Linnæus University

Dnr: LNU-2025/2450

Course syllabus

Faculty of Technology
Department of Computer Science and Media Technology

1DV704 Etisk hackning och penetrationstest, 7,5 högskolepoäng
Ethical Hacking and Penetration Testing, 7.5 credits

Main field of study
Computer Science

Subject
Informatics/Computer and Systems Sciences

Level
First cycle

Progression
G1F

Date of Ratification
Approved 2025-06-25.
The course syllabus is valid from spring semester 2026.

Prerequisites
Introduction to programming 7.5 credits (1DV501), Computer Security 7.5 credits (1DV700), System administration 7.5 credits (1DV721) and Computer Networks – Introduction, 7.5 credits (1DV701) or the equivalent.

Objectives

Upon completion of the course, the student should be able to:
Knowledge and Understanding

- A.1 explain ethical, legal, and regulatory considerations in penetration testing and offensive security,
- A.2 analyze contemporary cybersecurity threats, attacker tactics, and defense mechanisms based on current academic and industry research, and
- A.3 assess the role of AI-driven security tools in ethical hacking, including their

capabilities, limitations, and emerging trends.

Skills and Abilities

- B.1 conduct systematic reconnaissance, vulnerability analysis, and penetration testing using established methodologies,
- B.2 exploit vulnerabilities in networks, web applications, cloud services and operating systems within controlled environments while adhering to ethical guidelines, and
- B.3 produce structured penetration test reports, effectively communicating findings, exploitation steps, and evidence-based remediation strategies.

Judgement and Approach

- C.1 critically assess IT security risks by synthesizing findings from technical assessments and academic research,
- C.2 evaluate the ethical, legal, and societal implications of offensive security practices, including responsible disclosure, and
- C.3 demonstrate professional integrity and a research-driven approach when applying penetration testing techniques.

Content

This course provides an in-depth exploration of ethical hacking and penetration testing, equipping students with theoretical knowledge, practical skills, and a critical understanding of cybersecurity threats and defense mechanisms.

Ethical Hacking Foundations

- Legal, ethical, and regulatory aspects of penetration testing
- Responsible disclosure and compliance frameworks
- The role of AI in cybersecurity and ethical hacking

Penetration Testing Methodologies

- Reconnaissance, information gathering, and vulnerability analysis
- Exploitation techniques for networks, web applications, cloud services and operating systems
- Post-exploitation strategies: privilege escalation, persistence, and lateral movement

Offensive Security Tools and Techniques

- Industry-standard tools: Metasploit, Burp Suite, Nmap, Wireshark
- AI-assisted security tools and automated vulnerability assessment
- Evasion techniques to bypass security defenses

Security Assessment and Reporting

- Risk assessment methodologies and security auditing
- Structured penetration test reporting and remediation strategies
- Communicating findings to technical and non-technical audiences

Research and Emerging Trends in Ethical Hacking

- AI-driven offensive security techniques and adversarial machine learning
- Current academic and industry research in penetration testing
- Ethical considerations and the evolving landscape of cybersecurity threats

Type of Instruction

Teaching consists of lectures, seminars and instructor-led laboratory sessions. The laboratories are either individual or conducted in groups. Attendance at seminars and laboratory sessions is mandatory.

Examination

The course is assessed with the grades A, B, C, D, E or F.

Grade A constitutes the highest grade on the scale, and the remaining grades follow in descending order, whereas grade E is the lowest grade on the scale, which will result in a pass. The grade F means that the student's performance is assessed as fail (i.e. received the grade F).

Student performance assessment is conducted through individual written exams and practical assignments. The practical assignments are examined through submitted reports. To pass the course, a passing grade is required for all components. The final grade is determined by: written exam (40%) and practical assignments (60%).

Resit examination is offered in accordance with Linnaeus University's Local regulations for courses and examination at the first- and second-cycle levels.
In the event that a student with a disability is entitled to special study support, the examiner will decide on adapted or alternative examination arrangements.

Objectives achievement

The examination of the course is divided as follows:
Module 2601 Ethical hacking, practical assignments 4.5 credits with the grading system AF
Module 2602 Ethical hacking, exam 3.0 credits with the grading system AF

The examination elements are linked to the course objectives in the following ways:
Module 2601 links to the course objectives: B.1, B.2, B.3, C.3
Module 2602 links to the course objectives: A.1, A.2, A.3, C.1, C.2, C.3

Course Evaluation

A course evaluation should be conducted during the course or in connection with its conclusion. The results and analysis of the completed course evaluation should be promptly communicated to students who have completed the course. Students participating in the next course instance should be informed of the results of the previous course evaluation and any improvements that have been made, no later than at the start of the course.

Required Reading and Additional Study Material

Required reading

Harper Allen et. al., *Gray Hat Hacking: The Ethical Hacker's Handbook*, latest edition,

McGraw Hill. Pages 500 (700).

FTK, *Distributed material*. Pages 200.