JÖNKÖPING UNIVERSITY
School of Engineering

COURSE SYLLABUS

Penetration Testing, 7.5 credits

Penetrationstestning, 7.5 högskolepoäng

Course Code:	T2PMBS	Education Cycle:	Second-cycle level
Confirmed:	Sep 01, 2025	Disciplinary domain:	Technology
Valid From:	Aug 31, 2026	Subject group:	Computer Technology
		Specialised in:	A1F Second cycle, has second-cycle course/s as entry requirements
		Main field of study:	Computer Science

Intended Learning Outcomes (ILO)

On completion of the course the student shall:

Knowledge and understanding

- show familiarity with the concept of red team/blue team in cybersecurity operations
- show familiarity with how penetration testing contributes to the overall risk management process
- display knowledge of the different steps included in penetration testing methodologies
- display knowledge about current research directions within penetration testing

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

Content

Penetration testing is an essential 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 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
- Social engineering as part of 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
- State-of-the-art within penetration testing

Type of instruction

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

Language of instruction is in English.

Entry requirements

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 U.

Registration of examination:

Name of the Test	Value	Grading
Seminar [1]	4 credits	5/4/3/U
Laboratory	3.5 credits	G/U

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

Course literature

Please note that changes may be made to the reading list up until eight weeks before the start of the course.

Debar, H. (2021). The Cyber Security Body of Knowledge v1.1.0, 2021—Security Operations & Incident Management. University of Bristol. www.cybok.org.

Stringhini, G. (2021). The Cyber Security Body of Knowledge v1.1.0, 2021—Adversarial Behaviours. University of Bristol. www.cybok.org.

Lee, W. (2019). The Cyber Security Body of Knowledge v1.0, 2019—Malware & Attack Technology. University of Bristol. www.cybok.org.