC	HAFA BSc	Network Security	0	0,00
UPRC	MSc	Information Security of Public Services and Systems and Blockchain Technologies	0	0,00
UPRC	MSc	Information Security	0	0,00
UPRC	MSc	Applied Cryptography	0	0,00
UPRC	MSc	Software Security	0	0,00
UPRC	MSc	Advance Cryptographic and Security Technologies (Blockchain Technologies)	0	0,00
UPRC	MSc	Applied Cryptography	0	0,00
UPRC	MSc	Mobile Internet Security	0	0,00
UPRC	W West macedonia	Distributed Systems and Cloud Computing	0	0,00
UPRC	MSc Summerschol	AIS / GNSS spoofing	0	0,00

Maggioli		The Application Consultant	0	0,00
Maggioli		Junior Full Stack Developer	0	0,00
Maggioli		Data Scinece and Advance	0	0,00
Maggioli		Project Management	0	0,00
Maggioli	Seminar	Bootcamp Maggioli Academy	0	0,00
Maggioli	Seminar	H-Greenovation	0	0,00
Maggioli	Seminar	Girls Code it Better	0	0,00
Sintef	Msc	Introduction to Cyber Security	0	0,00
Sintef	Seminar	Digital Torc training	0	0,00
APIROPLUS		Introduction to the new ISO/IEC 27001 version	0	0,00
APIROPLUS		Cybersecurity Maturity Models Requirements / Auditing practices	0	0,00

Annex E: Tool description and assessment sheet (template)

Tool Name: ________________________________ Date: __________________ Duration:_________

Tool Offered by: ____

Provider's (Trainer) Report

A. TRAINING SESSION/tool - Introduction

Brief summary of the training session. Focus on tool, topic, learning objectives, prior knowledge.

B. TRAINING SESSION/tool – learning outcomes

Mark all that apply for the tool:

________ Understand viruses, worms, Trojans, ransomware, and spyware.

________ Perform malware detection and analysis using malware detection tools.

________ Perform static and dynamic malware analysis.

________ Sandbox and virtualize malware for analysis.

________ Reverse engineer malware behavior.

________ Identify and respond to malware attacks using IOCs and threat intelligence feeds.

________ Anti-malware and best practices protect systems and networks.

________ Investigate unusual network behavior using network traffic analysis techniques.

________ Memory forensics tools can analyze volatile data and detect live system attacks.

________ Recover and analyze hacked system data with disk forensics tools.

________ Windows, macOS, and Linux forensics.

________ Use digital forensics to track criminals.

________ Malware detection and forensic analysis include legal and ethical issues.

________ Present malware detection and forensic investigation results clearly.

________ Keep up with malware detection and forensic analysis developments and dangers.

OTHER: Please specify ____

OTHER: Please specify ____

OTHER: Please specify ____

OTHER: Please specify ____

OTHER: Please specify ____

OTHER: Please specify ____

C. TRAINING SESSION/tool - demonstration / (supplementary material)

Short description about the demo of the training tool. If supplementary material (slides) is available, then should be included.

D. TRAINING SESSION/tool - mock exercises and group work / (supplementary material)

Short description about the set-up of the training session. If supplementary material (slides) is available, then include it.

E. TRAINING SESSION/tool – results

Brief summary of the major outcomes of the training session. Focus on the methodology, the steps and the highlights.

F. TRAINING SESSION/tool – demographics

Info about:

Total number of persons

Nationalities: List ALL.

Level of education [undergraduate student (e.g. 10% or number of persons), BSc, postgraduate student, MSc, PhD student, PhD

Group ages [18-29 (e.g. 10% or number of persons), 30-39, 40-49, 50-59, 60-...]

Gender groups [% Male, % Female]

Annex F: CyberSecPro Training Program Analysis Training Session – Completed Tool Evaluation Report From Trainers

CyberSecPro Training Program Analysis Training Session – Tool Evaluation report

Tool Name: Nessus **Date:** 19/10/2023 **Duration:** min Training + 3H Exercises

Tool Offered by: Leo Johannesberg, Paresh Rathod & Paulinus Ofem

Provider's (Trainer) Report

TRAINING SESSION/tool - **Introduction**

Nessus is a vulnerability scanner tool to detect potential vulnerabilities within network infrastructures. This training session focused on leveraging the tool to identify, analyze, and remediate potential security risks in the network. The participants are expected to have a basic understanding of network security concepts, vulnerability management, and risk assessment.

TRAINING SESSION/tool – **learning outcomes**

Mark all that apply for the tool:

- □ Understand viruses, worms, Trojans, ransomware, and spyware.
- ☑ Perform malware detection and analysis using malware detection tools.
- □ Perform static and dynamic malware analysis.
- □ Sandbox and virtualize malware for analysis.
- □ Reverse engineer malware behavior.
- □ Identify and respond to malware attacks using IOCs and threat intelligence feeds.
- ☑ Anti-malware and best practices protect systems and networks.
- □ Investigate unusual network behavior using network traffic analysis techniques.
- □ Memory forensics tools can analyze volatile data and detect live system attacks.
- □ Recover and analyze hacked system data with disk forensics tools.
- □ Windows, macOS, and Linux forensics.
- □ Use digital forensics to track criminals.
- ☑ Malware detection and forensic analysis include legal and ethical issues.

□ Present malware detection and forensic investigation results clearly.

☑ Keep up with malware detection and forensic analysis developments and dangers.

□ OTHER: Please specify ______________________________

□ OTHER: Please specify ______________________________

□ OTHER: Please specify ______________________________

□ OTHER: Please specify ______________________________

□ OTHER: Please specify ______________________________

□ OTHER: Please specify ______________________________

TRAINING SESSION/tool - demonstration / (supplementary material)

During the training session, a live demonstration of Nessus was provided, showcasing how to scan a network for vulnerabilities, understand the generated reports, and propose remediation strategies. Supplementary material, including slide presentations.

TRAINING SESSION/tool - mock exercises and group work / (supplementary material)

Participants engaged in mock exercises where they had to scan simulated networks to identify vulnerabilities using Nessus. They worked in groups, discussed their findings, and suggested potential remediation steps. Supplementary material, such as guides and tips, was provided in slide format and web resources to assist them during these exercises.

TRAINING SESSION/tool – **results**

Positive result was recorded. 1) Participants used Nessus hands-on tool. 2) Participants were able to successfully finish the given practical scenario exercises

TRAINING SESSION/tool – **demographics**

Info about:
Total number of persons: 40
Nationalities: Finland, the Netherlands, Russia, Estonia, Vietnam, India, Turkey
Level of education: Graduate students in cybersecurity and tutors
Group ages: 18-29 , 30-39
Gender groups: 80% Male, 20% Female

CyberSecPro Training Program Analysis
Training Session – Tool Evaluation report

Tool Name: NMAP for Penetration Testing **Date:** 18/10/2023 **Duration:** 65 min Training + 3H Exercises

Tool Offered by: Leo Johannesberg, Paresh Rathod & Paulinus Ofem

Provider's (Trainer) Report

TRAINING SESSION/tool - **Introduction**

Nmap is an indispensable open-source tool for network discovery and security auditing. The session target is network enumeration, scanning techniques, and security concepts. Nmap allows professionals to find out which devices are running on network. The training is providing participants to have a basic understanding of networking and cybersecurity concepts within the knowledge areas of penetration testing, networks, and communication security.

TRAINING SESSION/tool – **learning outcomes**

Mark all that apply for the tool:

- □ Understand viruses, worms, Trojans, ransomware, and spyware.
- □ Perform malware detection and analysis using malware detection tools.
- ☑ Perform static and dynamic malware analysis.
- □ Sandbox and virtualize malware for analysis.
- □ Reverse engineer malware behavior.
- □ Identify and respond to malware attacks using IOCs and threat intelligence feeds.
- □ Anti-malware and best practices protect systems and networks.
- ☑ Investigate unusual network behavior using network traffic analysis techniques.
- □ Memory forensics tools can analyze volatile data and detect live system attacks.
- □ Recover and analyze hacked system data with disk forensics tools.
- □ Windows, macOS, and Linux forensics.
- □ Use digital forensics to track criminals.
- □ Malware detection and forensic analysis include legal and ethical issues.
- □ Present malware detection and forensic investigation results clearly.
- □ Keep up with malware detection and forensic analysis developments and dangers.
- □ OTHER: Please specify ______________________________
- □ OTHER: Please specify ______________________________

□ OTHER: Please specify ___________________________________

□ OTHER: Please specify ___________________________________

□ OTHER: Please specify ___________________________________

□ OTHER: Please specify ___________________________________

TRAINING SESSION/tool - **demonstration** / (supplementary material)

The Nmap (Network Mapper) demonstration involved real-time scanning of a controlled environment. Attendees were shown how to identify connected devices, their offered services in recorded video. Supplementary slides included screenshots of command outputs and the relevance of each command in real-world scenarios in short video recording.

