Blekinge Institute of Technology
Department of Computer Science

Revision: 1
Reg.no: BTH-4.1.14-0935-2023

COURSE SYLLABUS

Säkerhetshärdning för operativsystem

Operating System Security Hardening

3.5 credits (3,5 högskolepoäng)

Course code: DV2634
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: 2024-01-16
Approved: 2023-09-01

1. Decision

This course is established by Dean 2022-12-21. The course syllabus is approved by Head of Department of Computer Science 2023-09-01 and applies from 2024-01-16.

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 objective of the course is to give the participants the required knowledge, skills, and techniques to secure and defend operating systems against potential threats and vulnerabilities. The course focuses on various approaches to harden operating systems, starting with identifying configuration weaknesses and implementing measures to mitigate them.

3.2 Content

The course covers a comprehensive range of topics aimed at securing operating systems against various threats. It begins with an exploration of different hardening approaches, identification of default configuration weaknesses, and the implementation of the Zero-Trust model for network security. Participants learn to manage trusted sources for Linux installations and third-party software, as well as the significance of drivers and libraries signing. The course addresses OS patching and updating processes for Windows and Linux, cryptography for encrypting storage in both environments, and certificates management for secure communication. Participants also gain knowledge and skills in access and authentication methods, including the Least Privilege Principle, Role-Based Access Control (RBAC), and privilege access management tools.

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:
• understand different hardening approaches used to secure operating systems.

4.2 Competence and skills

On completion of the course, the student will be able to:
• implement various hardening techniques to secure operating systems effectively.
• identify and mitigate default configuration weaknesses in OS environments.

4.3 Judgement and approach

On completion of the course, the student will be able to:
• assess and analyze OS security vulnerabilities to apply appropriate hardening measures.

5. Learning activities

The teaching takes place in the form of online lectures, recorded video material, as well as presentations and basic literature (books and articles). Practical skills will be delivered through practical assignments. During the course there will be communication, feedback and discussions with teachers and other participants takes place via e-mail, the LMS platform and via online meetings.

6. Assessment and grading

Modes of examinations of the course

Code	Module	Credits	Grade
2405	Written assignment 1	1 credits	GU
2415	Written assignment 2	1 credits	GU
2425	Written assignment 3	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

• Mastering Windows Security and Hardening: Secure and protect your Windows environment from cyber threats using zero-trust security principles, 2nd Edition . Mark Dunkerley , Matt Tumbarello. ISBN 9781803236544.
• Mastering Linux Security and Hardening. Third Edition. A practical guide to protecting your Linux system from cyber attacks. Donald A. Tevault. ISBN 9781837630516.