Cybersecurity in practice (CIP)

Course description

The course comprehensively presents the issue of DCO-EDM consisting in the naturalization of the threat using the techniques of breaking the security.
The training environment is prepared on the Cyber Range operated in the Cyber Security Training Centre Of Excellence.

Training subjects:

Exploitation:

- Searching for vulnerabilities in operating systems;
- The sources of exploits and the possibility of their adaptation;
- Attack with a remote and local exploit;
- Reverse shell – how to manage the acquired systems;
- Actions on network infrastructure;

Data Acquisition:

- Exploitation of permissions – or how to become local administrator;
- Analysis of the hijacked systems – interesting files, saved passwords, private data;
- Special cases: web applications, WiFi networks.

- Covering traces and keeping access:
- Logging and activity monitoring systems;
- Clearing logs and blurring traces;
- Backdoor – how to leave entrance open;
- Verification of the performance tasks.

Acquired skills:

Able to:

- Hardening haterogeneous infrastructure based on Linux and Windows systems;
- Use of dedicated tools for infrastructure monitoring;
- Use of tools for fensic analysis of digital data.

Know:

- Concepts of threat analysis in ICT systems and network;
- Stand out the basics infrastructure monitoring methods;
- Critical lactions (system logs) in various systems from the Linux and Windows family;
- Basic Windows configuration.

Minimal requirements:

- Knowledge of general issues related to computer networks and Windows and Linux operating systems (system terminal).

Time: 24h

Data: To be defined

Location: Cyber Security Training Centre of Excellence, Warsaw.