TRAINING SESSION/tool - **mock exercises and group work** / (supplementary material)

Participants were divided into groups. Each participant was given access to a mock network. First, participants watch the Nmap ppt slides and live hands-on section. Participants were tasked with discovering devices and identifying open ports using Nmap. Supplementary material included task sheets detailing specific objectives for each group. https://youtu.be/fJkVT7myHxg

TRAINING SESSION/tool – **results**

Positive result was recorded. 1) Participants used Nmap to scan TCP-FTP connects. 2) Participants were able to successfully identify open ports 3) Participants were able to create report of investigation.

TRAINING SESSION/tool – **demographics**

Info about:
Total number of persons: 40
Nationalities: Finland, Netherland, Russia, Estonia, Vietnam, India, Turkish
Level of education: Graduate students in cybersecurity and tutors
Group ages: 18-29 , 30-39
Gender groups: 80% Male, 20% Female

CyberSecPro Training Program Analysis Training Session – Tool Evaluation report

Tool Name: ____________SmartViz-DMT__Date:26/09/2023____________ Duration:_70minutes________

Tool Offered by: ZELUS___________________________________

Provider's (Trainer) Report

TRAINING SESSION/tool - Introduction

Brief summary of the training session. Focus on tool, topic, learning objectives, prior knowledge. This course has been crafted to immerse attendees in cybersecurity experience via a direct and practical training regimen, using SmartViz DMT. The main usage of SmartViz in this training session is to as a SIEM aggregator, collecting data from multiple sources for improved further analysis (ELK, MISP, Zeek). The training incorporates a Red Team/Blue Team exercise, with the Red Team comprised of offensive security specialists aiming to infiltrate an organization's cybersecurity defenses, while the Blue Team works diligently to defend against and thwart these incursions. The training's primary focus lies in nurturing the Blue Team's perspective, emphasizing the application of digital forensics methodologies to bolster defense strategies. Tailored for individuals with fundamental knowledge in the cybersecurity domain, this session assumes a baseline understanding of cybersecurity basics.

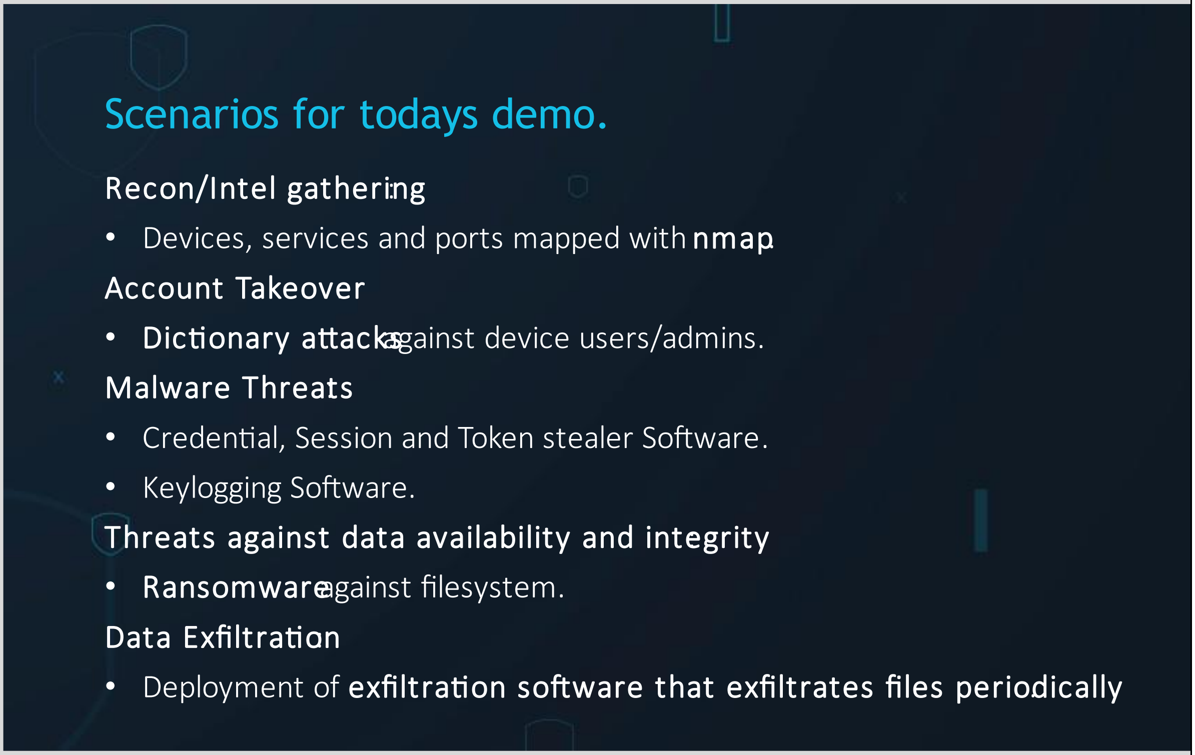
TRAINING SESSION/tool – learning outcomes

Mark all that apply for the tool:
√ Understand viruses, worms, Trojans, ransomware, and spyware.
Perform malware detection and analysis using malware detection tools.
Perform static and dynamic malware analysis.
Sandbox and virtualize malware for analysis.
Reverse engineer malware behavior.
√ Identify and respond to malware attacks using IOCs and threat intelligence feeds.
Anti-malware and best practices protect systems and networks.
√ Investigate unusual network behavior using network traffic analysis techniques.
√ Memory forensics tools can analyze volatile data and detect live system attacks.
Recover and analyze hacked system data with disk forensics tools.
Windows, macOS, and Linux forensics.
Use digital forensics to track criminals.
√ Malware detection and forensic analysis include legal and ethical issues.
√ Present malware detection and forensic investigation results clearly.
√ Keep up with malware detection and forensic analysis developments and dangers.
OTHER: Please specify ______________________________
OTHER: Please specify ______________________________
OTHER: Please specify ______________________________
OTHER: Please specify ______________________________
OTHER: Please specify ______________________________
OTHER: Please specify ______________________________

TRAINING SESSION/tool - demonstration / (supplementary material)

Short description about the demo of the training tool. If supplementary material (slides) is available, then should be included.
In the live demonstration of the training tool was a dynamic experience that started with simulated attacks on a victim laptop, setting the stage for an in-depth exploration of cybersecurity concepts. The session began with an introduction to the Security Information and Event Management (SIEM) framework, showcasing the integrated tools. Subsequently, the focus shifted to the Red Team's attacks, with a detailed explanation of the tactics employed. Participants gained valuable insights into offensive strategies and learned about various attack vectors. Finally, the session delved into the realm of digital forensics, demonstrating the methods

employed by the Blue Team to analyze and identify threats using the training tool. This comprehensive approach provided participants with an understanding of both offensive and defensive cybersecurity techniques, enhancing their overall expertise in the field.



Scenarios for todays demo.

Recon/Intel gathering

- Devices, services and ports mapped with **nmap**.

Account Takeover

- **Dictionary attacks** against device users/admins.

Malware Threats

- Credential, Session and Token stealer Software.
- Keylogging Software.

Threats against data availability and integrity

- **Ransomware** against filesystem.

