BM01.QT02/ĐNT-ĐT

TRƯỜNG ĐH NGOẠI NGỮ - TIN HỌC TP.HCM
KHOA CÔNG NGHỆ THÔNG TIN

CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM
Độc lập – Tự do – Hạnh Phúc

ĐỀ CƯƠNG CHI TIẾT HỌC PHẦN

1. Thông tin chung về học phần

- **Tên học phần :** An ninh mạng (Network Security)
- **Mã số học phần :** 4030244
- **Số tín chỉ học phần :** 4 (3+1) tín chỉ
- Thuộc chương trình đào tạo của bậc, ngành: Bậc cao đẳng, ngành Công nghệ thông tin
- **Số tiết học phần :**
  - Nghe giảng lý thuyết : 45 tiết
  - Làm bài tập trên lớp : 0 tiết
  - Thảo luận : 0 tiết
  - Thực hành : 30 tiết
  - Hoạt động theo nhóm : 0 tiết
  - Thực tế: : 0 tiết
  - Tự học : 120 giờ
- **Đơn vị phụ trách học phần:** Bộ môn Mạng máy tính / Khoa Công nghệ thông tin

2. Học phần trước:

- Mạng Máy Tính

3. Mục tiêu của học phần:

3.1 Tìm hiểu kiến thức về tấn công, các phương pháp tấn công.

3.2 Hiểu được lỗ hổng của hệ thống trên nền tảng Microsoft Windows, Linux

3.3 Hiểu được các kỹ thuật tấn công trên mạng nội bộ

3.4 Hiểu được các kỹ thuật tấn công trên website và webserver

3.5 Hiểu được các kỹ thuật tấn công về yếu tố con người

3.6 Hiểu được các kỹ thuật Virus

3.7 Hiểu được các kỹ thuật Tường lửa, IDS

3.8 Giải pháp phòng chống

4. Chuẩn đầu ra:

	Nội dung	Đáp ứng CĐR CTĐT
Kiến thức	4.1.1. Nhận biết được các điểm yếu cơ bản của hệ thống mạng.	**K1**
	4.1.2. Trình bày được các phương pháp mã hóa dữ liệu và ngăn chặn xâm nhập	**K2, K3**
Kỹ năng	4.2.1 Dùng công cụ dò tìm phát hiện các điểm yếu hệ thống mạng	**S1**
	4.2.2 Thu thập thông tin chiếm quyền và quét cổng	**S2, S3**
	4.2.3 Xây dựng giải pháp an toàn hệ thống mạng	**S2, S3**
Thái độ	4.3.1. Ý thức được tầm quan trọng của an toàn mạng thông tin và bảo mật hệ thống mạng cho doanh nghiệp	**A1**
	4.3.2. Chuẩn bị bài trước khi đến lớp. Đi học đầy đủ. Tham gia tích cực trong giờ học.	**A2, A3**

5. Mô tả tóm tắt nội dung học phần:

Học phần cung cấp khả năng tổng quan về an ninh mạng. Các kiến thức về tấn công, khai thác lỗ hổng và bảo mật trên từng loại tấn công đó. Kiến thức của chương trình sẽ bao gồm thu thập thông tin, quét lỗi, tấn công và sửa lỗi trên các mãng về mạng nội bộ, internet, website, virus, hệ điều hành, dữ liệu, thông tin cá nhân,…

6. Nội dung và lịch trình giảng dạy:

- Các học phần lý thuyết:

