



# 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 Spring 2023

## Grading scale

P, F

## 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

- 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.

## 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 responsables 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.

## Examination

- EXA1 - Examination, 8.0 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.

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.