European Security and Defence College
Doc: ESDC/2023/057
Date: 16 February 2023
Origin: ESDC Secretariat

Curriculum

To be reviewed by **Feb. 2025**	Activity number **266**	**Penetration Tester**	ECTS **1**

Target audience

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.

Open to:

- EU Member States / EU Institutions Bodies and Agencies

Aim

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.

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)]*

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 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: it makes use of *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 feed-back* is given in the level 1 evaluation on the residential modules.

In order to complete the course, the participants have to accomplish all learning objectives, which are evaluated based on their active contribution to the residential modules, including their syndicate sessions and practical activities as well as on their 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. **However, no formal verification of the learning outcomes is foreseen; proposed ECTS is based on participants' workload only**.

The Executive Academic Board takes these factors into account when considering the award of *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 module is held over 5 days.

Main Topic	Suggested Working Hours (required for individual learning)	Suggested Contents
1. Introduction to penetration testing	6(2)	• Penetration testing phases • Engagement • OS Kali Linux

2. Information gathering	8(2)	• Reconnaissance • Enumeration • System and network scanning
3. Vulnerability assessment	8(2)	• Frameworks – Guides • Vulnerability Assessment
4. Ethical hacking	14(8)	• Gaining the foothold - Initial Access • Executing the payload • Evading antivirus • Privilege Escalation • Movement Pivoting and Persistence
5. Communication	4(1)	• Document, report and present penetration testing results
TOTAL	**40(15)**	

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

Recommended:

- *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)*

Methodology

The course is based on the following methodology: Presentations, Panels talks, Q&A and/or workshops

Additional information

The Chatham House Rule is applied during all residential modules of the HLC: "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 mandatory EU security clearance to "Confidential" level should be valid for the entire duration of the HLC and participants must prove that they have an EU clearance certificate before the start of the first residential module (September).