NETWORK SECURITY

1.Thông tin về học phần (General Information)

Tên học phần (Course name):	Network Security
Mã học phần (Course code):	INT1482
Số tín chỉ (Number of credits):	3
Loại học phần (Course type):	Compulsory

Học phần tiên quyết (Prerequisites):

Học phần trước (Previous courses): Computer Networks (INT1336), Fundamentals of Information Security (INT1472)

Học phần song hành (Parallel courses):

Các yêu cầu đối với học phần (Course requirements):

- Lecture room: Projector, black board, microphone and speaker
- Laboratory: Computers with internet access

Giờ tín chỉ đối với các hoạt động (Teaching and Learning hours):

- Lý thuyết (Lectures):	30h
- Bài tập (Exercises):	0h
- Bài tập lớn (Projects):	8h
- Thực hành (Labs):	7h
- Tự học (Individual reading):	0h

Địa chỉ Khoa/Bộ môn phụ trách học phần (Address of the Faculty/Department in charge of the course):

- Address: Faculty of Information Technology 1 - Posts and Telecommunications Institute of Technology, Km10, Nguyen Trai Street, Ha Dong District, Hanoi.
- Phone number: (024) 33510432

2. Mục tiêu học phần (Objectives)

Về kiến thức (Knowledge):

The goal of this course is to provide learners with important knowledge about network security, including:

- basic concepts of network security
- threats and vulnerabilities in network security
- network attacks and defense techniques

Kỹ năng (Skills):

The aim of this course is to equip learners with skills in:

- applying the learned knowledge to recognize network security threats and vulnerabilities;
- determining and analyzing the type of network attacks and countermeasure;
- simulating network attacks and countermeasures in network security lab.

Thái độ, Chuyên cần (Attitude):

Students must ensure the required class attendance, assigned projects & labs and self-studying hours.

3. Tóm tắt nội dung học phần (Description)

The course introduces learners to knowledge about network security, including basic concepts of attacks and defenses, threats and vulnerabilities in network security, different types of attack techniques and countermeasures, prevention and response to network attacks.

4. Nội dung chi tiết học phần (Outlines)

Chapter 1. Introduction to network security

1.1. Network security requirements and methodology

- 1.1.1. Network security requirements
- 1.1.2. Security methodology

1.2. Risk analysis and defense models

- 1.2.1. Threat assessment
- 1.2.2. Risk analysis
- 1.2.3. Defense models

1.3. Security organization

- 1.3.1. Roles and responsibilities
- 1.3.2. Security operations management
- 1.3.3. Security awareness training

Chapter 2. Threat and vulnerability in network security

2.1. Threat and vulnerability in network protocols

- 2.1.1. Basic application layer protocols
- 2.1.2. DNS
- 2.1.3. TCP/UDP
- 2.1.4. Routing protocols
- 2.1.5. Others

2.2. Design and analysis of security protocols

2.3. Threat and vulnerability in network devices

- 2.3.1. Switches
- 2.3.2. Routers
- 2.3.3. Others

Chapter 3. Network attack techniques

3.1. Reconnaissance

- 3.1.1. Introduction
- 3.1.2. DNS reconnaissance
- 3.1.3. Collect and check domain name and IP address information
- 3.1.4. Reconnaissance using search engines

3.2. Scanning

- 3.2.1. Introduction
- 3.2.2. Determine active hosts
- 3.2.3. Determine active ports and services
- 3.2.4. Determine operating systems
- 3.2.5. Scan vulnerabilities

3.3. Intrusion techniques

3.3.1. Client intrusion
3.3.2. Firewall bypassing techniques

3.4. Denial of services attacks
3.4.1. Link layer denial of service attacks
3.4.2. Transport layer denial of service attacks
3.4.3. Application layer denial of service attacks

Chapter 4. Attack prevention and response

4.1. Attack prevention methods
4.1.1. Secure the physical environment
4.1.2. Keep patches updated
4.1.3. Secure user account
4.1.4. Secure the file system
4.1.5. Create a security defense plan

4.2. Incident response
4.2.1. Incident response plan
4.2.2. Forensics
4.2.3. Legal issues

4.3. Disaster recovery and business continuity
4.3.1. Disaster recovery plan
4.3.2. Business continuity plan

5. Học liệu (Textbooks)

5.1. Học liệu bắt buộc (Required Textbooks)

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

5.2. Học liệu tham khảo (Optional Textbooks)

[2]. John Chirillo, Hack attacks revealed: A complete reference with custom security hacking toolkit, John Wiley & Sons, 2001.

[3]. Jie Wang, Computer Network Security: Theory and Practice, Springer, 2009.

[4]. Michael T. Simpson, Kent Backman, Hands-On Ethical Hacking and Network Defense, Delmar Cengage Learning, 2010.

[5]. Stuart McClure, Joel Scambray and George Kurtz, Hacking Exposed 7: Network Security Secrets & Solutions, McGraw-Hill Osborne Media, 2012.

[6]. William Stallings, Cryptography and Network Security: Principles and Practice, Prentice Hall, 2016.

6. Phương pháp, hình thức kiểm tra – đánh giá kết quả học tập học phần (Grading Policy)

Grading method	Percentage	Group/Individual
- Attendance	10%	Individual
- Mid-term exams	10%	Individual
- Projects	30%	Group or individual
- Final examination	50%	Individual

Trưởng Bộ môn **(Head of Department)**	**Giảng viên biên soạn** **(Lecturer)**
Hoàng Xuân Dậu	**Nguyễn Ngọc Điệp**