Buổi/ Tiết	Nội dung	Hoạt động của giảng viên	Hoạt động của sinh viên	Giáo trình chính	Tài liệu tham khảo	Ghi chú
1/ (3)	**Chương 1: Khai thác thông tin** 1. Tìm kiếm thông tin và quét lỗi hệ thống 2. Giả mạo thông tin hệ thống 3. Quản lý thông tin trên hosting và Domain 4. Quản lý thông tin trong LAN 5. Hạn chế khai thác thông tin hệ thống	- Giới thiệu đề cương chi tiết - Thuyết giảng ngắn - Đặt câu hỏi - Nhấn mạnh những điểm chính	- Nghe giảng, ghi chú - Trả lời câu hỏi	Chương 2,3 Cuốn 1	Chương 2,3 Cuốn 3	Giải quyết mục tiêu 4.1.1
2-3/ (6)	**Chương 2: An Toàn trong LAN** 1. Phương thức truy cập và chứng thực trong LAN: LM, NTML 2. Các loại tấn công trong LAN 3. Crack password 4. Tấn công Remote Access 5. Đánh cắp tài nguyên: document, file, thư mục 6. Đánh cắp thông tin dùng Keylogger 7. Phân quyền thư mục 8. Ngăn chặn NetBIOS 9. Ngăn chặn Trojan và backdoor, Keylogger	- Thuyết giảng ngắn - Đặt câu hỏi - Cho bài tập - Nhấn mạnh những điểm chính - Yêu cầu chuẩn bị buổi học sau	- Nghe giảng, ghi chú - Trả lời câu hỏi - Làm bài tập	Chương 4,5 Cuốn 1	Chương 6,7,8 Cuốn 3	Giải quyết mục tiêu 4.1.1 4.2.1 4.3
4-5 / (6)	**Chương 3: An Toàn tài khoản truy cập** 1. Certificate 2. Tấn công account email: yahoo,	- Cho bài Quiz - Đặt vấn đề - Thuyết giảng ngắn	- Làm bài Quiz - Nghe giảng, ghi chú - Trả lời câu hỏi	Chương 6,7 Cuốn 1	Cuốn 3	Giải quyết mục tiêu 4.1.1

	gmail, smtp, ftp 3. Nghe lén nội dung thông tin trên đường truyền 4. Phòng chống giả mạo ARP	- Đặt câu hỏi - Cho bài tập - Nhấn mạnh những điểm chính - Yêu cầu chuẩn bị buổi học sau	- Làm bài tập			4.2.1 4.3
6-7/ (6)	Chương 4: Tấn công từ chối dịch vụ (DoS) 1. Các loại tấn công từ chối dịch vụ Dos, DDos 2. Các công nghệ hiện tại 3. Các phương pháp hạn chế	- Cho bài Quiz - Đặt vấn đề - Thuyết giảng ngắn - Đặt câu hỏi - Cho bài tập - Nhấn mạnh những điểm chính - Yêu cầu chuẩn bị buổi học sau	- Làm bài Quiz - Nghe giảng, ghi chú - Trả lời câu hỏi - Làm bài tập	Chương 8 Cuôn 1	Chương 12 cuốn 3	Giải quyết mục tiêu 4.1.1 4.2.1 4.3
8 /(3)	**Chương 5: Yếu tố con người** 1.Yếu tố con người và vai trò trong hệ thống 2.Một số trường lừa đảo Online 3.Giả mạo email, điện thoại 4.Lừa đảo qua yếu tố con người 5.An toàn thông tin cá nhân trong mạng xã hội 6.Các phương pháp phòng chống	- Cho bài Quiz - Đặt vấn đề - Thuyết giảng ngắn - Đặt câu hỏi - Cho bài tập - Nhấn mạnh những điểm chính - Yêu cầu chuẩn bị buổi học sau	- Làm bài Quiz - Nghe giảng, ghi chú - Trả lời câu hỏi - Làm bài tập	Chương 9 Cuốn 1		Giải quyết mục tiêu 4.1.1 4.2.1 4.3
9-10 /(6)	**Chương 6: An toàn cho Website và Webserver** 1. Website: o Unicode o Bypass o LFI, RFI o Sql injection	- Cho bài Quiz - Đặt vấn đề - Thuyết giảng ngắn - Đặt câu hỏi - Cho bài tập - Nhấn mạnh những điểm chính	- Làm bài Quiz - Nghe giảng, ghi chú - Trả lời câu hỏi - Làm bài tập	Chương 11,12,13,14 Cuốn 1	Chương 12, 14, 15 Cuốn 2, Chương 18 Cuốn 3, Chương 4 Cuốn 4	Giải quyết mục tiêu 4.1.1 4.2.1 4.3

