BAN CƠ YẾU CHÍNH PHỦ
HỌC VIỆN KỸ THUẬT MẬT MÃ

ĐẶNG XUÂN BẢO, HOÀNG THANH NAM, VŨ THỊ VÂN

NGÂN HÀNG CÂU HỎI THI TRẮC NGHIỆM
MÃ ĐỘC

Hà Nội, 2021

Phần I. TỔNG HỢP CÁC PHẦN NỘI DUNG MÔN HỌC

Môn học: Mã độc

Khoa: An toàn thông tin

Các chương trình đào tạo có sử dụng môn học:

P1: ĐH Chính quy An toàn thông tin

Các phần nội dung môn học trong các chương trình đào tạo:

TT	Phần nội dung	P1
1	Tổng quan về mã độc	☑
2	Phân tích mã độc cơ bản	☑
3	Dịch ngược mã độc	☑
4	Kỹ thuật phân tích mã độc dựa trên gỡ rối	☑
5	Phân tích các chương trình độc hại trên Windowss	☑
6	Phân tích một số cơ chế và hành vi thông thường của mã độc	☑
7	Các kỹ thuật chống phân tích	☑
8	Phát hiện và xử lý sự cố mã độc	☑

Phần II. TRÍCH LƯỢC ĐỀ CƯƠNG CHI TIẾT MÔN HỌC

1. Thông tin chung

Tên học phần	Mã độc
Tên tiếng Anh	Malware
Số tín chỉ	3
Học phần học trước	Kiến trúc máy tính và hợp ngữ

2. Mục tiêu học phần

2.1. Mục tiêu chung

Học phần này hướng đến giúp cho sinh viên xây dựng kỹ năng phân tích, phát hiện mã độc, dịch ngược các chương trình độc hại nhằm tìm kiếm các hành vi và tham số của mã độc qua đó đưa ra các phương pháp phát hiện và phòng chống mã độc thực tế.

2.2. Mục tiêu cụ thể

Mục tiêu	Mô tả
M1	Hiểu các khái niệm về mã độc
M2	Hiểu các cơ chế hoạt động và hành vi của mã độc, các dạng mã độc và cách thức phát tán, gây hại lên hệ thống thông tin
M3	Có khả năng xây dựng môi trường phân tích tĩnh và động mã độc
M4	Biết cách vận dụng các công cụ phân tích mã độc như: IDA Pro, OllyDbg, WinDbg, Process moniter, Process Explorer, PEiD, Dependency Walker,...
M5	Kỹ năng phân tích phát hiện mã độc
M6	Có kỹ năng làm việc nhóm và thuyết trình.
M7	Có khả năng đọc hiểu các tài liệu bằng tiếng Anh
M8	Có thái độ học tập tích cực, chủ động và có khả năng tương tác với giảng viên và các bạn trong nhóm

3. Mô tả học phần

Học phần này bao gồm ba phần nội dung chính. Phần thứ nhất trình bày tổng quan về mã độc, bao gồm: khái niệm mã độc, phân loại mã độc, hành vi tiêu biểu của mã độc và tác hại của mã độc, các con đường lây nhiễm mã độc và các phương pháp phòng chống. Phần thứ hai trình bày chi tiết cơ chế hoạt động của mã độc: cơ chế lây nhiễm của file virus, cơ chế tự bảo vệ của mã độc, kỹ thuật rootkit, cơ chế thực thi một số tác vụ điển hình của mã độc. Phần thứ ba trình bày chi tiết về phân tích mã độc, bao gồm: các phương pháp phân tích tĩnh, phân tích động, trích xuất mẫu nhận dạng mã độc cho công cụ diệt mã độc (antivirus).

4. Nội dung học phần

Chương 1. Tổng quan về mã độc (3 LT)

1.1. Mã độc

1.2. Phân loại mã độc

1.3. Một số cơ chế hoạt động của mã độc

Chương 2. Phân tích mã độc cơ bản (6 LT + 9 TH)

2.1. Các phương pháp phân tích mã độc

2.2. Công cụ và kiến thức cơ sở

2.3. Các nguyên tắc khuyến nghị trong phân tích mã độc

2.4. Phân tích tĩnh cơ bản

2.5. Phân tích động cơ bản

2.6. Xây dựng môi trường phân tích mã độc

2.7. Ví dụ

Chương 3. Dịch ngược mã độc (3 LT + 3 TH)

