Blekinge Institute of Technology
Department of Computer Science

Revision: 1
Reg.no: BTH-4.1.14-0663-2021

COURSE SYLLABUS

Analys av skadlig programvara

Malware Analysis

7.5 credits (7,5 högskolepoäng)

Course code: DV2613
Main field of study: Computer Science, Software Engineering
Disciplinary domain: Technology
Education level: Advanced level
Specialization: A1N - Second cycle, has only first-cycle course/s as entry requirements

Language of instruction: English.
Applies from: 2022-01-17
Approved: 2021-09-01

1. Decision

This course is established by Dean 2021-04-29. The course syllabus is approved by Head of Department of Computer Science 2021-09-01 and applies from 2022-01-17.

2. Entry requirements

Admission to the course requires 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 aims to provide students with the skills of real-world threats analysis such as phishing attacks, Advanced Persistent Threats (APTs), exploits, supply-chain attacks, cyberweapon (destroyers), and ransomware (cryptolockers) that have become popular nowadays.

3.2 Content

This course gives an overview of the modern threat landscape and that includes phishing, exploits, malicious implants in office documents, supply-chain attacks, cyberespionage and ransomware campaigns. The students will learn reverse engineering, static and dynamic analysis of malware based on "in-the-wild" examples for Windows and Android platforms (IA-32/Intel® 64, ARM architectures).

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:
• Account for the understanding of the modern security threats including phishing attacks, Advanced Persistent Threats (APTs), exploits, supply-chain attacks, cyberweapon (destroyers), and ransomware (cryptolockers)
• Gain a detailed understanding of reverse engineering, static and dynamic malware analysis techniques

4.2 Competence and skills

On completion of the course, the student will be able to:
• Detect malware and phishing attacks
• Analyse malware for Windows and Android platforms

4.3 Judgement and approach

On completion of the course, the student will be able to:
• Evaluate a cyber threat
• Select appropriate detection and analysis techniques

5. Learning activities

The teaching is organised around online lectures, pre-recorded videos, together with written material and research literature. Throughout the course, communication, feedback, and discussions with teachers and fellow participants will take place through email and the course's online learning platform.

6. Assessment and grading

Modes of examinations of the course

Code	Module	Credits	Grade
2205	Written assignment 1	2.5 credits	GU
2215	Written assignment 2	2.5 credits	GU
2225	Written assignment 3	2.5 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

Compulsory literature:

• Malware Reverse Engineering Handbook, https://ccdcoe.org/library/publications/malware-reverse-engineering-handbook/

Reference literature:

• Reverse Engineering for Beginners, https://beginners.re/main.html

• Michael Sikorski, Andrew Honig. Practical Malware Analysis: The Hands-On Guide to Dissecting Malicious Software 1st Edition, 2012.

• Joshua J. Drake , Zach Lanier , et al. Android Hacker's Handbook, 2014.

• J. Saxe, H. Sanders. Malware Data Science. Attack detection and Attribution, 2018.

Materials such as research articles and other course materials, as well as recommendations for additional reading, are provided via the courses' online platform.