CYBER SECURITY TRAINING CENTRE OF EXCELLENCE

EUROPEAN SECURITY AND DEFENCE COLLEGE
ESDC CESD
COLLÈGE EUROPÉEN DE SÉCURITÉ ET DE DÉFENSE

18-20 OCTOBER | Pentester Tools – Basic Course

2022

www.cstcoe.mil.pl

EUROPEAN SECURITY AND DEFENCE COLLEGE

And

Cyber Security Training Centre of Excellence, Warsaw, Poland

(Eksperckie Centrum Szkolenia Cyberbezpieczeństwa)

Invitation to the course:

"Pentester Tools-Basic Course"

(Activity number 22-23/213/1)

18 – 20 October 2022

The Cyber Security Training Centre of Excellence (CST CoE) under the auspices of the European Security and Defence College (ESDC) is organising the residential course, specialized at tactical-technical levels, from 18 to 20 October 2022 in Warsaw, Poland.

Newly emerged, rapidly developing and massively striking cyber threats have impacted all the business areas and domains having theirs processes supported by Information and Communication Technologies (ICTs). Vulnerabilities of IT solutions leaves the gates of organizations widely open for cyber criminals who are looking forward to get an access to the IT resources, seize sensitive information, disrupt services or obtain unauthorised rights. Consequently, due to high risk and considerable damages, cyber security and its assurance has been recognized as a pivotal objective and one of the corner stones for modern world stability.

In response to these circumstances, the European Union has been actively working on creating adequate, flexible and coherent cyber security environment, which covers not only political and legal frameworks but also capabilities development including education and training programmes.

Addressing capability development within respective EU bodies and authorities against cyber threats showed the need to spread and improve knowledge regarding vulnerabilities to the information and IT resources. Collective efforts of Cyber Security Training Centre of Excellence (Eksperckie Centrum Szkolenia Cyberbezpieczeństwa - ECSC, Warsaw, Poland) and the European Security and Defence College has resulted with a Pentester Tools-Basic Course that is now offered to the EU community as a part of ESDC's Cyber Education Training Exercise and Evaluation (ETEE) platform.

The overall goal of this course is to deliver and enhance participants' knowledge as well as practical skills on identifying potential vulnerabilities and how penetration testing contributes to improving cyber security. The course will be held in English and will consist of both lectures and practical exercises.

The course will be run on the Cyber Range training platform which delivers unique opportunities for reflecting IT infrastructure and complex scenarios including conducting cyber-attacks in dedicated virtual environment that could be compared with "live fire" experience.

Participants should be technical personnel (mid-ranking officials, engineers and technicians) from the Member States and the EU Institutions Bodies and Agencies dealing with technical aspects of cyber security. The course is scheduled to take place from the **18 to 20 October 2022 in residential form in Warsaw, Poland.**

Paweł DZIUBA
Director of CST CoE

Dirk Dubois
Head of ESDC

Annexes

1. Course administrative instructions
2. Draft programme
3. Venue « Cyber Security Training Centre of Excellence, Warsaw"
4. Additional personal information required to enter military facility

Annex 1

Course administrative instructions

The course is suitable to technical personnel (mid-ranking officials, engineers and technicians) dealing with cyber security. It will be held in English and can accommodate up to 12 participants (civilian and military) staff from EU Member States, relevant EU institutions and agencies. Due to the technical nature of this course it is recommended that attendees were familiar with Linux operating system including usage of terminal tool and basic network configuration aspects.

Applications from the EU Member States and institutions are to be filled out by the national ENLIST nominators via the ESDC secure registration system via the following link https://esdc.europa.eu/enlist/login, **no later than 09th September 2022**.

A list of relevant ENLIST nominators can be retrieved from the ESDC website at https://esdc.europa.eu/nominators/.

The course will consist of two mandatory parts. **Online part** (asynchronous) will be delivered through ESDC's e-learning platform while **live part** (*residential*), containing lectures and exercises in lab environment, is to be held at Cyber Security Training Centre of Excellence facilities in Warsaw.

The e-learning part will be available for those who will be selected as of 19th September 2022**.**

The particular cases covered during the lectures will be further modelled and simulated within Cyber Range environment where respective scenarios will be executed and examined by course participants. The results will be later assessed and discussed within course attendees.

All international travel, transportation, accommodation costs during the course are to be covered by the sending authorities. It is recommended that participants arrive at Warsaw Airport on Monday, October 17, 2022. Participants should arrange their own travel and accommodation. We suggest choosing the Polonia Palace hotel, from which the training organizer provides a shuttle transport to the course venue. Reservations should be made by September 20, using the password sent by the course organizer. No-cost cancellation will be possible up to 7 days before arrival. Further information will be sent to participants after registration.

The dress code is business attire for both civilians and military personnel.

The format of the course is residential in Warsaw. However, given the unpredictable nature of the COVID-19 pandemic and possible changes to restrictions imposed on public events and international travel in the upcoming months, the organisation of the course in a face to face format might not be possible. In that case, the course will be canceled. Please do not book flights and accommodation before receiving the confirmatory message.

