# FEP3370 Advanced Ethical Hacking 8.0 credits

## Avancerad etisk hackning

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

## Establishment

Course syllabus for FEP3370 valid from Autumn 2017

## Grading scale

G

## Education cycle

Third cycle

## Specific prerequisites

## Language of instruction

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

## Intended learning outcomes

After completed course, the student should 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,
- 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.

Additionally, students should be able to

- develop and test exploits of software vulnerabilities.

## Course contents

The main activity of the course is a project where students attack a corporate computer network with the aim of exfiltrating specific information. The network is rigged by the course responsibles in a virtual environment. Tools for network and vulnerability scanning, platforms for exploit development, command and control, password cracking, etc. are presented during the course, but students are free to employ methods and tools of their own choice.

Additionally, students are tasked with the development and testing of a new vulnerability exploit.

## Disposition

The course is structured around the penetration testing project, where students are tasked with the exfiltration of a number of data files from the exploited network. Additionally, students are expected to develop a new exploit, which subsequently is tested. In addition to these practical projects, seminars are offered on associated topics, including the ethical aspects of hacking.

## Course literature

Rafay Baloch's Ethical Hacking and Penetration Testing Guide, 2014, is recommended, but not required.

## Equipment

Students are expected to employ their own computer, for instance by deploying a penetration testing distribution as a virtual machine, in order to interact with the training computer network.

## Examination

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.

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

## Other requirements for final grade

- Submission of required data files exfiltrated from exploited network
- Submission and approval of developed exploit and test results
- Participation in all seminars
- Submission of weekly progress reports

## 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.