	o Web application 2.Web server: o Reverse o Local attack trên server IIS và Apache o Web backdoor 3.Google Hack 4.Crack Password 5.Lọc dữ liệu đầu vào 6.Tùy biến web application và database theo công nghệ 7.Config Server phòng chống tấn công local attack 8.Các công cụ mà hacker thường sử dụng 9.Lập trình web an toàn	- Yêu cầu chuẩn bị buổi học sau				
11/(3)	**Chương 7: Wireless** 1.Phân loại Wireless 2.Bắt gói, phân tích 3.Crack wep, wpa…key 4.Triển khai mã hóa cao cấp cho key 5.Radius	- Cho bài Quiz - Đặt vấn đề - Thuyết giảng ngắn - Đặt câu hỏi - Cho bài tập - Nhấn mạnh những điểm chính - Yêu cầu chuẩn bị buổi học sau	- Làm bài Quiz - Nghe giảng, ghi chú - Trả lời câu hỏi - Làm bài tập	Chương 15 cuốn 1		Giải quyết mục tiêu 4.1.1 4.2.1 4.3
12/(3)	**Chương 8: Virus** 1. Nguyên lý hoạt động của Virus 2. Lịch sử Virus 3. Công nghệ nhận dạng 4. Tự xuất bản virus bằng các ngôn	- Cho bài Quiz - Đặt vấn đề - Thuyết giảng ngắn - Đặt câu hỏi - Cho bài tập - Nhấn mạnh những	- Làm bài Quiz - Nghe giảng, ghi chú - Trả lời câu hỏi - Làm bài tập	Chương 16 cuốn 1		Giải quyết mục tiêu 4.1.1 4.2.1 4.3

	ngữ lập trình: Autoit, VB, assembly… 5. Phân tích virus và phòng chống reverse	điểm chính - Yêu cầu chuẩn bị buổi học sau				
13/(3)	**Chương 9: IDS** 1. Phân tích log 2. Các loại IDS 3. Cấu hình hệ thống IDS bằng Snort 4. Cấu hình hệ thống IDS bằng BlackIce	- Cho bài Quiz - Đặt vấn đề - Thuyết giảng ngắn - Đặt câu hỏi - Cho bài tập - Nhấn mạnh những điểm chính - Yêu cầu chuẩn bị buổi học sau	- Làm bài Quiz - Nghe giảng, ghi chú - Trả lời câu hỏi - Làm bài tập	Chương 18 cuốn 1	Chương 16 cuốn 3	Giải quyết mục tiêu 4.1.1 4.2.1 4.3
14/(3)	**Chương 10: Thiết kế hệ thống bảo mật theo tiêu chuẩn ISO** 1. Tiêu chuẩn ISO 27001, 27002 2. Security checklist	- Cho bài Quiz - Đặt vấn đề - Thuyết giảng ngắn - Đặt câu hỏi - Cho bài tập - Nhấn mạnh những điểm chính - Yêu cầu chuẩn bị buổi học sau	- Làm bài Quiz - Nghe giảng, ghi chú - Trả lời câu hỏi - Làm bài tập	Chương 6 cuốn 3		Giải quyết mục tiêu 4.1.1 4.2.1 4.3
15/(3)	**Ôn tập**	-	-			

Ghi chú: 1 buổi: 3 tiết

- Các học phần thực hành:

