European Security and Defence College
Doc: ESDC/2023/102
Date: 20/04/2023
Origin: ESDC Secretariat

Curriculum

To be reviewed by	Activity number	Cyber Range: Cybersecurity in Practice	ECTS
Feb. 2025	**215**		**3**

Target audience	Aim
The course is intended for technical personnel (mid-ranking officials, engineers and technicians) employed in the field of cybersecurity from Member States 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 aspects of network configuration.	The overall goal of this course is to improve participants' knowledge and practical skills in increasing the security of IT infrastructure they are responsible for. By executing prepared scenarios that allow testing of virtual machines and networks in Reconnaissance, Exploitation, Wi-Fi - Hacking, Web Pentesting, students discover how to identify potential vulnerabilities and weaknesses that might result in direct access to target resources. In doing so, they learn about the available cybersecurity tools and how they can be used in different cases. The course is run on the Cyber Range, a training platform that delivers unique opportunities for reflecting IT infrastructure and enacting complex scenarios, including conducting cyber-attacks in a dedicated virtual environment. It gives students an idea how such an environment can be used to improve the security of IT infrastructure. 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 (penetration testing procedures, offensive and defensive security procedures) LO02 – List tools and techniques applicable for different penetration testing (penetration testing tools) LO03 – Understanding wireless networking standards (computer network security) LO04 – Knowledge of wireless cards associated with monitor mode (cybersecurity recommendations and best practices, cybersecurity attack procedures) LO05 – Knowledge of issues related to XSS, CRSF, SQL Injection and security vulnerabilities (cybersecurity attack procedures, computer system vulnerabilities)
Skills	LO06 – Perform network reconnaissance including network discovery and host enumeration (identify and exploit vulnerabilities, use penetration testing tools effectively) LO07 – Intercept and analyse network traffic (identify and exploit vulnerabilities, conduct technical analysis and reporting) LO08 – Choose and operate proper pentester tools applicable for Wi-Fi hacking/cracking (use penetration testing tools effectively, think creatively outside the box) LO09 – Perform web reconnaissance and web code reading – gathering information (review coding, assess its security, identify and exploit vulnerabilities)

Responsibility and Autonomy	LO10 – Test and recon a local network in a basic way (select and develop appropriate penetration testing techniques) LO11 – Assess the potential impact of an identified weakness on an organisation (identify attack vectors, uncover and demonstrate exploitation of technical cybersecurity vulnerabilities) LO12 – Selecting and preparing a system and tools for penetration testing (select and develop appropriate penetration testing techniques, deploy penetration testing tools and test programs)

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 on the basis of their active contribution to the residential module, including syndicate sessions and practical activities, as well as on 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 only on participants' work.

Course structure

The residential module is held over three days.

Main topic	Suggested working hours (required for individual learning)	Suggested content
1. Tools for recon & enumeration	2(2)	1.1 Hands-on classes in Cyber Range environment: introduction to penetration testing tools. Practical & initial penetration test 1.1.1 Enumeration
2. Phishing and exploitation	2(3)	2.1 Hands-on classes in Cyber Range environment: exercise – exploitation & post-exploitation environment 2.1.1 Kali Linux 2.1.2 Metasploit 2.1.3 MSFVenom 2.1.4 SEToolkit
3. Password cracking	1(0)	3.1 Hands-on classes in Cyber Range environment: exercise – phishing & password-cracking 3.1.1 SEToolkit 3.1.2 John the Ripper
4. Web technologies and network reconnaissance	2(0)	4.1 Hands-on classes in Cyber Range environment: network architectures in the context of web application security 4.1.1 Network Infrastructure 4.1.2 Web Servers 4.1.3 Reconnaissance 4.1.4 Enumeration
5. Webserver Recon in Cyber Range	2(0)	5.1 Hands-on classes in Cyber Range environment: different types of vulnerabilities in web technologies 5.1.1 Web technologies 5.1.2 Vulnerabilities 5.1.3 Misconfigurations
6. Inside organisation's network	2(0)	6.1 Hands-on classes in Cyber Range environment: lateral movement inside the organisation's network

		6.1.1 Living off the land – operations behind the organisation's firewall
7. Wi-Fi cards & monitor mode	1(2)	7.1 Theory of wi-fi hacking, cracking & wi-fi tools 7.1.1 Parrot OS 7.1.2 Aircrack
8. Wi-Fi scanning networks and cracking passwords	2(0)	8.1 Hands-on classes in Cyber Range environment: exercise – complex scenario for wi-fi hacking – Wi-Fi Recon - practical
9. Analysing PCAP files	2(0)	9.1 Hands-on classes in Cyber Range environment: exercise – complex scenario for wi-fi hacking – network forensics & analysing a PCAP file – practical 9.2 Network analysis
TOTAL	**16(7)**	

Materials required:

- AKU 111 - Linux fundamentals
- AKU 114 – Cyber Range: cybersecurity in practice

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)

Methodology

The course is based on the following methodology: lectures, panels, workshops, exercises

Additional information

A pre-course questionnaire on learning expectations and possibly a briefing topic from the specific area of expertise may be used.

All course participants must 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.'