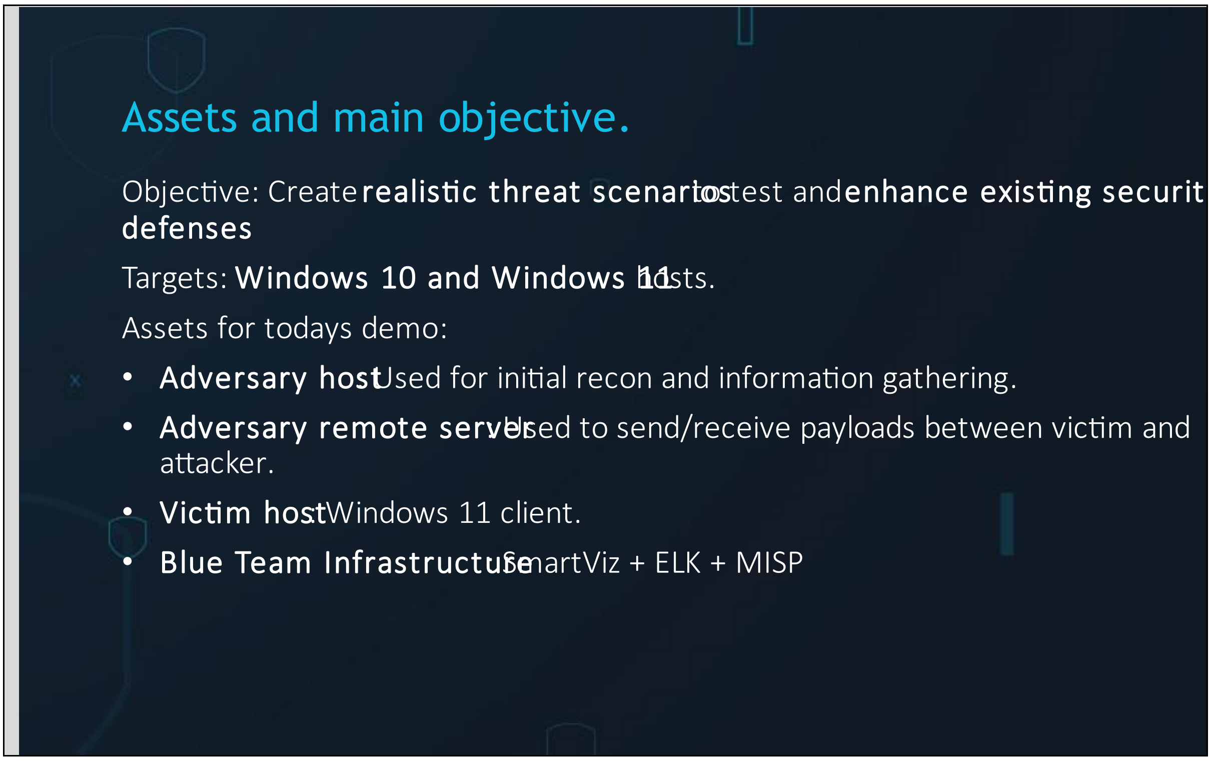
Data Exfiltration

- Deployment of **exfiltration software that exfiltrates files periodically**

TRAINING SESSION/tool - mock exercises and group work / (supplementary material)

Short description about the set-up of the training session. If supplementary material (slides) is available, then include it.

In this simulation setup, three laptops were utilized: one Windows laptop running the SmartViz Tool connected to a projector, demonstrating the tool's functionality for the Blue Team simulation. A second Windows 11OS laptop served as the victim machine, where the simulated attacks were executed. The third laptop, operating on a Linux OS, functioned as the Red Team, orchestrating the attacks in this simulation scenario.



Assets and main objective.

Objective: Create realistic threat scenarios to test and enhance existing securit defenses

Targets: Windows 10 and Windows 11 hosts.

Assets for todays demo:

- Adversary host: Used for initial recon and information gathering.
- Adversary remote server: Used to send/receive payloads between victim and attacker.
- Victim host: Windows 11 client.
- Blue Team Infrastructure: SmartViz + ELK + MISP

TRAINING SESSION/tool – results

Brief summary of the major outcomes of the training session. Focus on the methodology, the steps and the highlights.

Certainly, the training session yielded significant outcomes, marked by a comprehensive methodology, structured steps, and noteworthy highlights. The session commenced with an introduction to the Security Information and Event Management (SIEM) framework, laying the foundation for understanding integrated tools. The simulated attacks, orchestrated on a victim laptop, allowed participants to grasp offensive strategies. Notable steps included the detailed explanation of Red Team attacks, showcasing various tactics and attack vectors. The session's highlight was the live digital forensics experience, revealing the intricate methods employed by the Blue Team to analyze threats using the training tool.

TRAINING SESSION/tool – demographics

Info about:
Total number of persons : 5
Nationalities: Greek
Level of education [undergraduate student , BSc, postgraduate student (20%) , MSc(20%), PhD student(20%), PhD(40%)]
Group ages [18-29 (20%), 30-39(60%), 40-49, 50-59 (20%), 60-...]
Gender groups [80 Male, 20 Female]

CyberSecPro Training Program Analysis Training Session – Tool Evaluation report

Tool Name: ___ objdump - gdb ___ Date:___ 16/05/2023 ____ Duration:____2h____

Tool Offered by: _____OPEN SOURCE - UPRC______

Provider's (Trainer) Report – Koutras Dimitris

TRAINING SESSION/tool - Introduction

Learning objectives: Binary debugging, Buffer overflow exploit.
Prior knowledge and tools needed by trainees: Good knowledge of assembly and C
Description of syllabus: This training session presented a real case scenario of black box penetration testing against a binary. The first half hour was spent testing the capabilities of the binary, then we used the gdb tool to understand the structure of the binary. In the second session we use our findings to find the vulnerability. The last part was the exploitation.

TRAINING SESSION/tool – learning outcomes

Mark all that apply for the tool:
Understand viruses, worms, Trojans, ransomware, and spyware.
Perform malware detection and analysis using malware detection tools.
Perform static and dynamic malware analysis.
Sandbox and virtualize malware for analysis.
Reverse engineer malware behavior.
Identify and respond to malware attacks using IOCs and threat intelligence feeds.
Anti-malware and best practices protect systems and networks.
Investigate unusual network behavior using network traffic analysis techniques.
Memory forensics tools can analyze volatile data and detect live system attacks.
Recover and analyze hacked system data with disk forensics tools.
Windows, macOS, and Linux forensics.
Use digital forensics to track criminals.
Malware detection and forensic analysis include legal and ethical issues.
Present malware detection and forensic investigation results clearly.
Keep up with malware detection and forensic analysis developments and dangers.
OTHER: Memory analysis by hand ____________________________________
OTHER: Memory analysis with open source tools________________________
OTHER: Please specify ____
OTHER: Please specify ____
OTHER: Please specify ____
OTHER: Please specify ____

TRAINING SESSION/tool - demonstration / (supplementary material)

GDB, or the GNU Debugger, is a powerful and widely used command-line tool for debugging software programs on Unix-like operating systems.

TRAINING SESSION/tool - mock exercises and group work / (supplementary material)

Binary enumeration
Setting Breakpoints
Stepping through code
Examining variables
Breakpoint conditions

Memory inspection
Debugging

TRAINING SESSION/tool – results

We exploit a binary (black box). Then we patch the memory bug

TRAINING SESSION/tool – demographics

Info about:
Total number of persons: 6
Nationalities: Greek.
Level of education [undergraduate student, BSc, postgraduate student, MSc, PhD student, PhD(100%)
Group ages [18-29, 30-39, {40-49, 50-59, 60-…(100%)}]
Gender groups [100% Male, % Female]

CyberSecPro Training Program Analysis Training Session – Tool Evaluation report

Tool Name: __________Snort – Ossec ______________ Date: ______24/05/2023______
Duration:___ 2.30 h___

Tool Offered by: ____________OPEN SOURCE - UPRC__________________

Provider's (Trainer) Report – Koutras Dimitris

TRAINING SESSION/tool - Introduction

We start with an introduction to IDS. Then we install the Snort IDS and we cover a lot of technical details about how the snort IDS works. Then we test it by intercepting malicious traffic. After that, there was a detailed session on the Snort rules. Finally, we discuss the Ossec IDS with an example.

TRAINING SESSION/tool – learning outcomes

Mark all that apply for the tool:
Understand viruses, worms, Trojans, ransomware, and spyware.
Perform malware detection and analysis using malware detection tools.
Perform static and dynamic malware analysis.
Sandbox and virtualize malware for analysis.
Reverse engineer malware behavior.
Identify and respond to malware attacks using IOCs and threat intelligence feeds.
Anti-malware and best practices protect systems and networks.
Investigate unusual network behavior using network traffic analysis techniques.
Memory forensics tools can analyze volatile data and detect live system attacks.
Recover and analyze hacked system data with disk forensics tools.
Windows, macOS, and Linux forensics.
Use digital forensics to track criminals.
Malware detection and forensic analysis include legal and ethical issues.
Present malware detection and forensic investigation results clearly.
Keep up with malware detection and forensic analysis developments and dangers.
OTHER: Please specify ____
OTHER: Please specify ____
OTHER: Please specify ____
OTHER: Please specify ____
OTHER: Please specify ____
OTHER: Please specify ____

TRAINING SESSION/tool - demonstration / (supplementary material)

You can find it in
https://drive.google.com/file/d/10zgzwDYbmlmMulNSzP2I6ASoZjH3V4sf/view?usp=share_link

TRAINING SESSION/tool - mock exercises and group work / (supplementary material)

You can find it in https://drive.google.com/file/d/10zgzwDYbmlmMulNSzP2I6ASoZjH3V4sf/view?usp=share_link.