Buổi/ Tiết	Nội dung	Hoạt động của giảng viên	Hoạt động của sinh viên	Giáo trình chính	Tài liệu tham khảo	Ghi chú
1/(3)	Bài 1. Khai thác thông tin hệ thống	- Review điểm chính - Hướng dẫn sinh viên thực hiện - Trả lời câu hỏi của SV	- Nghe giảng, ghi chú - Đặt câu hỏi - Làm bài tập	Bài tập thực hành	Chương 2,3 Cuốn 3	Giải quyết mục tiêu 4.2, 4.3
2/(3)	Bài 2. Tấn công và ngăn chặn	- Review điểm chính - Hướng dẫn sinh viên thực hiện - Trả lời câu hỏi của SV	- Nghe giảng, ghi chú - Đặt câu hỏi - Làm bài tập	Bài tập thực hành	Chương 6,7,8 Cuốn 3	Giải quyết mục tiêu 4.2, 4.3
3/(3)	Bài 3. Đánh cắp tài khoản và nghe lén đường truyền	- Review điểm chính - Hướng dẫn sinh viên thực hiện - Trả lời câu hỏi của SV	- Nghe giảng, ghi chú - Đặt câu hỏi - Làm bài tập	Bài tập thực hành	Cuốn 3	Giải quyết mục tiêu 4.2, 4.3
4/(3)	Bài 4. Thực hiện tấn công DDoS	- Review điểm chính - Hướng dẫn sinh viên thực hiện - Trả lời câu hỏi của SV	- Nghe giảng, ghi chú - Đặt câu hỏi - Làm bài tập	Bài tập thực hành	Chương 12 cuốn 3	Giải quyết mục tiêu 4.2, 4.3
5/(3)	Bài 5. Các phương pháp phòng chống	- Review điểm chính - Hướng dẫn sinh viên thực hiện - Trả lời câu hỏi của SV	- Nghe giảng, ghi chú - Đặt câu hỏi - Làm bài tập	Bài tập thực hành		Giải quyết mục tiêu 4.2, 4.3
6/(3)	Bài 6. Thực hiện an toàn Website	- Review điểm chính - Hướng dẫn sinh viên thực hiện - Trả lời câu hỏi của SV	- Nghe giảng, ghi chú - Đặt câu hỏi - Làm bài tập	Bài tập thực hành	Chương 12, 14, 15 Cuốn 2, Chương 18 Cuốn 3, Chương 4 Cuốn 4	Giải quyết mục tiêu 4.2, 4.3

7/(3)	Bài 7. Chứng thực Wireless	- Review điểm chính - Hướng dẫn sinh viên thực hiện - Trả lời câu hỏi của SV	- Nghe giảng, ghi chú - Đặt câu hỏi - Làm bài tập	Bài tập thực hành		Giải quyết mục tiêu 4.2, 4.3
8/(3)	Bài 8. Phân tích mã độc và cách phòng chống	- Review điểm chính - Hướng dẫn sinh viên thực hiện - Trả lời câu hỏi của SV	- Nghe giảng, ghi chú - Đặt câu hỏi - Làm bài tập	Bài tập thực hành		Giải quyết mục tiêu 4.2, 4.3
9/(3)	Bài 9. Ngăn chặn xâm nhập và kiểm tra bảo mật	- Review điểm chính - Hướng dẫn sinh viên thực hiện - Trả lời câu hỏi của SV	- Nghe giảng, ghi chú - Đặt câu hỏi - Làm bài tập	Bài tập thực hành	Chương 16 cuốn 3	Giải quyết mục tiêu 4.2, 4.3
10/(3)	Thi	Coi thi và chấm điểm	Làm bài thi			

7. Nhiệm vụ của sinh viên:

Sinh viên phải thực hiện các nhiệm vụ như sau:

- Tham dự tối thiểu 80% số tiết học lý thuyết.
- Tham dự tối thiểu 50% giờ thực hành và giải tất cả bài tập.
- Tham dự kiểm tra thực hành.
- Tham dự thi kết thúc học phần.
- Chủ động tổ chức thực hiện giờ tự học.

