COURSE SYLLABUS
Ethical Hacking and Penetration Testing, 7.5 credits

Etisk hackning och penetrationstestning, 7,5 högskolepoäng

Course Code:	TEHS24	**Education Cycle:**	Second-cycle level
Confirmed by:	Dean Mar 1, 2024	**Disciplinary domain:**	Technology
Revised by:	Director of Education Apr 10, 2024	**Subject group:**	DT1
Valid From:	Aug 1, 2024	**Specialised in:**	A1F
Version:	2	**Main field of study:**	Computer Science

Intended Learning Outcomes (ILO)

After a successful course, the student shall:

Knowledge and understanding
- show familiarity with the concept of red team/blue team in cybersecurity operations
- show familiarity with key standards and frameworks for security audits, vulnerability assessments, and penetration testing and their part in the overall risk management process
- display knowledge of the different steps included in penetration testing methodologies

Skills and abilities
- demonstrate skills in using common tools and applications for cybersecurity assessment and penetration testing
- demonstrate the ability to conduct a penetration test using a predefined methodology
- demonstrate skills in documenting the process and reporting the results of a penetration test

Judgement and approach
- demonstrate an insight into the ethical and legal aspects of conducting a penetration test

Contents

Ethical hacking is a crucial part of assessing the security level of an organisation and is an important part of the overall risk management process. The course focuses on penetration testing as a tool to test the cybersecurity of an organisation’s networks, systems, and processes. The course covers key standards, frameworks, and methodologies for penetration testing. During the course, students will gain hands-on experience with common tools and applications used for penetration testing.

The course includes the following elements:
- The concepts of ethical hacking and offensive security
- The concept of red team/blue team in cybersecurity operations
- Penetration testing as part of the risk management process
- Standards and frameworks for security audits, vulnerability assessments, and penetration

testing
- Penetration testing methodologies
- Tools and applications for penetration testing
- Conducting a penetration test
- Documenting and reporting of a penetration test
- Ethical and legal aspects of penetration testing

Type of instruction

The course consists of lectures, laboratory work, and seminar.

The teaching is conducted in English.

Prerequisites

Passed courses at least 90 credits within the major subject in Computer Science, Informatics, Information Systems, Computer Engineering, or the equivalent, and taken course Cybersecurity Overview, 7,5 credits or the equivalent. Proof of English proficiency is required.

Examination and grades

The course is graded 5,4,3 or Fail.

Registration of examination:

Name of the Test	Value	Grading
Examination[I]	3 credits	5/4/3/U
Laboratory	3 credits	U/G
Seminar	1.5 credits	U/G

[I] Determines the final grade of the course, which is issued only when all course units have been passed.

Course literature

The literature list for the course will be provided eight weeks before the course starts.

• Debar, H. (2021). The Cyber Security Body of Knowledge v1.1.0, 2021—Security Operations & Incident Management. University of Bristol. http://www.cybok.org Links to an external site.

• Stringhini, G. (2021). The Cyber Security Body of Knowledge v1.1.0, 2021—Adversarial Behaviours. University of Bristol. http://www.cybok.org Links to an external site.

• Lee, W. (2019). The Cyber Security Body of Knowledge v1.0, 2019—Malware & Attack Technology. University of Bristol. http://www.cybok.org Links to an external site.

• Research articles according to the teacher's instruction