European Security and Defence College

European Security and Defence College
Doc: ESDC/2025/029
Date: 20 February 2025
Origin: ESDC Secretariat

Curriculum

To be reviewed by **February 2027**	Activity number **213**	**Cyber Range: pentester tools**	ECTS **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)]* • *Supports the European Cybersecurity Skills Framework (ECSF) of ENISA Profile role 12. 'Penetration Tester*

Learning outcomes	
Knowledge	LO01 – Describe the concept of penetration testing (penetration testing procedures, offensive and defensive security procedures, penetration testing tools). LO02 – Identify the nature of the different cyber threats affecting an organization (computer systems vulnerabilities, operating systems security, computer networks security). LO03 – List tools and techniques applicable for different penetration testing (penetration testing tools, penetration testing standards, methodologies and frameworks, cybersecurity attack procedures). LO04 – Identify potential threats and weaknesses of IT infrastructure (operating systems security, computer networks security, computer systems vulnerabilities). LO5 – List benefits resulting from conducting penetration testing (cybersecurity recommendations and best practices). LO6 – Name Understand dependencies between network (computer networks security).
Skills	LO7 – Perform network reconnaissance including network discovery and host enumeration (identify and exploit vulnerabilities, use penetration testing tools effectively).

	LO8 – Intercept network traffic and perform its analysis (identify and exploit vulnerabilities, conduct technical analysis and reporting). LO9 – Choose and operate proper pentester tools applicable for different technologies (use penetration testing tools effectively, think creatively outside the box, conduct ethical hacking, develop codes, scripts and programmes). LO10 – Conduct various penetration test against respective IT solutions (identify and solve cybersecurity-related issues , conduct ethical hacking, perform social engineering, communicate, present and report to relevant stakeholders, think creatively and outside the box). LO11 – Perform web reconnaissance and web code reading – gathering information (review codes assess its security, identify and exploit vulnerabilities, decompose and analyse systems to identify weaknesses and ineffective controls, perform social engineering).
Responsibility and Autonomy	LO12 – Reconstruct and evaluate a cyber attack (identify attack vectors, uncover and demonstrate exploitation of technical cybersecurity vulnerabilities). LO13 – Assess the potential impact of an identified weaknesses to an organization (identify, analyse and assess technical and organisational cybersecurity vulnerabilities). LO14 – Recommend adequate countermeasures responding identified weaknesses and vulnerabilities (deploy penetration testing tools and test programs, select and develop appropriate penetration testing techniques).

Evaluation and verification of learning outcomes

The course is evaluated according to the Kirkpatrick model, particularly level 1 evaluation (based on participants' satisfaction with the course) and level 3 evaluation (assessment of participants' long-term change in behaviour after the end of the course). Evaluation feedback is given in the level 1 evaluation of the residential modules.

In order to complete the course, participants have to fulfil all the learning objectives, and are evaluated on the basis of their active contribution to the residential modules, including their teamwork sessions and practical activities, and on their completion of the eLearning phases. Course participants must complete the autonomous knowledge units (AKUs) and pass the tests (mandatory), scoring at least 80% in the incorporated test/quiz. However, no formal verification of the learning outcomes is provided for; the proposed ECTS is based solely on participants' coursework.

The Executive Academic Board takes these factors into account when considering whether to award certificates to participants. Module leaders provide an evaluation report for each residential module. The Course Director is responsible for overall coordination, with the support of the ESDC Secretariat, and drafts the final evaluation report, which is presented to the Executive Academic Board.

Course structure

The residential course is held over 3 days.

Main topic	Suggested Residential Working Hours + (Hours required for individual learning, E-Learning etc)	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 (ex. Kali, Parrot)
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	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 (ex. Splunk, ELK stack, IBM QRadar) 4.2 Hands-on classes in Cyber Range environment – complex scenario for network reconnaissance
5. Vulnerability enumeration and exploitation	2	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(ex.Nessus,OpenVAS,BurpSuite)
6. Cyber attacks – dictionary and brute force	1	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	7.1 Proxychains
TOTAL	**14 + (8)**	

Materials required:

- AKU 112 - Linux fundamentals
- AKU 113 – Cyber Range: pentester tools
- AKU 115 - Pentester - First steps

Recommended:

- AKU 1 History and context of the CSDP
- 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)

Methodology

The course is based on the following methodology: lectures, panels, workshops, exercises and/or case studies, Q&A, laboratories

Additional information

Pre-course questionnaire on learning expectations and possible briefing topic form 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. Course participants must be willing to contribute with their specific expertise and experience throughout the course.

The Chatham House Rule is applied during all residential modules 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".

• The EU Cyber Diplomacy Toolbox (June 2017) • The EU Cybersecurity Act (June 2019) • COUNCIL DECISION (CFSP) 2020/1127 of 30 July 2020 amending Decision (CFSP) 2019/797 concerning restrictive measures against cyber-attacks threatening the Union or its Member States • The EU's Cybersecurity Strategy for the Digital Decade (December 2020) • EU Policy on Cyber Defence, JOIN(22) 49 final (10.11.2022) • Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 concerning measures for a high common level of cybersecurity across the Union (NIS 2) • Council Conclusion on EU Policy on Cyber Defence (22.05.2023)	