HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG
KHOA CÔNG NGHỆ THÔNG TIN
*****

ĐỀ CƯƠNG MÔN HỌC
(Phương pháp đào tạo theo tín chỉ)

TÊN HỌC PHẦN: PHÂN TÍCH MÃ ĐỘC

Mã học phần: INT14164
(2 tín chỉ)

Biên soạn
NGUYỄN NGỌC ĐIỆP

Hà Nội - 2021

ĐỀ CƯƠNG HỌC PHẦN: PHÂN TÍCH MÃ ĐỘC

Khoa: Công nghệ thông tin 1 **Bộ môn**: An toàn thông tin

1.Thông tin về giảng viên

1.1. Giảng viên 1:

Họ và tên: Nguyễn Ngọc Điệp
Chức danh, học hàm, học vị: Giảng viên – Tiến sỹ
Địa điểm làm việc: Bộ môn An toàn thông tin, Khoa Công nghệ thông tin 1,
Học viện Công nghệ Bưu chính Viễn thông
Địa chỉ liên hệ: Bộ môn An toàn thông tin, Khoa Công nghệ thông tin 1,
Học viện Công nghệ Bưu chính Viễn thông
Điện thoại: Email: diepnguyenngoc@ptit.edu.vn
Các hướng nghiên cứu chính: Điện toán lan tỏa, nhận dạng hoạt động người, An toàn và bảo mật thông tin.

1.2. Giảng viên 2:

Họ và tên: Hoàng Xuân Dậu
Chức danh, học hàm, học vị: Tiến sỹ, Giảng viên
Địa điểm làm việc: Bộ môn An toàn thông tin, Công nghệ thông tin 1,
Học viện Công nghệ Bưu chính Viễn thông
Địa chỉ liên hệ: Bộ môn An toàn thông tin, Công nghệ thông tin 1,
Học viện Công nghệ Bưu chính Viễn thông
Điện thoại: Email: dauhx@ptit.edu.vn
Các hướng nghiên cứu chính: Học máy, An toàn và bảo mật thông tin.

2. Thông tin chung về môn học

- Tên môn học: Phân tích mã độc
- Tên tiếng Anh của môn học: Malware analysis
- Mã môn học: INT14164
- Số tín chỉ (TC): 2
- Loại môn học: Tự chọn
- **Các môn học tiên quyết**: Cơ sở an toàn thông tin, Kiến trúc máy tính và hệ điều hành
- **Môn học trước:**
- **Môn học song hành:**
- Các yêu cầu đối với môn học (nếu có):
  Phòng học lý thuyết: Có máy chiếu
  Phòng thực hành: Phòng máy tính nối mạng Internet
- Giờ tín chỉ đối với các hoạt động:

+ Nghe giảng lý thuyết: 12 tiết
+ Chữa bài trên lớp: tiết
+ Bài tập lớn/Tiểu luận: 14 tiết
+ Thảo luận và Hoạt động nhóm: tiết
+ Thí nghiệm, Thực hành: 4 tiết
+ Tự học: tiết

Địa chỉ Khoa/Bộ môn phụ trách môn học:

- Địa chỉ: Bộ môn An toàn thông tin, Khoa Công nghệ thông tin 1, Học viện Công nghệ Bưu chính Viễn thông, Km 10 Nguyễn Trãi, Hà Đông, Hà Nội
- Điện thoại: 04.3854 5604

3. Mục tiêu của môn học

Về kiến thức: Cung cấp cho người học các khái niệm cơ bản và phương pháp phân tích mã độc, bao gồm:

- các khái niệm và nhiệm vụ cơ bản của phân tích mã độc
- các phương pháp phân tích tĩnh, phân tích động, các phương pháp phân tích cơ bản và nâng cao trên môi trường x86; phân tích hoạt động của chương trình Windows
- các hành vi của mã độc và cách thức mã độc che dấu khỏi bị phát hiện, chống lại phân tích.

Kỹ năng: Trang bị cho người học các kỹ năng về:

- vận dụng kiến thức đã học để phân tích mã đã biên dịch và hiểu được hoạt động của chương trình
- xây dựng môi trường máy ảo và thực hiện phân tích mã độc với các hành vi
- phân tích được các kỹ thuật mã độc sử dụng để chống lại việc phát hiện và phân tích mã độc.

Thái độ, Chuyên cần: Người học cần tham gia học tập đầy đủ trên lớp và làm các bài tập về nhà.