Supporting services:

- All administrative information, programmes and material will be made available to accepted participants through the ESDC's e-learning platform (ILIAS LMS).

Course points of contact

PoC at the European Security and Defence College:

Mr. **Giuseppe ZUFFANTI**,
Training Manager (Cyber) ESDC
Tel: +32 2 584 42 49, mobile: +32 460 84 42 49
E-mail: giuseppe.zuffanti@eeas.europa.eu

PoC at the Cyber Security Training Centre of Excellence, Warsaw, Poland:

Col AF Michal **MAJEWSKI**	Maj. Jan **KOLOWSKI**	Ms Joanna **ARCHACKA-STACHURA**
Tel: +48 261 837 996	Tel: +48 261 837 945	Tel: +48 571 221 051
E-mail: michal.majewski@ron.mil.pl	E-mail: j.kolowski@ron.mil.pl	E-mail: j.archacka-stachura@ron.mil.pl

Annex 2

European Security and Defence College (ESDC)

"Pentester Tools-Basic Course"

(22-23/213/1)

DRAFT PROGRAMME

18 October – 20 October – Residential form

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

(Eksperckie Centrum Szkolenia Cyberbezpieczeństwa, Warszawa, Polska)

Course Venue:

ul. gen. Sylwestra Kaliskiego 2
00-908 Warszawa 46

Director of CST CoE
Mr. Paweł DZIUBA

Course Director
COL Michał Majewski

DAY 1	Tuesday, 18 October 2022 (CEST)
09:00 – 09:30	*Registration* *Welcome coffee*
09:30 – 09:45	Welcome address and course opening: • Cyber Security Training Centre of Excellence (CSTCoE), Warsaw • European Security and Defence College (ESDC), Brussels
09:45 – 10:30	Introductory session – presenting Cyber Range environment.
10:30 – 10:45	*Coffee break*
11:45 – 12:25	SESSION 1 – Information gathering, trusted sources for knowledge on IT vulnerabilities and security gaps. *Keywords: CVE, Exploits*
12:25 – 13:35	*Lunch break*
13:35 – 15:15	SESSION 2 – Cyber reconnaissance and intelligence – dedicated tools for vulnerabilities discovery and identification *Keywords: Linux, Nmap, Recon, FPing*
15:15 – 15:30	Wrap-up and closing remarks
15:30 – 15:40	*Group photo.*
15:45 – 16:00	*Coffee break*

DAY 2	Wednesday, 19 October 2022 (CEST)
08:45 – 09:15	*Welcome coffee*
09:15 – 10:30	SESSION 3 - Hands-on classes in Cyber Range environment: Pentester tools in network discovery and host enumeration *Scenario 1* *Keywords: Linux, Nmap, Recon, FPing*
10:30 – 10:45	*Coffee break*
10:45 – 12:25	SESSION 4 - Hands-on classes in Cyber Range environment: possible access ways discovery and vulnerability identification *Scenario 1* *Keywords: Linux, Exploit, CVE, Nmap*
12:25 – 13:35	*Lunch break*
13:35 – 15:15	SESSION 5 - Hands-on classes in Cyber Range environment: dedicated tools for examining hosts vulnerabilities *Scenario 1* *Keywords: Linux, Network*
15:15 – 15:20	Wrap-up and closing remarks
15:20 – 15:35	*Coffee break*
19:30 – 21:00	*Icebreaker Dinner*

DAY 3	Thursday, 20 October 2022 (CEST)
08:45 – 09:15	*Welcome coffee*
09:15 – 10:30	SESSION 6 - Hands-on classes in Cyber Range environment: complex scenario for network reconnaissance *Scenario 2* *Keywords: Linux, Nmap, Recon,*
10:30 – 10:45	*Coffee break*
10:45 – 12:25	SESSION 7 - Hands-on classes in Cyber Range environment: complex scenario for vulnerability findings *Scenario 2* *Keywords: Linux, Exploits, CVE, Databases*
12:25 – 13:35	*Lunch break*
13:35 – 14:40	SESSION 8 - Hands-on classes in Cyber Range environment: complex scenario for penetration and exploitation *Scenario 2* *Keywords: Linux, Exploit, Penetration Test*
14:40 – 15:15	SESSION 9 - Security Information and Event Management: network traffic analysis and participants' activities/achievements evaluation collected from scenario 2 *Keywords: Network Traffic, Monitoring, SIEM*
15:15 – 15:20	*Wrap-up*
15:20 – 15:30	*Coffee break*
16:00 – 16:30	Certificate Ceremony • *Cyber Security Training Centre of Excellence (CSTCoE), Warsaw* • *European Security and Defence College (ESDC), Brussels*
16:30 – 16:45	*Closing remarks – End of the course*

