European Security and Defence College
Doc: ESDC/2022/ 287
Date: 15/12/2022
Origin: ESDC Secretariat

Curriculum

To be reviewed by	Activity number	Cyber Range: pentester tools	ECTS
Feb. 2025	213		3

Target audience	Aim
The course is intended for technical personnel (mid-ranking officials, engineers and technicians) employed in the field of cybersecurity from MS or EU institutions, bodies and agencies. Attendees should need to understand cybersecurity threats from a technical perspective. Due to the technical nature of this course it is recommended that attendees be familiar with the Linux operating system, including use of terminal tools and basic network configuration aspects.	The overall goal of this course is to enhance participants' knowledge and practical skills as regards identifying potential vulnerabilities and understanding how penetration testing contributes to improving cybersecurity. It presents basic aspects of network reconnaissance, host enumeration and vulnerability identification. Students should also learn about various applicable tools and techniques and how to run and conduct various penetration tests. Ultimately, they will perform penetration activities through executing scenarios on the Cyber Range (CR) platform, which is a complex virtual environment that allows part of a cyber sphere to be modelled and simulated. The course contributes to enhancing the skills of digital professionals and to building cyber-resilience and strategic autonomy – a pillar of CSDP.
Open to: ▪ EU Member States and EU institutions	

CORRELATION WITH CTG / MTG TRAs	EQUIVALENCES
CTG / MTG TRA on Cyber	• *Specialised tactical-technical levels* • *Linked with the strategic objectives of Pillar 2 of the EU's Cybersecurity Strategy for the Digital Decade [16.12.2020 JOIN (2020)]*

Learning outcomes	
Knowledge	LO01 – Describe the concept of penetration testing. LO02 – Identify the nature of the various cyber threats affecting an organisation. LO03 – List tools and techniques applicable for various types of penetration testing. LO04 – Identify potential threats to and weaknesses of IT infrastructure. LO05 – List benefits of conducting penetration testing. LO06 – Name Understand dependencies between network
Skills	LO07 – Perform network reconnaissance, including network discovery and host enumeration. LO08 – Intercept network traffic and perform analysis. LO09 – Choose and operate proper pentester tools applicable to different technologies. LO10 – Conduct various penetration tests against IT solutions. LO11 – Perform web reconnaissance and web code reading – gathering information.
Responsibility and Autonomy	LO12 – Reconstruct and evaluate a cyber attack LO13 – Assess the potential impact of identified weaknesses on an organisation. LO14 – Recommend adequate countermeasures in response to identified weaknesses and vulnerabilities.

Evaluation and verification of learning outcomes

The course is evaluated in accordance with the Kirkpatrick model, with level 1 evaluation (based on participants' satisfaction with the course).

In order to complete the course, participants have to accomplish all learning objectives, which are evaluated based on their active contribution to the residential module, including syndicate sessions and practical activities, as well as on the completion of the eLearning phases: course participants must finalise the autonomous knowledge units (AKUs) and pass the tests (mandatory), scoring at least 80% in the incorporated out-test/quiz. There is active observation by the course director/lead instructor and a feedback questionnaire is filled in by participants at the end of the course.

However, no formal verification of learning outcomes is planned; the proposed ECTS is based on participants' workload only.

Course structure

The residential module is held over three days.

Main topic	Suggested working hours (required for individual learning)	Suggested content
1. Cybersecurity within the EU	1(4)	1.1 Current EU regulations on cybersecurity, including the Cyber Defence Policy Framework (CDPF)
2. Various cyber threats that can potentially affect an organisation	2(3)	2.1 Mapping of selected techniques onto the MITRE ATT&CK matrix and discussion of mitigants. 2.2 Problems associated with software supply chain risk 2.3 Various threats: RCE, Fuzzing, XSS, CSRF, SQL Injection 2.4 Linux distributions
3. Cyber reconnaissance and intelligence	1(1)	3.1 Information gathering from trusted sources of knowledge on IT vulnerabilities and security gaps 3.1.1 CVE 3.1.2 Exploits 3.2 Dedicated tools for vulnerability discovery and identification
4. Network discovery and host enumeration	6(0)	4.1 Pentester tools in network discovery and host enumeration 4.1.1 Netdiscover 4.1.2 Netcat 4.1.3 Fping 4.1.4 Nmap 4.1.5 DNSMap 4.1.6 GoBuster 4.1.7 Wireshark 4.1.8 Spiderfoot 4.1.9 Recon-NG 4.1.10 Parsero 4.1.11 SIEM 4.2 Hands-on classes in Cyber Range environment – complex scenario for network reconnaissance
5. Vulnerability enumeration and exploitation	2(0)	5.1 Cyber reconnaissance and intelligence – dedicated tools for vulnerability discovery and identification 5.2 Dedicated tools for examining hosts' vulnerabilities 5.2.1 Searchsploit 5.2.2 Metasploit

		5.3 Hands-on classes in Cyber Range environment – complex scenario for vulnerability finding
6. Cyber attacks – dictionary and brute force	1(0)	6.1 Security information and event management 6.2 Pentester tools in dictionary and brute force attacks 6.2.1 John the ripper 6.2.2 Hydra 6.3 Hands-on classes in Cyber Range environment – complex scenario for penetration and exploitation
7. Pivoting	1(0)	7.1 Proxychains
TOTAL	**14(8)**	

Materials required: • AKU 111 - Linux fundamentals • AKU 113 – Cyber Range: pentester tools Recommended: • Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union • Council Conclusions on Strengthening Europe's Cyber Resilience System and Fostering a Competitive and Innovative Cybersecurity Industry (November 2016) • The EU Cybersecurity Act (June 2019) • The EU's Cybersecurity Strategy for the Digital Decade (December 2020)	<u>Methodology</u> The course is based on the following methodology: lectures, panels, workshops, exercises <u>Additional information</u> Pre-course questionnaire on learning expectations and possible briefing topic from the specific area of expertise may be used. All course participants have to prepare for the residential module by going through the relevant eLearning preparatory phase, which is mandatory. The materials proposed for supplementary (eLearning) study will reflect current developments in the field of cybersecurity/cyber-defence in general and EU policies in particular. The Chatham House rule is applied during the residential phase of the course: "participants are free to use the information received, but neither the identity nor the affiliation of the speaker(s), nor that of any other participant, may be revealed".