Mục tiêu chi tiết cho từng nội dung của môn học

Mục tiêu / Nội dung	Bậc 1	Bậc 2	Bậc 3
Chương 1: Tổng quan về phân tích mã độc	Hiểu được mã độc là gì và phân loại mã độc, phân biệt được một số kỹ thuật phân tích mã độc		
Chương 2: Các kỹ thuật phân tích mã độc cơ bản	Hiểu được kỹ thuật phân tích và yêu cầu đối với môi trường cần thiết để thực hiện phân tích mã độc	Cài đặt được môi trường và mô phỏng mạng đáp ứng cho phân tích mã độc, phân tích được mã độc đơn giản trong môi trường lab	
Chương 3: Các kỹ thuật phân tích mã độc nâng cao	Hiểu được phương pháp, kỹ thuật phân tích mã độc nâng cao	Sử dụng công cụ để phân tích một số mã độc cụ thể trong môi trường lab	Vận dụng được các công cụ phân tích mã độc để hiểu được cách thức hoạt động của mã độc thực tế
Chương 4: Một số hành vi và kỹ thuật sử dụng trong mã độc	Nắm được các hành vi của mã độc và các kỹ thuật được sử dụng trong mã độc	Sử dụng công cụ để phân tích được các hành vi và kỹ thuật của mã độc trong môi trường lab	Sử dụng công cụ để hiểu được hành vi và kỹ thuật sử dụng trong mã độc thực tế

4. Tóm tắt nội dung môn học

Môn học cung cấp cho người học những kiến thức cơ bản về mã độc, phương pháp phân tích mã độc sử dụng các công cụ thích hợp. Với những kiến thức này, người học có thể thực hiện phân tích, gỡ rối và dịch ngược các phần mềm mã độc an toàn. Nội dung môn học bao gồm 4 chương như sau. Chương 1 trình bày tổng quan về phân tích mã độc. Chương 2 giới thiệu các kỹ thuật phân tích mã độc cơ bản. Chương 3 trình bày các kỹ thuật phân tích mã độc nâng cao. Chương 4 mô tả về một số hành vi của mã độc cũng như các kỹ thuật được sử dụng trong đó nhằm chống lại việc phát hiện và phân tích mã độc.

5. Nội dung chi tiết môn học

Chương 1. Tổng quan về phân tích mã độc

1.1. Khái quát về mã độc

1.2. Phân loại mã độc

1.3. Một số kỹ thuật phân tích mã độc

Chương 2. Các kỹ thuật phân tích mã độc cơ bản

2.1. Kỹ thuật phân tích tĩnh

2.2. Phân tích mã độc sử dụng máy ảo

2.3. Kỹ thuật phân tích động cơ bản

2.4. Phân tích động với dịch vụ mạng mô phỏng

Chương 3. Các kỹ thuật phân tích mã độc nâng cao

3.1. Dịch mã máy sang hợp ngữ

3.2. Nhận dạng các cấu trúc lệnh mức cao trong hợp ngữ

3.3. Phân tích mã độc trên Windows

3.4. Phân tích động với trình gỡ rối

3.5. Phân tích nhân Windows với trình gỡ rối

Chương 4. Một số hành vi và kỹ thuật sử dụng trong mã độc

4.1. Một số hành vi của mã độc

4.2. Khởi chạy mã độc bí mật

4.3. Mã hóa dữ liệu

4.4. Chống phân tích

4.5. Đóng gói và mở gói

6. Học liệu

6.1. Học liệu bắt buộc

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

6.2. Học liệu tham khảo

[2] 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.

[3] Steven Adair, Matthew Richard, Michael Hale Ligh, Blake Hartstein, *Malware Analyst's Cookbook and DVD: Tools and Techniques for Fighting Malicious Code*. Wiley Publishing, Inc, 2010.

[4] 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.

7. Hình thức tổ chức dạy học

7.1 Lịch trình chung:

Nội dung	Hình thức tổ chức dạy môn học					Tổng cộng
	Lên lớp			Thực hành	Tự học	
	Lý thuyết	BT lớn/Tiểu luận	Thảo luận			
Nội dung 1: Khái quát về mã độc; Phân loại mã độc và kỹ thuật phân tích mã độc	2					2
Nội dung 2: Kỹ thuật phân tích tĩnh; Phân tích mã độc sử dụng máy ảo; Kỹ thuật phân tích động cơ bản và mô phỏng dịch vụ mạng	2	2		2		6
Nội dung 3: Dịch mã máy sang hợp ngữ; Nhận dạng các cấu trúc lệnh mức cao trong hợp ngữ; Phân tích mã độc trên Windows	2	4				6
Nội dung 4: Phân tích động với trình gỡ rối; Phân tích nhân Windows với trình gỡ rối	2	4		2		8
Nội dung 5: Một số hành vi của mã độc; Khởi chạy mã độc bí mật	2	2				4
Nội dung 6: Mã hóa dữ liệu; Chống phân tích; Đóng gói và mở gói	2	2				4
Tổng cộng	**12**	**14**		**4**		**30**

7.2. Lịch trình tổ chức dạy học cụ thể

Tuần 1, Nội dung 1: Khái quát về mã độc; Phân loại mã độc và kỹ thuật phân tích mã độc.

