Blekinge Institute of Technology
Department of Computer Science

Revision: 4
Reg.no: BTH-4.1.1–0219-2018

COURSE SYLLABUS

Analys av illasinnad programvara (malware)

Malware Analysis

7.5 credits (7,5 högskolepoäng)

Course code: DV2582
Main field of study: Computer Science
Disciplinary domain: Technology
Education level: Second cycle
Specialization: A1N - Second cycle, has only first cycle course/s as entry requirements

Subject area: Computer Technology
Language of instruction: Swedish but teaching in English may occur.
Applies from: 2018-03-01
Approved: 2018-03-01

1. Decision

This course is established by Dean 2017-12-20. The course syllabus is approved by Head of Department of Computer Science and Engineering 2018-03-01 and applies from 2018-03-01.

2. Entry requirements

Admission to the course requires completed courses in Programming, 12 credits, Realtime Systems and Operating Systems, 6 credits, Computer Networking, 6 credits. Attended course in Computer Security, 7.5 credits or Network Security, 8 credits.

3. Objective and content

3.1 Objective

The aim of the course is to enable students to learn how to analyse harmful and malicious software in a safe way. Such analysis is the first step in a systematic approach to prevent or neutralise malware. The focus is on analysis of the advanced methods used in the manufacturing of so-called "cyber arms" and the practical countermeasures to detect and neutralise them.

3.2 Content

- Different techniques to attack and infect systems with malware
- Extortion programs (ransomware/scareware)
- Botnets
- Mobile threats to Android and iOS
- Vulnerabilities online and in social networks
- Rootkits and bootkits
- Antivirus techniques
- Data mining for the detection and analysis of malware

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:
On completion of the course, the students shall be able to
- describe the classification of different types of malware and know their history
- explain and exemplify the behaviour of malicious software, antivirus technologies and security architectures in Windows, Android and iOS

4.2 Competence and skills

On completion of the course, the student will be able to:
On completion of the course, the students shall be able to
- perform reverse engineering of software for ARM and x86 processor architectures
- perform static and dynamic analysis of malicious codes in Windows, Android and iOS
- compile and document analyses of malicious codes in accordance with established standards

4.3 Judgement and approach

On completion of the course, the student will be able to:
On completion of the course, the students shall be able to
- use a completed analysis to assess a threat
- identify and implement appropriate countermeasures

5. Learning activities

The course is given on campus and includes lectures and laboratories (including laboratory reports). Theoretical aspects of the course are presented in the lectures and students should apply the content of the lectures in the course labs.

6. Assessment and grading

Modes of examinations of the course

Code	Module	Credits	Grade
1810	Laboratory Exercise 1	2.5 credits	GU
1820	Laboratory Exercise 2	1.5 credits	GU
1830	Laboratory Exercise 3	1 credits	GU
1840	Exam	2.5 credits	AF

The course will be graded A Excellent, B Very good, C Good, D Satisfactory, E Sufficient, FX Fail, supplementation required, F Fail.

The course information for each course revision should include the assessment criteria and make explicit in which modes of examination that the learning outcomes are assessed.

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

10. Additional information

This course replaces the course DV2567