8. Đánh giá kết quả học tập của sinh viên:

8.1. Cách đánh giá

Sinh viên được đánh giá tích lũy học phần như sau:

TT	Thành phần	Điểm thành phần	Quy định	Trọng số điểm	Trọng số thành phần	Mục tiêu
1	Thực hành	Điểm chuyên cần	- Tham dự ít nhất 70% số tiết học và số bài tập được giao	30%	30%	4.3.2
		Điểm thi thực hành	- Thực hành trên máy	70%		4.2
2	Lý thuyết	Điểm thi kết thúc học phần	- Thi viết (60 phút)		70%	4.1 4.2.1

8.2. Cách tính điểm

- Điểm đánh giá thành phần và điểm thi kết thúc học phần được chấm theo thang điểm 10 (từ 0 đến 10), làm tròn đến 0.5.
- Điểm học phần là tổng điểm của tất cả các điểm đánh giá thành phần của học phần nhân với trọng số tương ứng. Điểm học phần theo thang điểm 10 làm tròn đến một chữ số thập phân.

9. Tài liệu học tập:

9.1. Giáo trình/Tài liệu chính:

[1]. Ethical Hacking and Countermeasures : Attack Phases, EC-Council, Cengage, 2017

9.2. Tài liệu tham khảo:

[2]. Web Hacking: Attacks and Defense, Stuart McClure, Saumil Shah, Shreeraj Shah, Addison-Wesley Professional, 2003

[3]. Hacking Exposed 7: Network Security Secrets and Solutions, Stuart McClure, Joel Scambray, George Kurtz, McGraw-Hill Education, 2012.

10. Hướng dẫn sinh viên tự học:

Tuần/ Buổi	Nội dung	Lý thuyết (tiết)	Nhiệm vụ của sinh viên
1/1	**Chương 1:** Khai thác thông tin	3	-Nghiên cứu trước: Slide bài giảng: Chương 1
1/1	**Chương 2:** An Toàn trong LAN	3	-Nghiên cứu trước: Slide bài giảng: Chương 2
1/1	**Chương 3:** An Toàn tài khoản truy cập	3	-Nghiên cứu trước: Slide bài giảng: Chương 3
1/1	**Chương 4:** Tấn công từ chối dịch vụ (DoS)	3	-Nghiên cứu trước: Slide bài giảng: Chương 4
1/1	**Chương 5:** Yếu tố con người	3	-Nghiên cứu trước: Slide bài giảng: Chương 5
1/1	**Chương 6:** An toàn cho Website và Webserver	3	-Nghiên cứu trước: Slide bài giảng: Chương 6
1/1	**Chương 7:** Wireless	3	-Nghiên cứu trước: Slide bài giảng: Chương 7
1/1	**Chương 8:** Virus	3	-Nghiên cứu trước: Slide bài giảng: Chương 8
1/1	**Chương 9:** IDS	3	-Nghiên cứu trước: Slide bài giảng: Chương 9
1/1	**Chương 10:** Thiết kế hệ thống bảo mật theo tiêu chuẩn ISO Ôn tập	3	-Nghiên cứu trước: Slide bài giảng: Chương 10

Thực hành:

Sinh viên làm trước các bài tập có hướng dẫn trong tài liệu thực hành ở nhà theo bảng lịch trình giảng dạy phía trên, tham khảo thêm tài liệu [1] các nội dung tương ứng để có thể làm bài tốt hơn.

Ngày… tháng…. Năm 2017	*Ngày… tháng…. Năm 2017*	*Ngày… tháng…. Năm 2017*
Trưởng khoa	**Trưởng Bộ môn**	**Người biên soạn**
(Ký và ghi rõ họ tên)	***(Ký và ghi rõ họ tên)***	***(Ký và ghi rõ họ tên)***
	Phạm Đình Thắng	**Phạm Đình Thắng**

Ngày… tháng…. Năm 2017
Ban giám hiệu