TRAINING SESSION/tool – results

You can find it in https://drive.google.com/file/d/10zgzwDYbmlmMulNSzP2I6ASoZjH3V4sf/view?usp=share_link

TRAINING SESSION/tool – demographics

Info about:
Total number of persons = 10
Nationalities: Greece - German
Level of education [undergraduate student (10%), BSc, postgraduate student, MSc(60%), PhD student(10%), PhD(20%)
Group ages [from 20 to 35]
Gender groups [80% Male, 20% Female]

CyberSecPro Training Program Analysis Training Session – Tool Evaluation report

Tool Name: ***X - Certificate and Key management, XCA tool*** Date: 26-Sep-2023 Duration: 60 min

Training Session Offered by: Cristina Alcaraz, University of Malaga

Provider's (Trainer) Report

TRAINING SESSION/tool - **Introduction**

In this training session, the XCA (X Certificate and Key management) tool is presented with an estimated time of 1h. XCA is an open-source tool[1] capable of creating and managing X.509 certificates, allowing learners to understand the role of the Certificate Authority (CA) and its main operations, as well as the role of end users requesting digital certificates. Thus, it is very useful for those knowledge areas that require the generation of digital certificates to, for example, establish client-server communications.

Basically, the tool is based on user-friendly interfaces and uses various standardized formats to manage the user's private keys and X.509 certificates. In this process, trainees will generate certificates, assign information to these certificates and certify them through an authority. Therefore, some prior knowledge about cryptography (especially that related to public key cryptography) and digital certificates (X.509) is necessary to understand and follow the programmed activities for this session training.

TRAINING SESSION/tool – **learning outcomes**

Mark all that apply for the tool:
Understand viruses, worms, Trojans, ransomware, and spyware.
Perform malware detection and analysis using malware detection tools.
Perform static and dynamic malware analysis.
Sandbox and virtualize malware for analysis.
Reverse engineer malware behavior.
Identify and respond to malware attacks using IOCs and threat intelligence feeds.
Anti-malware and best practices protect systems and networks.
Investigate unusual network behavior using network traffic analysis techniques.
Memory forensics tools can analyze volatile data and detect live system attacks.
Recover and analyze hacked system data with disk forensics tools.
Windows, macOS, and Linux forensics.
Use digital forensics to track criminals.
Malware detection and forensic analysis include legal and ethical issues.
Present malware detection and forensic investigation results clearly.
Keep up with malware detection and forensic analysis developments and dangers.
X OTHER: Understand the process required to generate digital certificates.
X OTHER: Perform the operations required to generate and certify digital certificates.
OTHER: Please specify ____
OTHER: Please specify ____
OTHER: Please specify ____
OTHER: Please specify ____

TRAINING SESSION/tool - **demonstration** / (supplementary material)

[1] XCA: open-source tool located at https://www.hohnstaedt.de/xca

The tool will be presented following a live demonstration, in which the trainees will actively follow the trainer's guidance in order to address the following training points or topics:
How to prepare the tool for its general use
How to generate private keys
How to generate digital certificates, including self-signed ones
How to prepare and use templates
How to generate certificate revocation lists and revoke certificates

To follow the demonstration, each trainee should previously have installed:
The XCA tool, which can be downloaded from https://www.hohnstaedt.de/xca/index.php/download.
Latest stable version: XCA 2.4.0; suitable for platforms: Mac and Windows
The Word tool for generating PDF files, and the Adobe tool for signing PDF files.
In addition, connection to the Internet is required to send e-mails.

For this session, the trainer provides supplementary training material (slides) as a support tool for the trainees, and a guide for the trainer during her session.

TRAINING SESSION/tool - **mock exercises and group work** / (supplementary material)

As previously mentioned, the session training will be based on a live demonstration addressing a set of topics about how to use the tool and how to generate standardized digital certificates X.509, considering the different roles (CAs and users).

The training methodology and the scheduling of the session will consist in:
Explaining the goals of the session and the tool. Estimated time: 5 min.
Explaining how to use the tool, following a live demonstration. Estimated time: 25 min.
Carrying out two particular practical exercises, one in a group and one individually. Estimated time: 30 min. Note that the second exercise is only addressed if time permits.

Therefore, the session training will be composed of two main blocks:
Block 1: presentation and live demonstration of XCA. Estimated time: 30 min.
Block 2: practical exercises, one focusing on group work and the other on individual work. Estimated time: 30 min. Note that the second exercise is only addressed if time permits.

Regarding Block 2, two activities will be executed:
Exercise 1 – group work: in groups of two, each trainee in the group will act as either a CA or a user, and will execute a set of actions that will require: 1) creating (self-signed) certificates, 2) signing certificates, 3) requesting revocation, and 4) exporting certificates.
Exercise 2 – individual work: each trainee will put the knowledges learnt into practice again by creating a self-signed certificate and signing a PDF file.

TRAINING SESSION/tool – **results**

The major outcomes of the training session are:
To understand how to use the tool to generate standardized certificates, and its usefulness for multiple applications such as configuring TLS clients/servers.
To Interact in society and enhance communication, leading various actions and roles.

As above state, the training session methodology will be focused on:
Explaining the goals of the session and the tool. Estimated time: 5 min.

Explaining how to use the tool, following a live demonstration. Estimated time: 25 min. Carrying out two particular practical exercises, one in a group and one individually. Estimated time: 30 min. Note that the second exercise is only addressed if time permits. Thus, the methodology is based on a masterclass session with a live demonstration, and subsequently a practical session based on two different types of activities. As also mentioned above, it is required to have installed a set of tools prior to the session.

TRAINING SESSION/tool – **demographics**

CyberSecPro Training Program Analysis Training Session – Tool Evaluation report

Tool Name: gdb Date: 26/9/2023 Duration: 45 minutes

Tool Offered by: UCY

Provider's (Trainer) Report

TRAINING SESSION/tool - **Introduction**

The seminar discusses how modern debuggers, like GNU gdb, realize software breakpoints.

TRAINING SESSION/tool – **learning outcomes**

Mark all that apply for the tool:
Understand viruses, worms, Trojans, ransomware, and spyware.
X Perform malware detection and analysis using malware detection tools.
X Perform static and dynamic malware analysis.
Sandbox and virtualize malware for analysis.
Reverse engineer malware behavior.
Identify and respond to malware attacks using IOCs and threat intelligence feeds.
Anti-malware and best practices protect systems and networks.
Investigate unusual network behavior using network traffic analysis techniques.
Memory forensics tools can analyze volatile data and detect live system attacks.
Recover and analyze hacked system data with disk forensics tools.
Windows, macOS, and Linux forensics.
Use digital forensics to track criminals.
Malware detection and forensic analysis include legal and ethical issues.
Present malware detection and forensic investigation results clearly.
Keep up with malware detection and forensic analysis developments and dangers.
OTHER: Please specify ____
OTHER: Please specify ____
OTHER: Please specify ____
OTHER: Please specify ____
OTHER: Please specify ____
OTHER: Please specify ____

TRAINING SESSION/tool - **demonstration** / (supplementary material)

There are two programs that are demonstrated (a) a simplified strace(1) tool, and (b) an example code for setting and triggering a software breakpoint. Code is attached below.

TRAINING SESSION/tool - **mock exercises and group work** / (supplementary material)

Short description about the set-up of the training session. If supplementary material (slides) is available, then include it.

TRAINING SESSION/tool – **results**

TRAINING SESSION/tool – **demographics**

Info about:
Total number of persons
Nationalities: List ALL.
Level of education [undergraduate student (e.g. 10% or number of persons), BSc, postgraduate student, MSc, PhD student, PhD
Group ages [18-29 (e.g. 10% or number of persons), 30-39, 40-49, 50-59, 60-…]
Gender groups [% Male, % Female]

CyberSecPro Training Program Analysis Training Session – Tool Evaluation report

Tool Name: ____________________C2M ___________________ Date: __26 Sep_2023_______ Duration:_1h___

Tool Offered by: _______________trustilio

Provider's (Trainer) Report

TRAINING SESSION/tool - **Introduction**

Brief summary of the training session. Focus on tool, topic, learning objectives, prior knowledge.

