# PHÂN TÍCH MÃ ĐỘC (MALWARE ANALYSIS)
# Đề cương chi tiết (Course Syllabus)

## 1. General Information

**Course name**: Phân tích mã độc (Malware Analysis)

**Course code**: SEC1411_CLC

**Course type:** Compulsory

**Number of credits**: 3

## 2. Objectives

***Knowledge:***

The aim of this course is to provide students with fundamental malware knowledge and analysis techniques, including: classification, behaviors, analysis methods, and cybersecurity applications.

***Skills:***

On successful completion of this course a student will be able to:

- Analyze malware using both static and dynamic analysis techniques
- Use various tools and techniques for practical malware analysis

***Attitude:***

Students are required to attend the classes and complete assignments/projects.

## 3. Abstracts

This course provides students with basic knowledge about malware and malware analysis techniques. It covers malware classification, common malware behaviors, static and dynamic analysis methods, tools for malware analysis, and applications of malware analysis in cybersecurity. The course also includes practical exercises and labs to reinforce theoretical concepts.

## 4. Teaching and learning methods

| | |
|---|---|
| Lectures: | 24h |
| Exercises: | 5h |
| Projects : | 8h |
| Labs: | 8h |
| Individual reading: | 0h |

**5. Prerequisites**: Assembly Programming and Reverse Engineering - SEC1302_CLC

## 6. Learning outcomes

After completing this course, the student is able to:
[CLO1]: Explain the basic concepts of malware and malware analysis

[CLO2]: Apply appropriate static and dynamic analysis techniques and tools to effectively practical malware analysis
[CLO3]: Explain the applications of malware analysis in cybersecurity

**7. Assignment criteria**

| Learning outcomes | Assignment criteria |
|---|---|
| [CLO1]: Explain the basic concepts of malware and malware analysis | Chapter 1 |
| [CLO2]: Apply appropriate static and dynamic analysis techniques and tools to effectively practical malware analysis | Chapter 2, Chapter 3 |
| [CLO3]: Explain the applications of malware analysis in cybersecurity | Chapter 4 |

**8. Outlines**

**Chapter 1 Overview of Malware and Malware Analysis**
- 1.1. Definition and classification of malware
- 1.2. Common behaviors of malware
- 1.3. Overview of malware analysis techniques
- 1.4. Applications of malware analysis in cybersecurity

**Chapter 2 Static Malware Analysis Techniques**
- 2.1. Concepts and principles of static analysis
- 2.2. Tools and methods for static analysis
- 2.3. Static analysis process
- 2.4. Challenges and limitations of static analysis
- 2.5. Practical static analysis

**Chapter 3 Dynamic Malware Analysis Techniques**
- 3.1. Concepts and principles of dynamic analysis
- 3.2. Tools and methods for dynamic analysis
- 3.3. Dynamic analysis process
- 3.4. Challenges and limitations of dynamic analysis
- 3.5. Practical dynamic analysis

**Chapter 4 Applications of Malware Analysis in Cybersecurity**
- 4.1. Malware detection using signatures and behavioral analysis
- 4.2. Digital forensics and incident response for malware attacks
- 4.3. Developing malware prevention and mitigation solutions

**9. Required Textbooks**

[1] Michael Sikorski and Andrew Honig, *Practical Malware Analysis: The Hands-On Guide to Dissecting Malicious Software*, No Starch Press, 2012.

**10. Suggested Textbooks**

[2] Monnappa, K. A. (2018). *Learning Malware Analysis: Explore the concepts, tools, and techniques to analyze and investigate Windows malware*. Packt Publishing Ltd.
[3] Zhussupov, Z. (2024). *Malware Development for Ethical Hackers: Learn how to Develop Various Types of Malware to Strengthen Cybersecurity*. Packt Publishing Limited.
[4] Bruce Dang, Alexandre Gazet, Elias Bachaalany and Sébastien Josse, *Practical Reverse Engineering: x86, x64, ARM, Windows Kernel, Reversing Tools, and Obfuscation*. John Wiley & Sons, 2014.
[5] Alexey Kleymenov and Amr Thabet, *Mastering Malware Analysis: The Complete Malware Analyst's Guide to Combating Malicious Software, APT, Cybercrime, and IoT Attacks*. Packt Publishing, 2019.

**11. Schedule**

| Main contents | Duration | Specific contents |
|---|---|---|
| Chapter 1: Overview of Malware and Malware Analysis | 6h lecture | 1.1. Definition and classification of malware<br>1.2. Common behaviors of malware<br>1.3. Overview of malware analysis techniques<br>1.4. Applications of malware analysis in cybersecurity |
| Chapter 2: Static Malware Analysis Techniques | 8h lecture<br>2h exercise<br>3h project<br>3h lab | 2.1. Concepts and principles of static analysis<br>2.2. Tools and methods for static analysis<br>2.3. Static analysis process<br>2.4. Challenges and limitations of static analysis<br>2.5. Practical static analysis |
| Chapter 3: Dynamic Malware Analysis Techniques | 8h lecture<br>2h exercise<br>3h project<br>3h lab | 3.1. Concepts and principles of dynamic analysis<br>3.2. Types of dynamic analysis methods<br>3.3. Tools for dynamic analysis<br>3.4. Dynamic analysis process<br>3.5. Challenges and limitations of dynamic analysis<br>3.6. Practical dynamic analysis |
| Chapter 4: Applications of Malware Analysis in Cybersecurity | 2h lecture<br>1h exercise<br>2h project<br>2h lab | 4.1. Malware detection using signatures and behavioral analysis<br>4.2. Digital forensics and incident response for malware attacks<br>4.3. Developing malware prevention and mitigation solutions |

**12. Grading Policy**

| | |
|---|---|
| Attendance: | 10% |
| Mid-term exam/exercises: | 10% |
| Course projects: | 30% |
| Final examination: | 50% |