AN TOÀN MẠNG NÂNG CAO (ADVANCED NETWORK SECURITY)
Đề cương chi tiết (Course Syllabus)

1. General Information

Course name: An toàn mạng nâng cao (Advanced Network Security)

Course code: SEC1410_CLC

Course type: Compulsory

Number of credits: 3

2. Objectives

Knowledge:

The aim of this course is to provide students with advanced knowledge to secure the information and network systems.

Skills:

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

- Analyze and select practical security measures to protect information and network systems;
- Deploy suitable security measures to protect information and network systems.

Attitude:

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

3. Abstracts

This course provides students with advanced knowledge of security measures to protect information and network systems, including techniques and technologies to ensure network security; techniques to secure transferred information, security for network systems; and security for cloud computing.

4. Teaching and learning methods

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

5. Prerequisites: Network Security - SEC1406_CLC

6. Learning outcomes

After completing this course, the student is able to:
[CLO1]: Explain the security measures to protect information and network systems
[CLO2]: Analyze and select practical security measures to protect information and network systems
[CLO3]: Deploy suitable security measures to protect information and network systems

7. Assignment criteria

Learning outcomes	Assignment criteria
[CLO1]: Explain the security measures to protect information and network systems	Chapter 1, Chapter 2, Chapter 3, Chapter 4
[CLO2]: Analyze and select practical security measures to protect information and network systems	Chapter 1, Chapter 2, Chapter 3, Chapter 4
[CLO3]: Deploy suitable security measures to protect information and network systems	Chapter 1, Chapter 2, Chapter 3, Chapter 4

8. Outlines

Chapter 1 Techniques and technologies to ensure network security

1.1. Access control
1.2. Firewalls
1.3. Virtual private network technologies
1.4. Honeypots and honeynets

Chapter 2 Security for information transmission

2.1. Information security requirements for transmission
2.2. Information security solutions based on cryptography
2.3. Information security protocols

Chapter 3 Security for network systems

3.1. LAN security
3.2. WLAN security
3.3. Intranet security
3.4. Mobile networks and security issues
3.5. IoT and security issues

Chapter 4 Security for cloud computing

4.1. Introduction to cloud computing
4.2. Cloud computing architecture
4.3. Platform technologies of cloud computing
4.4. Security issues in cloud computing

9. Required Textbooks

[1] Roberta Bragg, Mark Rhodes-Ousley and Keith Strassberg, *Network Security: The Complete Reference*, McGraw-Hill Osborne Media, 2013.

10. Suggested Textbooks

[2] Mark Rhodes-Ousley. *Information Security: The Complete Reference*, McGraw-Hill Osborne Media, 2nd edition, 2013.
[3] William Stallings, *Cryptography and Network Security Principles and Practice*, 7th edition, Pearson Education Limited, 2022.

[4] Michael E. Whitman, Herbert J. Mattord. *Principles of Information Security*, 7th edition, Cengage Learning, 2021.
[5] 5. Michael T. Simpson, Nicholas Antill. *Hands-On Ethical Hacking and Network Defense*, 3rd edition, Cengage Learning, 2016.

11. Schedule

Main contents	Duration	Specific contents
Chapter 1 Techniques and technologies to ensure network security	6h lecture 1h exercise 2h project 2h lab	1.1. Access control 1.2. Firewalls 1.3. Virtual private network technologies 1.4. Honeypots and honeynets
Chapter 2 Security for information transmission	6h lecture 2h exercise 3h project 3h lab	2.1. Information security requirements for transmission 2.2. Information security solutions based on cryptography 2.3. Information security protocols
Chapter 3 Security for network systems	6h lecture 1h exercise 2h project 2h lab	3.1. LAN security 3.2. WLAN security 3.3. Intranet security 3.4. Mobile networks and security issues 3.5. IoT and security issues
Chapter 4 Security for cloud computing	4h lecture 1h exercise 1h project 1h lab	4.1. Introduction to cloud computing 4.2. Cloud computing architecture 4.3. Platform technologies of cloud computing 4.4. Security issues in cloud computing

12. Grading Policy

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