



European Security and Defence College (ESDC)
"Cyber Range – Pentester Tools"

(25-26/213/1)

DRAFT PROGRAMME

30 September – 2 October 2025

Residential form

Cyber Security Training Centre of Excellence (ECSC)
Warsaw, Poland

Course Venue:

EKSPERCKIE CENTRUM SZKOLENIA CYBERBEZPIECZEŃSTWA (ECSC)
ul. gen. Sylwestra Kaliskiego 2
00-908 Warszawa 46

Director of ECSC

Col. Mariusz Krawczyk

Course Director

Col. Michał Majewski

ESDC Cyber ETEE Training Manager at ESDC Secretariat

Ms Anna Malec

PoC at ECSC

Lt. Col. Przemysław Pleszkun

Cyber Range Instructor

Lt. Marcin Urbański



DAY 1 (CEST)	Tuesday, 30 September 2025
08:40 – 08:50	<i>Registration</i> <i>Welcome coffee</i>
08:50 – 10:10	Welcome address and course opening: <ul style="list-style-type: none">• Cyber Security Training Centre of Excellence (ECSC), Warsaw• European Security and Defence College (ESDC), Brussels• Group photo• Informal Tour-de-Table - introduction of instructors and participants
10:10 – 10:55	SESSION 1 – Host discovery – identifying live systems in the network using scanning tools and techniques. <i>Keywords: ARP scan, ICMP sweep, netcat</i>
10:55 – 11:00	<i>Coffee break</i>
11:00 – 11:45	SESSION 2 – Network reconnaissance – mapping network structure and services for further exploitation. <i>Keywords: OS detection, Service enumeration, NSE</i>
11:45 – 14:00	SESSION 3 – Spoofing attack and packet interception – simulating man-in-the-middle scenarios and capturing network traffic <i>Keywords: ARP spoofing, Packet sniffing, MITM</i>
14:00 – 14:15	Wrap-up and closing remarks
14:30 – 15:30	<i>Lunch break</i>
15:30 – 18:30	<i>Transportation to the hotel & guided tour (Warsaw & history of Poland)</i>
18:30 – 21.00	<i>Icebreaker dinner</i>



DAY 2 (CEST)	Wednesday, 1 October 2025
09:00 – 09:15	<i>Welcome coffee</i>
09:15 – 10:45	SESSION 4 – Exploiting vulnerabilities – using public exploits and frameworks for system compromise. <i>Keywords: Exploits, CVE, Metasploit, Payloads</i>
10:45 – 11:00	<i>Coffee break</i>
11:00 – 12:45	SESSION 5 – Password attacks and brute-force techniques – cracking credentials and targeting exposed authentication services. <i>Keywords: John the Ripper, Hydra, brute-force</i>
12:45 – 13:00	<i>Coffee break</i>
13:00 – 14: 50	SESSION 6 – Privilege escalation and persistence – gaining higher privileges and maintaining access on compromised systems. <i>Keywords: Peas-ng, backdoors</i>
14:50 – 15:00	Wrap-up and closing remarks
15:00 – 16:00	<i>Lunch break</i>
16:00	<i>Transportation to the hotel</i>



DAY 3 (CEST)	Thursday, 2 October 2025
08:45 – 09:15	<i>Welcome coffee</i>
09:15 – 10:30	SESSION 7 – Phishing and malicious payloads – crafting deceptive emails and generating malware for initial access <i>Keywords: email spoofing, social engineering, MSFvenom</i>
10:30 – 10:45	<i>Coffee break</i>
10:45 – 12:00	SESSION 8 – Web application enumeration and exploitation – identifying entry points and compromising vulnerable web servers <i>Keywords: Ffuf, OWASP, payloads</i>
12:00 – 13:10	SESSION 9 – Active Directory enumeration and exploitation – identifying AD structure and leveraging weaknesses for domain compromise <i>Keywords: AD, CrackMapExec</i>
13:10 – 13:55	SESSION 10 – Privilege escalation and persistence in Active Directory – advancing privileges and maintaining access within the domain <i>Keywords: BloodHound, Kerberoasting, Golden Ticket</i>
13:55 – 14:20	Summary
14:20 – 14:40	Certificate Ceremony
14:40 – 15:00	<i>Closing Remarks - End of the Course</i>
15:00 – 16:00	<i>Lunch break</i>
16:00	<i>Transportation to the hotel/airport</i>



Annex 3

Place of the course: Eksperckie Centrum Szkolenia Cyberbezpieczeństwa (ECSC) internationally known as the Cyber Security Training Centre of Excellence.