Hình thức tổ chức dạy học	**Thời gian** *(tiết TC)*	**Nội dung chính**	**Yêu cầu đối với sinh viên**	**Ghi chú**

Lý thuyết	2	- Khái quát về mã độc - Phân loại mã độc và kỹ thuật phân tích mã độc	- Đọc phần đầu quyển 1	

Tuần 2, Nội dung 2: Kỹ thuật phân tích tĩnh; Phân tích mã độc sử dụng máy ảo; Kỹ thuật phân tích động cơ bản và mô phỏng dịch vụ mạng

Hình thức tổ chức dạy học	Thời gian *(tiết TC)*	Nội dung chính	Yêu cầu đối với sinh viên	Ghi chú
Lý thuyết	2	- Kỹ thuật phân tích tĩnh; Phân tích mã độc sử dụng máy ảo; Kỹ thuật phân tích động cơ bản	- Đọc phần 1, quyển 1	

Tuần 3, Nội dung 2: Kỹ thuật phân tích tĩnh; Phân tích mã độc sử dụng máy ảo; Kỹ thuật phân tích động cơ bản và mô phỏng dịch vụ mạng (tiếp)

Hình thức tổ chức dạy học	Thời gian *(tiết TC)*	Nội dung chính	Yêu cầu đối với sinh viên	Ghi chú
Bài tập lớn/Tiểu luận	2	- Tìm hiểu về các kỹ thuật phân tích động cơ bản và công cụ để phân tích một file mã độc cụ thể	- Chuẩn bị bài tiểu luận theo nhóm và viết báo cáo	

Tuần 4, Nội dung 3: Dịch mã máy sang hợp ngữ; Nhận dạng các cấu trúc lệnh mức cao trong hợp ngữ; Phân tích mã độc trên Windows

Hình thức tổ chức dạy học	Thời gian *(tiết TC)*	Nội dung chính	Yêu cầu đối với sinh viên	Ghi chú
Lý thuyết	2	- Dịch mã máy sang hợp ngữ; - Nhận dạng các cấu trúc lệnh mức cao trong hợp ngữ - Phân tích mã độc trên Windows	- Đọc phần 2 quyển 1	

Tuần 5, Nội dung 3: Dịch mã máy sang hợp ngữ; Nhận dạng các cấu trúc lệnh mức cao trong hợp ngữ; Phân tích mã độc trên Windows (tiếp)

Hình thức tổ chức dạy học	Thời gian *(tiết TC)*	Nội dung chính	Yêu cầu đối với sinh viên	Ghi chú
Bài tập lớn/Tiểu luận	4	- Sử dụng công cụ IDA pro để phân tích mã độc trên Windows, gồm: dịch ngược hợp ngữ, các chức	- Chuẩn bị bài tiểu luận theo nhóm và viết báo cáo	

		năng trong IDA, phân tích các khối code C trong hợp ngữ của mã độc, nhận dạng các API Windows, chạy mã độc và từ đó tìm ra các tính năng của ứng dụng này.		

Tuần 6, Nội dung 4: Phân tích động với trình gỡ rối; Phân tích nhân Windows với trình gỡ rối

Hình thức tổ chức dạy học	Thời gian *(tiết TC)*	Nội dung chính	Yêu cầu đối với sinh viên	Ghi chú
Lý thuyết	2	- Phân tích động với trình gỡ rối; Phân tích nhân Windows với trình gỡ rối	- Đọc phần 3, quyển 1	

Tuần 7, Nội dung 4: Phân tích động với trình gỡ rối; Phân tích nhân Windows với trình gỡ rối (tiếp)