Annex 3

Place of the course: Cyber Security Training Centre of Excellence

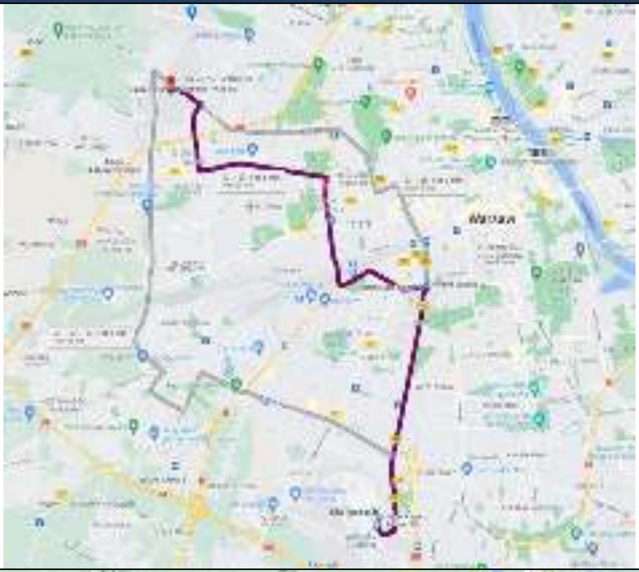
Adress: Kaliskiego 2 (entrance from Radiowa, gate No. 4, building WAT 65)

00-908 Warsaw, Poland

Phone: + 48 22 261 83 79 90 / Mail: cstcoe@mon.gov.pl / https://cstcoe.mil.pl/en

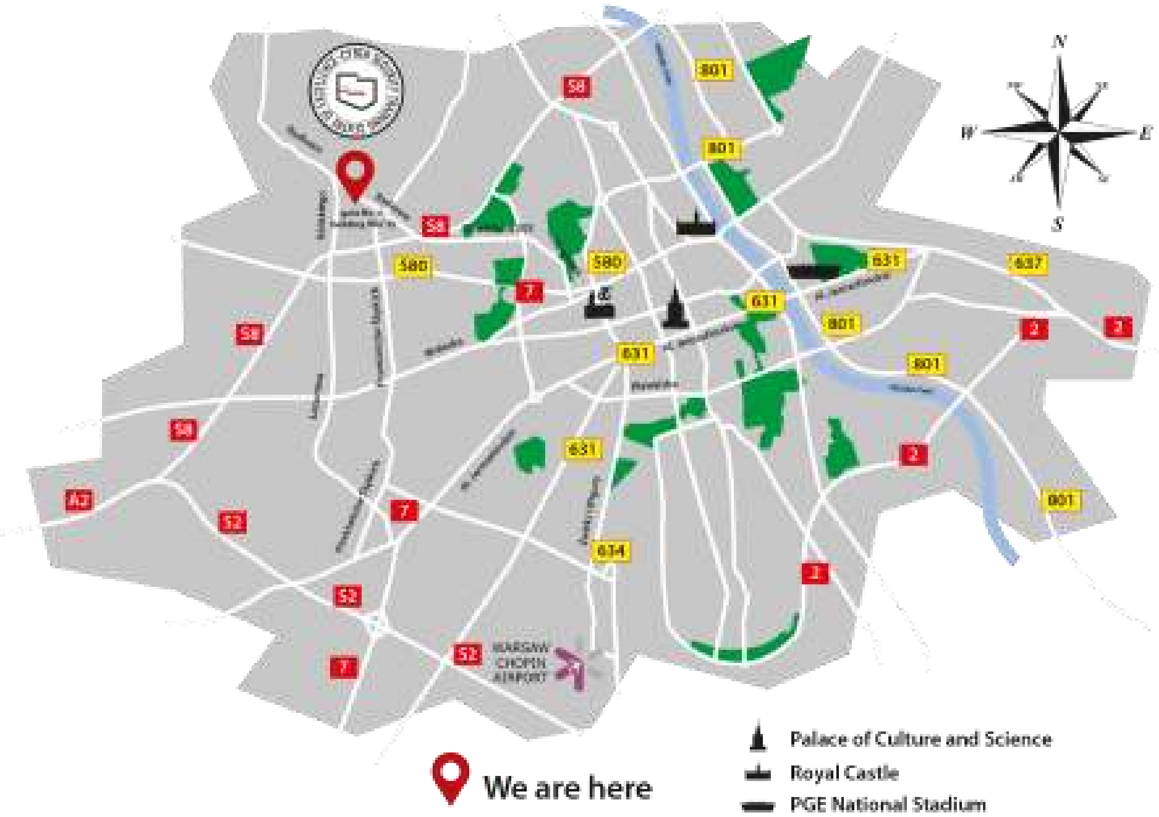
In case of any changes to the organisation of the course, CST CoE will send an appropriate notification to enrolled individuals.

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
1. From the Warsaw Chopin Airport to the CST CoE Active link	
2. From the Masovian Warsaw-Modlin Airport to the CST CoE Active link	

S2 523 175

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 facilities additional personal information is required. Therefore, all qualified for this course candidates will be kindly requested to provide below information not later than 19th September 2022 (deadline due to procedures connected with issuance of an access permission).

Complete set of information should be sent via email to PoCs at 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 lacks in above information might result with a risk regarding access to the venue of a course.