# Course memo Autumn 2024

EN2720 Ethical Hacking 7.5 credits
version 1

July 12, 2024

## 1 Content and learning outcomes

### 1.1 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.

### 1.2 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.

### 1.3 Lecture schedule

| Date | Lecture | Room | Info |
|---|---|---|---|
| 30/8, 15:00 | L1 | Q1 | Introductory lecture |
| 13/9, 13:00 | GL1 | F1 (Alfvénsalen) | Guest lecture 1 |
| 20/9, 15:00 | GL2 | F1 (Alfvénsalen) | Guest lecture 2 |
| 26/9, 15:00 | GL3 | F1 (Alfvénsalen) | Guest lecture 3 |
| 4/10, 10:00 | GL4 | F1 (Alfvénsalen) | Guest lecture 4 |

## 2 Preparation before course starts

Ethical Hacking is an advanced problem-based course in a topic that relies on skills and knowledge related to programming, computer networking, web technologies, and operating systems. If you are new to working with Linux, we recommend playing through some ethical hacking tutorials and introductory challenges. Otherwise, the potential knowledge gaps could make the course highly demanding.

As a starting point, try the following rooms from TryHackMe:

- Tutorial
- OpenVPN
- Linux fundamentals part 1
- Introductory networking
- Web fundamentals
- Pentesting fundamentals
- Hacker methodology
- Introductory research
- Vulnerabilities 101

- Kenobi
- Vulnversity

For an alternative to the TryHackMe rooms, try playing OverTheWire.

## 2.1 Recommended prerequisites

We strongly recommend that you have some familiarity with communication networks (for example EP1100 Data communication and computer networks) and operating systems (for example ID1206 Operating systems). If you do not, please plan for significantly a higher course load than otherwise expected.

### 2.1.1 Literature

Students are strongly encouraged to search for information in many different sources. Nevertheless, for those that would like to start with a single book, we recommend:

- Learn Ethical Hacking from Scratch: Your stepping stone to penetration testing by Zaid Sabih.

It contains much of the information required for completing the course, but not everything. Conversely, it contains much that is not required for the course. Furthermore, all the relevant information contained in the book is also available on the public Internet. In brief, the book is not required. Therefore, it may be best viewed as a scoping of the course contents, providing ideas on what attack paths to explore. For instance, already the table of contents will give you an indication of what you might encounter in the course:

Chapter 18: Website Pentesting - Information Gathering
Chapter 19: File Upload, Code Execution, and File Inclusion Vulnerabilties
Chapter 20: SQL Injection Vulnerabilities
Chapter 21: Cross-Site Scripting Vulnerabilities
Chapter 22: Discovering Vulnerabilities Automatically Using OWASP ZAP

### 2.2 Software

We recommend setting up and using a virtual machine with a Linux penetration testing distribution installed, such as Kali Linux. The course provides instructions and support for setting up Kali Linux with VirtualBox.

In the event that you are unable set up a penetration testing distribution, then the course also contains instructions for setting up a Kali Linux machine in the cloud.

### 2.3 Support for students with disabilities

Students at KTH with a permanent disability can get support during studies from Funka:

Funka - compensatory support for students with disabilities

## 3 Examination and completion

### 3.1 Grading scale

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

### 3.2 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.

### 3.3 Grading criteria/assessment criteria

To pass the course, the following mandatory parts are required:

- Attendance at all guest lectures, or the execution of a substitution assignment (a summary of the lecture of 800 - 1500 words) for every missing attendance.
- Valid submission of the quiz on Cyber Law, the home assignment.
- Submission of hacking logs each week until completing the project.
- A minimum of 20 % of maximum flag points.
- Submission of each flag before the set deadline.
- A passing grade on the written exam.
- Abiding by the rules.

The final grade in the course will mainly depend on:

- The aggregated value of captured flags.
- Your operational security, your actions did not negatively impact other students.
- A successfully completed (optional) bug bounty bonus assignment is worth 20 points.

If hacking logs, the exam, and other factors are satisfactory, we aim to grade as follows:

A: 90-100 % of the maximum flag points
B: 70-90 % of the maximum flag points
C: 50-70 % of the maximum flag points
D: 30-50 % of the maximum flag points
E: 20-30 % of the maximum flag points

It is not possible to increase the grade of the course after the course has been completed.

## 3.4 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.