The benefits of Source Code Quality Analysis, Classification of Code Risks, Planning Risk Mitigation

TRAINING SESSION/tool – **learning outcomes**

Mark all that apply for the tool:
Understand viruses, worms, Trojans, ransomware, and spyware.
Perform malware detection and analysis using malware detection tools.
Perform static and dynamic malware analysis.
Sandbox and virtualize malware for analysis.
Reverse engineer malware behavior.
Identify and respond to malware attacks using IOCs and threat intelligence feeds.
Anti-malware and best practices protect systems and networks.
Investigate unusual network behavior using network traffic analysis techniques.
Memory forensics tools can analyze volatile data and detect live system attacks.
Recover and analyze hacked system data with disk forensics tools.
Windows, macOS, and Linux forensics.
Use digital forensics to track criminals.
Malware detection and forensic analysis include legal and ethical issues.
Present malware detection and forensic investigation results clearly.
Keep up with malware detection and forensic analysis developments and dangers.
OTHER: Please specify ______Static Application Security Test (SAST)________
OTHER: Please specify ______SOFTWARE COMPOTION ANALYSIS (SCA)_____
OTHER: Please specify ______AUTOMATED CODE REVIEWS_______________
OTHER: Please specify ____
OTHER: Please specify ____
OTHER: Please specify ____

TRAINING SESSION/tool - **demonstration** / (supplementary material)

Short description about the demo of the training tool. If supplementary material (slides) is available, then should be included.

c2m is a suite of static code analysis tools assess the code quality and the security of a source code base. c2m is unique in its ability to comprehensively assess the quality, security, and compliance of source code. It has been purpose-built from the ground up to provide a holistic evaluation of the codebase, from the initial stages of development through to the final product.

https://www.codewetrust.com/test-cases

TRAINING SESSION/tool - **mock exercises and group work** / (supplementary material)

Short description about the set-up of the training session. If supplementary material (slides) is available, then include it.
CyberSecPro-Code Quality Audit Trustilio

TRAINING SESSION/tool – **results**

Brief summary of the major outcomes of the training session. Focus on the methodology, the steps and the highlights.
Detect vulnerabilities on proprietary and 3rd party code, inspect associated Security Advisories, Risk Mitigation plan

TRAINING SESSION/tool – **demographics**

Info about:
Total number of persons
Nationalities: List ALL.
Level of education [undergraduate student (e.g. 10% or number of persons), 100%PhD
Group ages [18-29 (e.g. 10% or number of persons),100% 30-39
Gender groups 50% Male, 50% Female

CyberSecPro Training Program Analysis Training Session – Tool Evaluation report

Tool Name: Wazuh and Metadon (PDM SIEM) ______________ Date: 26/08/2023________
Duration: 60 minutes

Tool Offered by: Open Source____

Provider's (Trainer) Report

TRAINING SESSION/tool - **Introduction**

In this training session, we will delve into the world of security information and event management (SIEM) with a specific focus on Wazuh. Wazuh is a robust open-source SIEM tool widely recognized for its capabilities in intrusion detection and security monitoring. This session is designed to cater to participants who already possess a foundational understanding of security concepts and basic Linux skills, as Wazuh is typically deployed on Linux systems. We will also introduce Metadon (PDM SIEM), highlighting its significance in the context of Linux logs, the Windows Event Viewer, and SYSMON. Our aim is to equip attendees with the knowledge and skills necessary to effectively utilize Wazuh and Metadon for proactive security monitoring and intrusion detection. This training will encompass installation, configuration, use cases, and best practices, ensuring participants leave with a solid grasp of SIEM principles and practical application.

TRAINING SESSION/tool – **learning outcomes**

Mark all that apply for the tool:
X Understand viruses, worms, Trojans, ransomware, and spyware.
Perform malware detection and analysis using malware detection tools.
Perform static and dynamic malware analysis.
Sandbox and virtualize malware for analysis.
Reverse engineer malware behavior.
X Identify and respond to malware attacks using IOCs and threat intelligence feeds.
Anti-malware and best practices protect systems and networks.
X Investigate unusual network behavior using network traffic analysis techniques.
Memory forensics tools can analyze volatile data and detect live system attacks.
Recover and analyze hacked system data with disk forensics tools.
X Windows, macOS, and Linux forensics.
X Use digital forensics to track criminals.
Malware detection and forensic analysis include legal and ethical issues.
Present malware detection and forensic investigation results clearly.
Keep up with malware detection and forensic analysis developments and dangers.
OTHER: Please specify ____
OTHER: Please specify ____
OTHER: Please specify ____
OTHER: Please specify ____
OTHER: Please specify ____
OTHER: Please specify ____

TRAINING SESSION/tool - **demonstration** / (supplementary material)

Tool Exploration: The demo will begin with an exploration of the Wazuh user interface and its various components, including the Wazuh manager, agents, and the Kibana dashboard.

Log Analysis: The demo will showcase how logs are retrieved and the rule-based log analysis system operates in real-time. This includes the identification of security events and the generation of alerts.

Customization: Attendees will see how Wazuh can be customized to meet specific security requirements. This includes the creation and modification of rules to adapt to unique organizational needs.

Incident Response: The demo will cover the incident response capabilities of Wazuh, highlighting how it assists in the investigation of alerts and the containment of security incidents.

TRAINING SESSION/tool - **mock exercises and group work** / (supplementary material)

Accompanying the demo, participants will have access to presentation slides that provide additional context, detailed instructions, and visual aids. These slides will reinforce the key concepts demonstrated during the session and serve as valuable reference material for future use.

TRAINING SESSION/tool – **results**

The audience's interest in using Wazuh as an open-source SIEM tool, primarily driven by their lack of plans to employ commercial solutions internally, underscores their desire to explore the capabilities of SIEM in a more cost-effective manner. This signifies a conscious effort to leverage open-source alternatives to meet their security monitoring and intrusion detection needs. Additionally, the introduction of Windows forensics using tools like Event Viewer and SYSMON was a valuable addition to their knowledge base, as it expanded their understanding of how to monitor and analyze security-related data on Windows systems. This newfound knowledge has the potential to enhance their overall security posture and response capabilities. The training session seems to have successfully addressed their specific needs and interests in the realm of SIEM and security monitoring.

TRAINING SESSION/tool – **demographics**

Info about:
Total number of persons: 15-20
Nationalities: Greece, Denmark, Portugal, Spain,
Level of education [undergraduate student (50%), BSc (10%), postgraduate student (10%), MSc (10%), PhD student (30%), PhD (30%)
Group ages [18-29 (50%), 30-39 (20%), 40-49 (20%), 50-59 (10%)]
Gender groups [% 85 Male, % 15 Female]

CyberSecPro Training Program Analysis Training Session – Tool Evaluation report

Tool Name: Security Infusion Date: 12/10/2023 Duration: 1 h

Tool Offered by: ITML

Provider's (Trainer) Report

TRAINING SESSION/tool - **Introduction**

This training session aims to introduce trainees to the main features and capabilities of ITML's Security Infusion complete software package. Security Infusion is an all-in-one solution, leveraging a plethora of the state-of-the-art technologies delivered by a security experts' team. Its main features are:

Monitoring of critical infrastructure 24x7 through a single dashboard – drill down to a low-level historical event when needed!

Endpoint protection by taking security to the edge. With the Security Infusion agents, the initial data collection and evaluation takes place on the edge device.

Alerting & Reporting via notifications via email or slack account about malicious activity. Export reports for the systems' status identifying new vulnerabilities with actionable feedback.

Forensics investigation of historical data and identification of the series of events that caused an incident. Security Infusion then acts to restore and secure against the identified root cause.

This training session is divided into the following sub-sessions:

SIEM concepts and benefits, with a focus to Security Infusion extended capabilities

Security baseline per operating system (Windows, Linux, macOS)

Threat intelligence (tools and frameworks, security intelligence, endpoint protection)

Data loss prevention (data security and protection, data protection best practices)

Scanning for threats (vulnerability assessment, port scanning, etc)

An overview of Security Infusion features and offerings

Demonstration training on deploying parts of Security Infusion; the goal is to identify patterns, get to know the infrastructure and processes, and identify a security incident.

Important prior knowledge to this session comprises the following:

IT Security vs Information Security, roles in Security

Software application security (common threats and attacks, prevention and defense, security patterns).

TRAINING SESSION/tool – **learning outcomes**

Mark all that apply for the tool:

Understand viruses, worms, Trojans, ransomware, and spyware.

☒ Perform malware detection and analysis using malware detection tools.

Perform static and dynamic malware analysis.

Sandbox and virtualize malware for analysis.

Reverse engineer malware behavior.

☒ Identify and respond to malware attacks using IOCs and threat intelligence feeds.

☒ Anti-malware and best practices protect systems and networks.

Investigate unusual network behavior using network traffic analysis techniques.

☒ Memory forensics tools can analyze volatile data and detect live system attacks.

