European Security and Defence College
Doc: ESDC/2025/038
Date: 20 February 2025
Origin: ESDC Secretariat

Curriculum

To be reviewed by **Feb. 2027**	Activity number **266**	**Penetration Tester**	ECTS **1**

Target audience	Aim
The participants should be mid-ranking to senior military or civilian officials dealing with penetration testing, cyber incident monitoring, security operations centre and cybersecurity professionals from EU Institutions, Bodies and Agencies as well as EU Member States.	The aim of the course is to provide a basic and advanced knowledge of Penetration Testing using free and open-source tools, applications and scripts. Furthermore, this course will allow the mid-ranking to senior officials to exchange their views and share best practices on penetration testing topics by improving their knowledge, skills and competencies. By the end of the course, the participants will develop skills to organize and perform penetration testing to systems, applications and services. Through the combination of theoretical lectures and practice labs, the participants will greatly improve their ability to identify existing or potential vulnerabilities to IT systems.
Open to: • EU Member States / EU Institutions Bodies and Agencies	

CORRELATION WITH CTG / MTG TRAs	EQUIVALENCES
CTG / MTG TRA on Cyber and the EU Policy on Cyber Defence	• *Specialised cyber course, at tactical, operational, and strategic level.* • *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 'Penetration Tester' profile*

Learning Outcomes

Knowledge	LO1- Describe penetration testing methodologies LO2- List types and categories of penetration testing LO3- Outline the principles and difference of penetration testing, vulnerability assessment, red and purple teaming LO4- Identify operating systems security LO5- Identify Computer networks security

Skills	LO6- Use of open source tools for penetration testing LO7- Apply the five phases of penetration testing LO8- Perform social engineering LO9- Conduct information gathering/ reconnaissance/ enumeration with open source tools LO10- Perform vulnerability assessment with open source tools LO11- Conduct ethical hacking LO12- Conduct technical analysis and reporting LO13- Decompose and analyse systems to identify weaknesses and ineffective controls LO14- Communicate, present and report to relevant stakeholders
Responsibility and Autonomy	LO15- Conduct technical analysis and reporting LO16- Detect and mitigate vulnerabilities and insecurities in IT systems LO17- Analyse and assess technical and organisational cybersecurity vulnerabilities LO18- Identify attack vectors, uncover and demonstrate exploitation of technical cybersecurity vulnerabilities LO19- Test systems and operations compliance with regulatory standards LO20- Select and develop appropriate penetration testing techniques LO21- Organise test plans and procedures for penetration testing LO22- Establish procedures for penetration testing result analysis and reporting LO23- Document and report penetration testing results to stakeholders LO24- Deploy penetration testing tools and test programs

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 5 days.

Main Topic	**Suggested Residential Working Hours + (Hours required for individual learning E-Learning etc)**	**Suggested Contents**

1. Introduction to penetration testing	18 + (10)	• Overview of PTES (Penetration Testing Execution Standard) • OWASP Testing Guide for Application Security • NIST SP 800-115 (Technical Guide to Information Security Testing and Assessment) • Assessment frameworks: OSSTMM (Open Source Security Testing Methodology Manual) and ISSAF (Information Systems Security Assessment Framework) • Types of penetration tests (black box, white box, gray box)
2. Information gathering	9 + (4)	• Reconnaissance (Maltego, theHarvester, and Recon-ng) • Enumeration (NMAP, SNMPcheck, SMBEnum, SuperScan) • Social engineering and the use of AI
3. Vulnerability assessment	7 + (4)	• OWASP top ten • Nessus • OpenVAS • Nikto
4. Ethical hacking	31 + (8)	• Overview of Windows Defender, SELinux, and AppArmor • Concepts of secure boot and firmware security • Importance of agile and DevSecOps methodologies in penetration testing • OS Kali Linux • Metasploit, Burp Suite • Gaining the foothold - Initial Access • Executing the payload • Evading antivirus • Privilege Escalation • Movement Pivoting and Persistence • Capture the Flag (CTF) challenges
5. Communication	2 + (1)	• Document, report and present penetration testing results
TOTAL	**67 + (27)**	

Material

Required:

- AKU 104: Module 1 – Understand the Organisation
- AKU 104: Module 2 – Learn about Information Security
- AKU 104: Module 8 – Review Organizational Controls
- AKU 104: Module 9 – Review Technical Controls
- Legal frameworks and compliance (GDPR, HIPAA
- Windows architecture
- Common Windows commands and PowerShell
- Linux architecture
- Common Linux commands and shell scripting

Recommended:

Methodology

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

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".

• AKU 1 – History and Context of the CSDP • 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**) • EU Policy on Cyber Defence, JOIN(22) 49 final, 10.11.2022 • The EU's Cybersecurity Strategy for the Digital Decade (December 2020) • The EU Cybersecurity Act (June 2019) • The EU Cyber Diplomacy Toolbox (June 2017) • Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) • Council conclusions on Strengthening Europe's Cyber Resilience System and Fostering a Competitive and Innovative Cybersecurity Industry (November 2016)	