3.1. Nhắc lại về Assembly

3.2. Sử dụng IDA pro để dịch ngược mã độc

3.3. Sử dụng đối sánh chéo

3.4. Phân tích hàm

3.5. Sử dụng biểu đồ hàm

3.6. Một số lưu ý

Chương 4. Kỹ thuật phân tích mã độc dựa trên gỡ rối (3 LT + 3 TH)

4.1. Gỡ rối

4.2. Gỡ rối mức mã nguồn và mức Assembly

4.3. Gỡ rối ở chế độ nhân và chế độ người dùng

4.4. Sử dụng trình gỡ rối trong phân tích mã độc

4.5. Xử lý ngoại lệ

4.6. Sửa đổi thực thi chương trình với trình gỡ rối

4.7. Phân tích mã độc với OllyDbg

Chương 5. Phân tích các chương trình độc hại trên Windowss (3 LT + 3 TH)

5.1. Windowss API

5.2. Windowss Registry

5.3. Các API xử lý kết nối mạng

5.4. Phân tích mã độc trên Windowss

5.5. Chế độ nhân và chế độ người dùng

5.6. Các native API

Chương 6. Phân tích một số cơ chế và hành vi thông thường của mã độc (6 LT + 3 TH)

6.1. Downloader và Launcher

6.2. Backdoor

6.3. Công cụ đánh cắp thông tin

6.4. Các cơ chế duy trì hiện diện

6.5. Leo thang đặc quyền

6.6. Các kỹ thuật trong Rootkit

6.7. Launcher

6.8. Tiêm vào tiến trình

6.9. Thay thế tiến trình

6.10. Tiêm vào hook

6.11. Detour

6.12. Tiêm vào APC

Chương 7. Các kỹ thuật chống phân tích (3 LT + 3 TH)

7.1. Nén

7.2. Mã hóa

7.3. Làm rối mã

7.4. Một số kỹ thuật khác

Chương 8. Phát hiện và xử lý sự cố mã độc (3 LT + 6 TH)

8.1. Quy trình xử lý sự cố mã độc

8.2. Chuẩn bị

8.3. Phát hiện

8.4. Ngăn chặn

8.5. Xử lý triệt để

8.6. Phục hồi

5. Một số ghi chú về đề cương chi tiết môn học

Phần III. PHÂN RÃ CHUẨN ĐẦU RA HỌC PHẦN

1. Các chuẩn đầu ra được đánh giá

TT	Ký hiệu	Chuẩn đầu ra	P1
1	CLO1	Trình bày được các khái niệm cơ bản và cơ chế hoạt động, hành vi của một số loại mã độc	☑
2	CLO2	Phân tích được một số mẫu mã độc sử dụng môi trường và một số công cụ phân tích	☑
3	CLO3	Trình bày được quy trình xử lý sự cố mã độc	☑

Phần IV. MA TRẬN ĐỀ THI

1. Chương trình ĐH Chính quy An toàn thông tin (P1)

Tổng số câu hỏi: 45 câu. Thời gian làm bài: 60 phút.

Tài liệu được phép sử dụng: Không

Cấu trúc đề thi:

TT	Nhóm câu hỏi	SL	Điểm	NB	TH	VD	VDC
1	1.1. Khái niệm và phân loại (NB)	3	3	3			
2	1.2. Khái niệm và phân loại (TH)	4	4		4		
3	1.3. Cơ chế hoạt động của mã độc (TH)	5	5		4		
4	1.4. Cơ chế chống phân tích (TH)	2	2		2		
5	2.1. Một số kiến thức Assembly quan trọng (NB)	3	3	3			
6	2.2. Một số kiến thức Windows quan trọng (NB)	4	4	4			
7	2.3. Tổng quan về các công cụ phân tích mã độc (TH)	4	4		4		
8	2.4. Tổng quan về các công cụ phân tích mã độc (TH)	8	8		8		
9	2.4. Phân tích cơ bản (VD)	2	2			2	

TT	Nhóm câu hỏi	SL	Điểm	NB	TH	VD	VDC
10	2.5. Phân tích nâng cao (VD)	3	3			3	
11	2.6. Phân tích các cơ chế chống phân tích của mã độc (VD)	2	2			2	
12	3.1. Quy trình ứng phó sự cố mã độc (TH)	5	5		5		
	Tổng	**45**	**45**	**10**	**28**	**7**	