Recover and analyze hacked system data with disk forensics tools.

☒ Windows, macOS, and Linux forensics.

Use digital forensics to track criminals.
Malware detection and forensic analysis include legal and ethical issues.
☒ Present malware detection and forensic investigation results clearly.
Keep up with malware detection and forensic analysis developments and dangers.
☒ OTHER: Please specify _______Monitoring for misconfigured OS/SW settings
OTHER: Please specify ______________________________________
OTHER: Please specify ______________________________________
OTHER: Please specify ______________________________________
OTHER: Please specify ______________________________________
OTHER: Please specify ______________________________________

TRAINING SESSION/tool - **demonstration** / (supplementary material)

Short description about the demo of the training tool. If supplementary material (slides) is available, then should be included.
The demo is performed online. It entails a series of steps from setting up the agents and master agents to customize the system for targeted information and to visualize the results of the security assessment via intuitive and interactive interfaces.

TRAINING SESSION/tool - **mock exercises and group work** / (supplementary material)

Short description about the set-up of the training session. If supplementary material (slides) is available, then include it.
The mock exercise entails the following steps:
Admin panel set up: Agent & Master Agents installation and configuration
Reports panel: selection of nodes, time period, minimum severity level, report type
Reports panel: visualization of intuitive graphs on monitoring and alerting functionality
Monitoring panel: after the selection of agent and time range, visualization of (i) processes, (ii) CPU usage, (iii) available RAM, (iv) physical disks reads/writes/queue, (v) paging file usage, (vi) handle/threat count, (vii) processes queue, (viii) kbits received/sent
Event analyser: a list on all labelled event, including event type, occurrences, severity level and last occurrence
Visualisation of security configuration assessment via the dashboard: online agents, services, labelled events, top events by security, event count, maximum event security level
Run policy scan (optional).

TRAINING SESSION/tool – **results**

Brief summary of the major outcomes of the training session. Focus on the methodology, the steps and the highlights.

The trainees are able to understand basic concepts of security and SIEMs, special features offered by the Security Infusion comprehensive solution and how the latter can be set up and applied in a demonstration scenario. The session commences with an introduction to basic principles of security (e.g., threat intelligence, data loss prevention, etc), which lays the foundation for presenting Security Infusion’s features and capabilities. The session continues with a demonstration of the solution, covering all the steps from installing and configuring agents and master agents, selecting nodes to apply the solution to, running the software and monitoring important information on the security status of the system.

TRAINING SESSION/tool – **demographics**

Info about:
Total number of persons: 5
Nationalities: Greek
Level of education [undergraduate student, BSc, postgraduate student, MSc (20%), PhD student (20%), PhD (60%)
Group ages [18-29 (40%), 30-39, 40-49 (20%), 50-59 (40%), 60-…]
Gender groups [85% Male, 15% Female]

CyberSecPro Training Program Analysis Training Session – Tool Evaluation report

Tool Name: Pentest Methodology Date: 12/10/2023

Duration: 1h

Tool Offered by: COFAC

Provider's (Trainer) Report

TRAINING SESSION/tool - **Introduction**

COFAC Training “Penetration Testing Methodology" training session. In this session, we will provide an overview of penetration testing and the methodology used by cybersecurity professionals to identify vulnerabilities in computer systems, networks, and applications.

Session Objective: By the end of this training session, you will have a fundamental understanding of penetration testing, its purpose, and the step-by-step methodology employed in the process. You will also gain insights into the essential tools and techniques used by penetration testers to assess the security of digital assets.

Agenda:
What is Penetration Testing?
Types of Penetration Testing
Penetration Testing Methodology
Tools and Techniques
Q&A and Discussion

Training Methodology:
Interactive presentations and discussions
Hands-on demonstrations of various penetration testing tools
Real-world examples and case studies
Q&A sessions for clarifying doubts and fostering discussions.

Who Should Attend:
This training session is suitable for IT professionals, cybersecurity enthusiasts, network administrators, and anyone interested in understanding the fundamentals of penetration testing. No prior experience is required.

Prerequisites:
A basic understanding of computer networks, security concepts, and operating systems would be beneficial but is not mandatory.

TRAINING SESSION/tool – **learning outcomes**

Mark all that apply for the tool:

☒ Understand viruses, worms, Trojans, ransomware, and spyware.
Perform malware detection and analysis using malware detection tools.
Perform static and dynamic malware analysis.
☒ Sandbox and virtualize malware for analysis.
Reverse engineer malware behavior.

☒ Identify and respond to malware attacks using IOCs and threat intelligence feeds.
Anti-malware and best practices protect systems and networks.
☒ Investigate unusual network behavior using network traffic analysis techniques.
☒ Memory forensics tools can analyze volatile data and detect live system attacks.
☒ Recover and analyze hacked system data with disk forensics tools.
Windows, macOS, and Linux forensics.
☒ Use digital forensics to track criminals.
Malware detection and forensic analysis include legal and ethical issues.
Present malware detection and forensic investigation results clearly.
Keep up with malware detection and forensic analysis developments and dangers.
OTHER: Please specify ____
OTHER: Please specify ____
OTHER: Please specify ____
OTHER: Please specify ____

TRAINING SESSION/tool - **demonstration** / (supplementary material)

Short description about the demo of the training tool. If supplementary material (slides) is available, then should be included:
The session is performed online and in classroom and enables trainees to immerse in a digital laboratory where they can use tools in a sandbox environment and test a multitude of technological solutions and scenarios. Trainees will explore several external systems and networks mapping and evaluating the risk of intrusion by identifies soft sports of the infrastructure.

TRAINING SESSION/tool - **mock exercises and group work** / (supplementary material)

Short description about the set-up of the training session. If supplementary material (slides) is available, then include it.
The mock exercises entail the following steps:
Certainly, here are some mock exercises and group work activities for your Penetration Testing Methodology training session:
Information Gathering
Vulnerability Scanning and Enumeration
Exploitation
Post-Exploitation
Real-World Case Study
Penetration Testing Reporting
These exercises and group activities are designed to provide participants with practical experience in penetration testing and reinforce the concepts covered in the training. They encourage teamwork, critical thinking, and hands-on application of the methodology., and they can be integrated with other tools and platforms to enhance the data collection process.

TRAINING SESSION/tool – **results**

Brief summary of the major outcomes of the training session. Focus on the methodology, the steps and the highlights.

Results of a Penetration Testing Methodology training session include improved knowledge, hands-on skills, proficiency in tools, and the ability to analyze real-world cases. Participants also gain reporting expertise, teamwork experience, ethical understanding, and readiness for practical application in cybersecurity.

TRAINING SESSION/tool – **demographics**

Info about:
Total number of persons: 10
Nationalities: Greek, Spanish, Portuguese, Estonian, Cyprus
Level of education MSc (20%), PhD student (20%), PhD (60%)
Group ages [18-29 (40%), 30-39, 40-49 (20%), 50-59 (40%), 60-…]
Gender groups [85% Male, 15% Female]

CyberSecPro Training Program Analysis Training Session – Tool Evaluation report

Tool Name: OSINT with Maltego Date: 12/10/2023
Duration: 1h

Tool Offered by: COFAC

Provider's (Trainer) Report

TRAINING SESSION/tool - **Introduction**

COFAC Training Maltego OSINT Session aims the training "hands-on" to grasp the ability to harness open-source intelligence, becoming vital skills for individuals and organizations alike. Maltego, a powerful and versatile data mining tool, is at the forefront of transforming open source data into actionable insights. This training session will equip treinees with the knowledge and skills to leverage Maltego for your OSINT needs.

Session Objectives:
Understanding Open Source Intelligence (OSINT): We will begin by exploring the fundamentals of OSINT, its significance in various domains, and how it contributes to informed decision-making and threat analysis.
Introduction to Maltego: Get acquainted with the Maltego platform, its features, and the role it plays in simplifying the collection, analysis, and visualization of open-source intelligence.
Data Collection and Transformation: Learn how to collect data from diverse sources and transform it into a structured format that can be used for analysis.
Entity and Link Analysis: Dive into the core of Maltego by understanding entities and links. You'll discover how to create and analyze these components to uncover hidden connections and insights.
Transforms and Integrations: Explore the power of Maltego's transforms and integrations. Discover how to access various data sources and automate data gathering tasks.
Case Studies: Examine real-world case studies that demonstrate how Maltego OSINT can be applied in various scenarios, including cybersecurity, digital forensics, and fraud prevention.
Best Practices and Legal Considerations: Learn about ethical and legal considerations in OSINT, as well as best practices to ensure responsible and effective data collection.