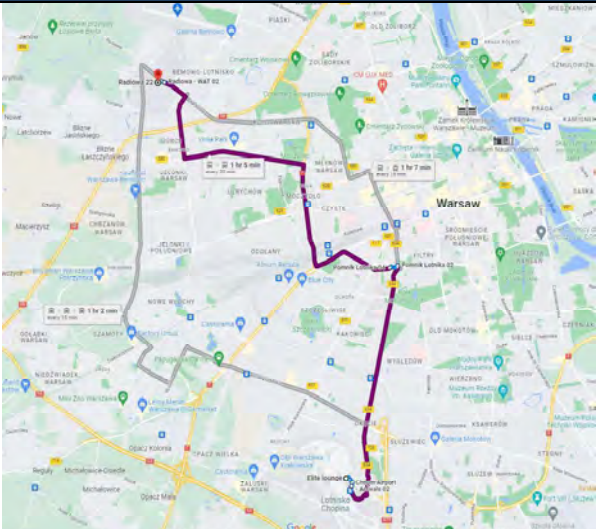


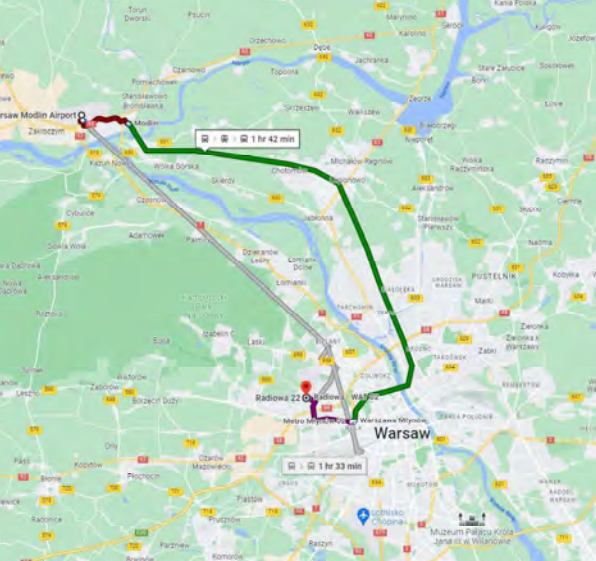
Adress: Kaliskiego 2 (entrance from Radiowa, gate No. 4, building WAT 65)

00-908 Warsaw, Poland

Phone: + 48 22 261 83 79 90 / **Mail:** ecsc@mon.gov.pl / www.ecsc.mil.pl/en/

In case of any changes to the organisation of the course, ECSC will send an appropriate notification to enrolled individuals.

Information on the proposed hotel from which shuttle service will be provided will be communicated at a later date to those who qualify for the course.

Driving direction	Access route
<p>1. From the Warsaw Chopin Airport to the ECSC</p> <div></div> <p>Active link</p>	
<p>2. From the Masovian Warsaw-Modlin Airport to the ECSC</p> <div></div> <p>Active link</p>	



Link to public transport in Warsaw: [how can I get to](#)





Annex 4

Additional personal information required to enter military facility

Please be informed, that due to national security regulations, in order to get an access to Cyber Security Training Centre of Excellence (ECSC) facilities, additional personal information is required. Therefore, all qualified for this course candidates will be kindly requested to provide below information not later than **11th September 2025** (deadline due to procedures connected with issuance of an access permission).

Complete set of information should be sent via email to PoCs at the Cyber Security Training Centre of Excellence listed in Annex 1.

- name, second name (if applicable) and surname
- nationality
- organization/company
- job title
- course name
- date of birth
- ID type (national ID/passport) and number
- military rank (if applicable)
- security clearance (if applicable) - please indicate information domain (national, EU/UE, NATO) and security level

Please bear in mind that any delays or lack of the above information might result with a risk regarding access to the venue of the course.