PENETRATION TESTING

1.Thông tin về học phần (General Information)

Tên học phần (Course name): Penetration testing

Mã học phần (Course code): INT14107

Số tín chỉ (Number of credits): 3

Loại học phần (Course type): Elective

Học phần tiên quyết (Prerequisites):

Học phần trước (Previous courses): Fundamentals of Information Security (INT1472)

Học phần song hành (Parallel courses): Network Security (INT1482)

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 fundamental knowledge about penetration testing, including:

- basic concepts of penetration testing
- penetration testing techniques for information systems
- knowledge of techniques for exploiting using shellcode
- knowledge of vulnerability analysis.

Kỹ năng (Skills):

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

- applying the learned knowledge to perform penetration testing
- analyzing and exploiting some vulnerabilitie.

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)

This course introduces learners to basic knowledge of penetration testing, including types of penetration testing techniques; the detailed steps of penetration testing with planning, implementation and completion; techniques of penetration testing for information systems and supporting tools; and in-depth knowledge of techniques for exploiting and analyzing vulnerabilities.

4. Nội dung chi tiết học phần (Outlines)

Chapter 1. Introduction

1.1. Introduction to penetration testing

1.2. Roles of penetration testing

1.3. Ethics of penetration testing

1.4. Penetration testing stages

1.5. Supporting tools

Chapter 2. Essential techniques for penetration testing

2.1. Social engineering

2.1.1. Introduction

2.1.2. Common attack techniques

2.1.3. Social engineering prevention

2.2. Physical penetration testing

2.2.1. Introduction

2.2.2. Common attack techniques

2.2.3. Prevention

2.3. Insider attack penetration testing

2.3.1. Introduction

2.3.2. Conduct an insider attack

2.3.3. Insider attack prevention

2.4. Network penetration testing

2.4.1. Network penetration testing techniques

2.4.2. Prevention

Chapter 3. Vulnerability exploit using shellcode

3.1. Buffer overflow vulnerability exploit

3.1.1. Introduction to buffer overflow

3.1.2. Exploiting buffer overflow

3.1.3. Memory protection methods

3.2. Shellcode and its application in exploiting vulnerabilities

3.3. Types of shellcode

3.3.1. Shellcode in user space

3.3.2. Shellcode in kernel space

3.4. Create a shellcode

3.4.1. Create a simple shellcode

3.4.2. Create a shell bind shellcode

3.4.3. Create a reverse shell shellcode

3.4.4. Encrypt a shellcode

3.4.5. Shellcode generator

Chapter 4. Vulnerability analysis

4.1. Source code analysis

4.1.1. Manual source code analysis

4.1.2. Automated source code analysis

4.2. Binary code analysis

4.2.1. Manual auditing of binary code

4.2.2. Automated binary analysis

4.3. Fuzzing technique

4.3.1. Fuzzing with known protocols

4.3.2. Fuzzing with unknown protocols

4.4. Client-side vulnerability

4.4.1. Impacts of client-side vulnerability

4.4.2. Detecting client-side vulnerability

4.4.3. Prevention

4.5. Vulnerability exploitation

4.5.1. Exploitability

4.5.2. Payload construction

4.6. Exploit mitigation

4.6.1. Some common methods

4.6.2. Patching

Chapter 5: Post exploitation

5.1. Rules of engagement

5.2. Data gathering, network analysis

5.3. Pillaging

5.4. Pivoting

5.5. Clean-up

5. Học liệu (Textbooks)

5.1. Học liệu bắt buộc (Required Textbooks)

[1]. Lee Allen, *Advanced Penetration Testing for Highly-Secured Environments: The Ultimate Security Guide*, Packt Publishing, 2012.

[2]. Harper, Allen, et al, *Gray Hat Hacking: The Ethical Hackers Handbook*, McGraw-Hill

Osborne Media, 2011.

5.2. Học liệu tham khảo (Optional Textbooks)

[3]. Stuart McClure, Joel Scambray, George Kurtz, *Hacking Exposed 7: Network Security Secrets and Solution*s, McGraw Hill, 2012.

[4]. Sean-Philip Oriyano, Michael Gregg, *Hacker Techniques, Tools, and Incident Handling*, Jones & Bartlett Learning, 2010.

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)

Hoàng Xuân Dậu

Giảng viên biên soạn
(Lecturer)

Nguyễn Ngọc Điệp