Who Should Attend:
This training session is designed for:
Security professionals
Digital forensics experts
Investigators and law enforcement
Threat analysts
Researchers
Anyone interested in enhancing their OSINT skills.

Prerequisites:
To make the most of this training, attendees should have basic computer skills and familiarity with online research. No prior experience with Maltego is required.

Session Format:
The training will consist of a combination of presentations, hands-on exercises, and interactive discussions. You'll have the opportunity to work on real-world scenarios and apply your knowledge in a supportive learning environment.

By the end of this training session, you will have the skills and confidence to leverage Maltego OSINT for uncovering hidden insights and connections that can aid your decision-making and analysis processes.

TRAINING SESSION/tool – **learning outcomes**

Mark all that apply for the tool:
Understand viruses, worms, Trojans, ransomware, and spyware.
Perform malware detection and analysis using malware detection tools.
Perform static and dynamic malware analysis.
Sandbox and virtualize malware for analysis.
Reverse engineer malware behavior.
☒ Identify and respond to malware attacks using IOCs and threat intelligence feeds.
Anti-malware and best practices protect systems and networks.
Investigate unusual network behavior using network traffic analysis techniques.
Memory forensics tools can analyze volatile data and detect live system attacks.
Recover and analyze hacked system data with disk forensics tools.
Windows, macOS, and Linux forensics.
☒ Use digital forensics to track criminals.
Malware detection and forensic analysis include legal and ethical issues.
Present malware detection and forensic investigation results clearly.
Keep up with malware detection and forensic analysis developments and dangers.
☒ OTHER: Please specify - Risk Assessment: Identify and map targets and assess their digital vulnerabilities, helping organizations strengthen their security against social engineering and phishing attacks.
☒ OTHER: Please specify - Threat Intelligence: Collection and analysis of threat intelligence data.
OTHER: Please specify ____
OTHER: Please specify ____
OTHER: Please specify ____
OTHER: Please specify ____
OTHER: Please specify ____

TRAINING SESSION/tool - **demonstration** / (supplementary material)

Short description about the demo of the training tool. If supplementary material (slides) is available, then should be included:
The session is performed online recurring to open-source data and information repositories to train the users with the artificial intelligence component of the tool and to access to Open Source data. The session is conducted with live demonstrations of the tool manipulation information and outsourcing patters and additional information.

TRAINING SESSION/tool - **mock exercises and group work** / (supplementary material)

Short description about the set-up of the training session. If supplementary material (slides) is available, then include it.
The mock exercises entail the following steps:
Entity and Link Analysis: Maltego represents data as entities (e.g., people, websites, email addresses) and links (connections between entities). Trainees will visualize and explore the relationships between these entities.

Transforms: Trainees will use Maltego for "transforms" to fetch data from different sources, such as social media platforms, public records, DNS databases, and more. Trainees will Transform and enable retrieving, process, and analyze data.
Visualization: Trainees will analyze visualization options, including graphs and charts, to help organizations understand complex data and relationships.
Integration: Trainees will use the tool for support and collect numerous data sources, and they can be integrated with other tools and platforms to enhance the data collection process.

TRAINING SESSION/tool – **results**

Brief summary of the major outcomes of the training session. Focus on the methodology, the steps and the highlights.

Maltego is a data analysis and visualization tool specializing in Open-Source INTelligence (OSINT). It allows trainees to investigate, collect, and visualize data from various sources, supports customization, and offers ethical and legal guidance. Multiple editions and cross-platform accessibility make it versatile, while a supportive user community enhances its user-friendliness.

TRAINING SESSION/tool – **demographics**

Info about:
Total number of persons: 10
Nationalities: Greek, Spanish, Portuguese, Estonian, Cyprus
Level of education MSc (20%), PhD student (20%), PhD (60%)
Group ages [18-29 (40%), 30-39, 40-49 (20%), 50-59 (40%), 60-...]
Gender groups [85% Male, 15% Female]

CyberSecPro Training Program Analysis
Training Session – Tool Evaluation report

Tool Name: Risk Assessment and Management Platform Date:16/10/23 Duration:1 hour

Tool Offered by: Security Lab Consulting(SLC)

Provider's (Trainer) Report

TRAINING SESSION/tool - Introduction

The aim of the training session is to provide demonstration and hands on practical for risk assessment and management using the platform provided by SLC. The tool relies on common security knowledge including CVSS 3.1 (vulnerability calculation), CAPEC (threat identification), CWE (Weakness identification) for analyzing the risks.

Learning Objective

- To provide learners with the ability to assess and manage cybersecurity risk
- To facilitate an understanding of SLC's risk management tool and open intelligence

Topics Covered

- Open Intelligence for Vulnerability Management

- Asset Identification and Visual Representation
- Individual and Cascading Risk Assessment and reporting
- Security Control Declaration and Customization

Prior knowledge

- Basic cyber security knowledge

TRAINING SESSION/tool – learning outcomes

Mark all that apply for the tool:

- □ Understand viruses, worms, Trojans, ransomware, and spyware.
- □ Perform malware detection and analysis using malware detection tools.
- □ Perform static and dynamic malware analysis.
- □ Sandbox and virtualize malware for analysis.
- □ Reverse engineer malware behavior.
- □ Identify and respond to malware attacks using IOCs and threat intelligence feeds.
- □ Anti-malware and best practices protect systems and networks.
- □ Investigate unusual network behavior using network traffic analysis techniques.
- □ Memory forensics tools can analyze volatile data and detect live system attacks.
- □ Recover and analyze hacked system data with disk forensics tools.
- □ Windows, macOS, and Linux forensics.
- □ Use digital forensics to track criminals.
- □ Malware detection and forensic analysis include legal and ethical issues.
- □ Present malware detection and forensic investigation results clearly.
- □ Keep up with malware detection and forensic analysis developments and dangers.
- □ OTHER: Risk assessment and management
- □ OTHER: Open intelligence for vulnerability management

TRAINING SESSION/tool - demonstration / (supplementary material)

Short description about the demo of the training tool. If supplementary material (slides) is available, then should be included.
The Platform automate the risk assessment and management activities and provide recommendations to organizations for the selection of the most appropriate control measure, indicating optimization practices, in order to minimize the expected potential loss of the identified risk. The key feature of the tool includes open intelligence, assess identification , attack scenario generation and visualization of asset modelling and cascading risks.

TRAINING SESSION/tool - mock exercises and group work / (supplementary material)

Demonstration of the tool using online portal

TRAINING SESSION/tool – results

Brief summary of the major outcomes of the training session. Focus on the methodology, the steps and the highlights.

The session initiates with basic information about risk management and common security knowledge including CWE, CAPEC and CVE. Then it continues with risk identification for any given scenario and link with the open intelligence to identify and assess the vulnerability so that suitable control can be identified to mitigate the risk.

TRAINING SESSION/tool – demographics

Info about:
Total number of persons: 29
Nationalities: UK, Nigeria, Kenya, USA, Germany, Greece, India
Level of education [MSc, PhD student]
Group ages [18-29]
Gender groups [86% male , 14% Female]

CyberSecPro Training Program Analysis
Training Session – Tool Evaluation report

Tool Name: RxB game

Date: 26.09.2023

Duration: ca. 50 min

Tool Offered by: Serious Games Interactive A/S

Provider's (Trainer) Report

TRAINING SESSION/tool - Introduction

As the manager of a team of tech savvy individuals your aim is to assess, identify and manipulate a networked systems security in order to win over an opponent who is directly trying to prevent you in this.

Red can train hackers and use an arsenal of offensive tools to complete their objectives. Blue on the other hand has to balance resources, employee training, and close vulnerability gaps before red discovers them.

No practical technical skill is required to play, however, it helps to know about cybersecurity terminology and concepts - if not, you will learn by failing.

Main learning objectives:

- Risk assessment, prioritisation and resource management
- Recognize the many different types of vulnerabilities
- Various attack vectors and strategies

- Various defensive mitigations and strategies

RxB aims to deliver more awareness within the following areas:

- Cyber security defenses require regular adjustment
- Promote Situation awareness by navigating through an active attack
- Familiarisation with Hacker- and Cyber-Defence-terminology

TRAINING SESSION/tool – learning outcomes

Mark all that apply for the tool:

Understand viruses, worms, Trojans, ransomware, and spyware.
Perform malware detection and analysis using malware detection tools.
Perform static and dynamic malware analysis.
Sandbox and virtualize malware for analysis.
Reverse engineer malware behavior.
Identify and respond to malware attacks using IOCs and threat intelligence feeds.
Anti-malware and best practices protect systems and networks.
Investigate unusual network behavior using network traffic analysis techniques.
Memory forensics tools can analyze volatile data and detect live system attacks.
Recover and analyze hacked system data with disk forensics tools.
Windows, macOS, and Linux forensics.
Use digital forensics to track criminals.
Malware detection and forensic analysis include legal and ethical issues.
Present malware detection and forensic investigation results clearly.
Keep up with malware detection and forensic analysis developments and dangers.
Cyber security defenses require regular adjustment
Familiarisation with Hacker- and Cyber-Defence-terminology
Promotion and Situation awareness by navigating through an active attack

TRAINING SESSION/tool - demonstration / (supplementary material)

Players either control Red or Blue in multiplayer mode. In Single player mode the AI controls the red team.