Hình thức tổ chức dạy học	Thời gian *(tiết TC)*	Nội dung chính	Yêu cầu đối với sinh viên	Ghi chú
Bài tập lớn/Tiểu luận	4	- Tìm hiểu sử dụng công cụ OllyDbg và WinDbg để gỡ rối. So sánh với IDA Pro. Phân tích, gỡ rối ứng dụng, gồm: khởi tạo và chạy ứng dụng, sử dụng breakpoint, trace, phân tích shellcode, nạp DLL. Sử dụng WinDbg để phân tích nhân Windows.	- Chuẩn bị bài tiểu luận theo nhóm và viết báo cáo	

Tuần 8, Nội dung 5: Một số hành vi của mã độc; Khởi chạy mã độc bí mật

Hình thức tổ chức dạy học	Thời gian *(tiết TC)*	Nội dung chính	Yêu cầu đối với sinh viên	Ghi chú
Lý thuyết	2	- Một số hành vi của mã độc; Khởi chạy mã độc bí mật	- Đọc phần 1, quyển 4, chương 11, 12	

Tuần 9, Nội dung 5: Một số hành vi của mã độc; Khởi chạy mã độc bí mật (tiếp)

Hình thức tổ chức dạy học	Thời gian *(tiết TC)*	Nội dung chính	Yêu cầu đối với sinh viên	Ghi chú
Bài tập lớn/Tiểu	2	- Phân tích ứng dụng mã	- Chuẩn bị bài tiểu	

luận		độc để thấy được hành vi download, upload, cửa hậu, đánh cắp tài khoản, cơ chế persistance, nâng quyền, tiêm process, hook.	luận theo nhóm và viết báo cáo	

Tuần 10, Nội dung 6: Mã hóa dữ liệu; Chống phân tích; Đóng gói và mở gói

Hình thức tổ chức dạy học	Thời gian *(tiết TC)*	Nội dung chính	Yêu cầu đối với sinh viên	Ghi chú
Lý thuyết	2	- Mã hóa dữ liệu; Chống phân tích; Đóng gói và mở gói	- Đọc phần 1, quyển 4, chương 13, 14	

Tuần 11, Nội dung 6: Mã hóa dữ liệu; Chống phân tích; Đóng gói và mở gói (tiếp)

Hình thức tổ chức dạy học	Thời gian *(tiết TC)*	Nội dung chính	Yêu cầu đối với sinh viên	Ghi chú
Bài tập lớn/Tiểu luận	2	- Phân tích ứng dụng mã độc để thấy được hành vi Mã hóa dữ liệu; Chống phân tích; Đóng gói và mở gói.	- Chuẩn bị bài tiểu luận theo nhóm và viết báo cáo	

8. Chính sách đối với môn học và các yêu cầu khác của giảng viên:

- Các bài tập/tiểu luận phải làm đúng hạn.
- Thiếu một điểm thành phần (bài tập, bài kiểm tra giữa kỳ), hoặc nghỉ quá 20% tổng số giờ của môn học, không được thi hết môn.
- Tham gia đầy đủ và hoàn thành các bài thực hành theo yêu cầu.

9. Phương pháp, hình thức kiểm tra – đánh giá kết quả học tập môn học

9.1. Kiểm tra đánh giá định kỳ

Hình thức kiểm tra *(Tham khảo ví dụ dưới đây)*	Tỷ lệ đánh giá	Đặc điểm đánh giá
- Tham gia học tập trên lớp (đi học đầy đủ, tích cực thảo luận)	10 %	Cá nhân
- Các bài tập/tiểu luận và thảo luận trên lớp	20%	Nhóm
- Kiểm tra giữa kỳ	20%	Cá nhân
- Kiểm tra cuối kỳ	50%	Cá nhân

9.2. Nội dung và Tiêu chí đánh giá các loại bài tập

Các loại bài tập lớn/thảo luận	Tiêu chí đánh giá
- Bài tập lớn/Tiểu luận	- Yêu cầu sinh viên nắm vững và trình bày được kiến thức căn bản của môn học

	- Tìm tài liệu, tổng hợp kiến thức và viết báo cáo theo yêu cầu của bài tập lớn được giao cho nhóm - Phân chia công việc và cộng tác theo nhóm - Chuẩn bị slides và trình bày trước lớp
- Thảo luận	- Tìm hiểu theo yêu cầu của nội dung thảo luận và trả lời câu hỏi trực tiếp
- Kiểm tra giữa kỳ, cuối kỳ	- Nắm vững kiến thức môn học - Trả lời đúng các câu hỏi và bài tập

Duyệt	**Chủ nhiệm bộ môn**	**Giảng viên** *(Chủ trì biên soạn đề cương)*
	Nguyễn Ngọc Điệp	**Nguyễn Ngọc Điệp**