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 2021 in accordance with Head of School decision: J-2021-0338.Decision date: 15/04/2021

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 programming, 6 higher education credits, equivalent to completed course DD1310/DD1311/DD1312/DD1314/DD1315/DD1316/DD1318/DD1331/DD100N/ID1018.

Language of instruction

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

Intended learning outcomes

Ethical hackers are contracted for practical assessment of computer network security. For an effective defense against cyber attacks, a deep understanding of attackers' available range of action is required. After completed course, the student should therefore be able to

- perform reconnaissance, identifying and selecting targets for attack, e.g. by means of network scanning
- identify vulnerabilities in network equipment and applications
- customize exploits for software vulnerabilities
- deploy and execute exploits on vulnerable systems,
- install and use remote access trojans for remote system control
- identify password files and extract passwords
- exfiltrate data
- implement solutions to strengthen the information security of computer networks
- carry out legal and ethical security testing.

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
- PROA - Project, 7.0 credits, grading scale: A, B, C, D, E, FX, 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.

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.