Red is an offensive team of hackers that tries to infiltrate and hack into Blue's network.

Blue is the defending team that tries to protect the network from attacks.The virtual domain is represented by a predefined asset graph.

Red will have to work all the way from reconnaissance through exploitation and persistency until they reach their objective

Blue on the other hand has to balance resources, employee training, and close vulnerability gaps before red discovers them.

TRAINING SESSION/tool - mock exercises and group work / (supplementary material)

Internet browser with online internet connection.

TRAINING SESSION/tool – results

In order to improve the training application in future releases we conducted a feedback session after the training session. Here valuable comments were presented and received. Such as that the game might be very much suited for managers to understand the impact of cybersecurity on their business and resource situation.

TRAINING SESSION/tool – demographics

Total number of persons: 12

Nationalities: Greek, Portuguese, Danish, American.

Level of education: 10% undergraduate student, 30% BSc, 20% postgraduate student, 5% MSc, 10% PhD student, 25% PhD

Group ages: 70% 18-29, 20% 30-39, 8% 40-49, 2% 50-59

Gender groups: 90% Male, 10 % Female

Tool Name: ___HtB platform___ Date:___ 29th September 2023____ Duration:____1 Day____

Tool Offered by: Hack the Box enterprise - UPRC, FP, Trustilio, TUC

Provider's (Trainer) Report – Tejas Patel, Christos Grigoriadis, Koutras Dimitris

TRAINING SESSION/tool - Introduction

The CyberHOT training program, based upon NATO Red Teaming knowledge and expertise, will enable the participants to implement various red-teaming methodologies and tools. Utilizing the dedicated labs by HacktheBox, a wide range of penetration testing scenarios will be showcased.

The aim is to raise the skills of the workforce to meet current and future cyber incidents and challenges.

An introductory session will cover popular red-teaming/penetration testing tools, along with basic steps followed in penetration testing methodologies. Having introduced a general methodology to penetration testing along with the tools to apply it, the participants will be introduced to the Dedicated labs of the Hack the Box platform where each participant will boot their own instances of attacker and target machines and pawn them along with the lecturers.

TRAINING SESSION/tool – learning outcomes

Mark all that apply for the tool:

- □ Understand viruses, worms, Trojans, ransomware, and spyware.
- □ Perform malware detection and analysis using malware detection tools.
- □ Perform static and dynamic malware analysis.
- ✓ Sandbox and virtualize malware for analysis.
- ✓ Reverse engineer malware behavior.
- □ Identify and respond to malware attacks using IOCs and threat intelligence feeds.
- □ Anti-malware and best practices protect systems and networks.
- ✓ Investigate unusual network behavior using network traffic analysis techniques.
- ✓ Memory forensics tools can analyze volatile data and detect live system attacks.
- □ Recover and analyze hacked system data with disk forensics tools.
- ✓ Windows, macOS, and Linux forensics.
- □ Use digital forensics to track criminals.
- □ Malware detection and forensic analysis include legal and ethical issues.
- □ Present malware detection and forensic investigation results clearly.
- ✓ Keep up with malware detection and forensic analysis developments and dangers.
- ✓ Penetration testing
- ✓ Exploit creation
- □ OTHER: Please specify ____

□ OTHER: Please specify ____

TRAINING SESSION/tool - demonstration / (supplementary material)

The CyberHOT Summer school sessions through the HtB platform aims for the participants:

To be able to implement enumeration on web services.

To be able to research existing vulnerabilities of known components.

To be able to exploit existing vulnerabilities utilising metasploit and other public exploits.

To be able to implement privilege elevation on compromised targets.

TRAINING SESSION/tool - mock exercises and group work / (supplementary material)

Enumeration, ROP, Cracking keepass databases, Basic web fuzzing techniques, Locating modified files, CVEs searching, Debugging, SQL injection

TRAINING SESSION/tool – results

We exploit and take priviledges into a variety of HtB VMs

TRAINING SESSION/tool – demographics

Info about:
Total number of persons: 17
Nationalities: 5
Level of education [undergraduate student, BSc, postgraduate student, MSc, PhD student, PhD
Group ages [18-29, 30-39, 40-49,]
Gender groups [80% Male, 20% Female]

CyberSecPro Training Program Analysis Training Session

Tool Name: Seaport Security Date: 13/9/-3/10/23 Duration:_25hrs___

Tool Offered by: AIT/UPRC

Provider's (Trainer) Report: Nineta Polemi

TRAINING SESSION/tool - **Introduction**

Overview on International Ship and Port Facility Security (ISPS) Code, International Safety Management (ISM) Code, Ships and Marine Technology (ISO 20858) standard, IMO Guidelines on maritime cyber risk management, IMO Guidelines and Djibouti Code of Conduct (DCoC) against piracy and armed robbery; presentation of physical and cyber threats in maritime port infrastructures; discussion of novel threat trends for seaport operators; examine potential mitigation strategies for those threats; characterizing and assessing interdependencies within maritime port infrastructures; security aspects integrating the physical and cyber domain; identifying cascading effects in port infrastructures; concepts towards an Hybrid Situational Awareness; identifying and assessing interdependencies with supplier/customer organizations; security aspects in maritime supply chains; approaches towards a supra organizational cybersecurity infrastructure in the supply chain

TRAINING SESSION/tool – **learning outcomes**

Mark all that apply for the tool:
Perform malware detection and analysis using malware detection tools.
OTHER: Please specify __risk assesment tools (MITIGATE)

TRAINING SESSION/tool - **demonstration** / (supplementary material)

Hands on Exercises: Illustrative but artificial port infrastructure with realistic physical assets and cyber infrastructure to serve as a "demo site" for exercises throughout the training;
Paper and-pen exercises on different topics related to physical security (facility security,perimeter protection, etc.); cyber assets of the artificial port in the cyber range, specific cybersecurity training scenarios

TRAINING SESSION/tool – **results**

Brief summary of the major outcomes of the training session. Focus on the methodology, the steps and the highlights.
Detect vulnerabilities on proprietary and 3rd party code, inspect associated Security Advisories, Risk Mitigation plan

TRAINING SESSION/tool – **demographics**

Info about: 4 women , 13 men
Total number of persons: 17
Nationalities: Omani, Greek
Level of education: , Professors for the Advance Cybersecurity Center, Administrators of the Maritime Authority of Oman
Group ages : 28-48

Annex G: Audience (Trainees) Report Template

We really hope that the knowledge and experience gained will be beneficial to you.

YOUR OPINION MATTERS TO US ...	**Poor**	**Fair**	**Good**	**Outstanding**
THE TRAINING SESSION CONTENT				
THE SUPPORT MATERIALS – MANUAL AND RESOURCES SUPPLIED				
THE TRAINER/ASSESSOR'S KNOWLEDGE AND EXPERTISE				
THE TRAINER/ASSESSOR'S DEMONSTRATION OF THE PURPOSE AND USE OF THE TOOL				
THE USE OF THE TOOL IN MOCK EXERCISES/ GROUP EXERCISES				
THE GUIDANCE AND SUPPORT OFFERED BY THE TRAINER/ASSESSOR DURING EXERCISE				
FEEDBACK ON TOOL USE AND/OR RESULTS				

FINAL ASSESSMENT OF THE TOOL				
YOUR OVERALL RATING FOR THIS COURSE (DID IT MEET THE LEARNING OUTCOMES PROVIDED)				

PLEASE TELL US WHICH PART OF THE TRAINING SESSION IS MOST RELEVANT:

PLEASE TELL US WHICH PART OF THE TRAINING SESSION IS LEAST RELEVANT:

PLEASE TELL US HOW WE COULD IMPROVE THIS TRAINING SESSION/TOOL:

	YES	**NO**
Did this training tool meet your expectations?		

DO YOU HAVE ANY OTHER COMMENTS REGARDING ANY ASPECT OF YOUR EXPERIENCE WITH THE TRAINING SESSION?