EN2720 Ethical Hacking 7.5 credits

Etisk hackning

This is a translation of the Swedish, legally binding, course syllabus.

If the course is discontinued, students may request to be examined during the following two academic years

Establishment

The official course syllabus is valid from the autumn semester 2024 in accordance with the decision from the director of first and second cycle education: J-2024-0704.Decision date: 2024-03-27

Grading scale

A, B, C, D, E, FX, F

Education cycle

Second cycle

Main field of study

Computer Science and Engineering,Electrical Engineering

Specific prerequisites

Knowledge and skills in basic programming, 6 credits, corresponding to completed course DD1310-DD1319/DD1321/DD1331/DD1337/DD100N/ID1018.

Language of instruction

The language of instruction is specified in the course offering information in the course catalogue.

Intended learning outcomes

After passing the course, the student should, at an introductory level, be able to

- establish resources to support offensive security operations
- perform reconnaissance and discovery to plan operations
- access credentials, such as account names, passwords and access tokens
- achieve initial access to networks and systems
- execute malicious code on remote devices
- establish command and control capabilities to communicate with compromised systems
- elevate privileges on systems to gain higher-level permissions
- persist on networks by maintaining access across interruptions
- move laterally, pivoting through the computing environment
- avoid detection by network defenders
- collect and exfiltrate data from computing environments
- assess the security of computer systems, applications, and services
- carry out legal and ethical security testing.

This will provide students with a practical understanding of the capabilities and possibilities of an attacker, in order to evaluate the cybersecurity of computer networks.

Course contents

The main activity of the course is a project where students independently attack a corporate computer network with the aim of exfiltrating specific information. The network is rigged by the course responsibles in a virtual environment. To carry out the attack, the students are free to use their imagination and tools available on Internet. Tools for network and vulnerability scanning, platforms for exploit development, command and control, passwork creacking, etc. are presented during the course, but students are free to employ methods and tools of their own choice.

Examination

- INL2 - Home assignment, 0.5 credits, grading scale: P, F
- PRO2 - Project assignment, 6.5 credits, grading scale: A, B, C, D, E, FX, F
- TEN2 - Written exam, 0.5 credits, grading scale: P, F

Based on recommendation from KTH's coordinator for disabilities, the examiner will decide how to adapt an examination for students with documented disability.

The examiner may apply another examination format when re-examining individual students.

Transitional regulations

The earlier written assignment INL1 has been replaced by INL2.

The earlier project PROA has been replaced by PRO2 and TEN2.

Ethical approach

- All members of a group are responsible for the group's work.
- In any assessment, every student shall honestly disclose any help received and sources used.
- In an oral assessment, every student shall be able to present and answer questions about the entire assignment and solution.