Blekinge Institute of Technology
Department of Computer Science

Revision: 1
Reg.no: BTH-4.1.14-0911-2022

COURSE SYLLABUS

Penetrationstestning och etisk hackning

PEN testing and Ethical Hacking

7.5 credits (7,5 högskolepoäng)

Course code: DV2630
Main field of study: Computer Science, Software Engineering
Disciplinary domain: Technology
Education level: Second cycle
Specialization: A1N - Second cycle, has only first cycle course/s as entry requirements

Language of instruction: English
Applies from: 2023-01-16
Approved: 2022-09-01

1. Decision

This course is established by Dean 2022-06-08. The course syllabus is approved by Head of Department of Computer Science 2022-09-01 and applies from 2023-01-16.

2. Entry requirements

Admission to the course require at least 120 credits, of which at least 90 credits are in a technical area, and a minimum of 2 years professional experience within an area related to software-intensive product and/or service development (shown by, for example, a work certificate from an employer).

3. Objective and content

3.1 Objective

The course provides in-depth understanding of the penetration testing phases, various attack vectors, and preventative countermeasures. Penetration Testing course encompasses that the student should learn to understand and discover weaknesses and vulnerabilities in information systems, perform the attacks, check the strength of existing security controls, etc.

3.2 Content

- Introduction and processes
- Footprinting and reconnaissance
- Network scanning, tunneling and firewalls evasion
- Different enumeration techniques
- Vulnerability analysis
- Access attacks
- Session spoofing nd hijacking
- Wireless attacks
- Exploitation with Metasploit
- Post exploitation and privilege escalation

4. Learning outcomes

The following learning outcomes are examined in the course:

4.1 Knowledge and understanding

On completion of the course, the student will be able to:

- Know the key issues including plaguing the information security world, ethical hacking, information security laws and standards
- Understand the processes in information assurance as well as neds in penetration testing

4.2 Competence and skills

On completion of the course, the student will be able to:

- Perform footprinting and reconnaissance using latest techniques and tools.
- Perform network and vulnerability scanning

- Execute enumeration
- Break the security controls and perform access attacks
- Execute post-exploitation scripts
- Elevate the privileges and hijack the existing user sessions
- Execute wireless network attacks

4.3 Judgement and approach

On completion of the course, the student will be able to:

- Conduct penetration testing
- Analyse the penetration testing results

5. Learning activities

The teaching is organised around online lectures, recorded videos, online lab assignments, together with presentations and literature. Throughout the course, communication, feedback, and discussions with teachers and fellow participants will take place through the course's online learning platform and online-messengers.

6. Assessment and grading

Modes of examinations of the course

Code	Module	Credits	Grade
2305	Laboratory Session 1	1.5 credits	GU
2315	Laboratory Session 2	1.5 credits	GU
2325	Laboratory Session 3	1.5 credits	GU
2335	Laboratory Session 4	1.5 credits	GU
2345	Written Assignment	1.5 credits	GU

The course will be graded G Pass, UX Fail, supplementation required, U Fail.

The information before a course occasion states the assessment criteria and make explicit in which modes of examination that the learning outcomes are assessed.

An examiner can, after consulting the Disability Advisor at BTH, decide on a customized examination form for a student with a long-term disability to be provided with an examination equivalent to one given to a student who is not disabled.

7. Course evaluation

The course evaluation should be carried out in line with BTH:s course evaluation template and process.

8. Restrictions regarding degree

The course can form part of a degree but not together with another course the content of which completely or partly corresponds with the contents of this course.

9. Course literature and other materials of instruction

THE HACKER PLAYBOOK 3. Practical Guide to Penetration Testing Red Team Edition. Peter Kim. 2018. ISBN-13: 978-1980901754