IT4263 AN NINH MẠNG

Phiên bản:

1. THÔNG TIN CHUNG

Tên học phần: An ninh mạng
(Computer Network Security)

Mã số học phần: IT4263

Khối lượng: 3(2-0-2-6)
- Lý thuyết: 30 tiết
- Bài tập/BTL: 0 tiết
- Thí nghiệm: 30 tiết

Học phần tiên quyết: -

Học phần học trước:
- IT1110: Tin học đại cương
- IT4015: Nhập môn An toàn thông tin

Học phần song hành: Không

2. MÔ TẢ HỌC PHẦN

Học phần này cung cấp các kiến thức về an toàn an ninh thông tin trên môi trường mạng; mô hình an toàn an ninh mạng, ứng dụng các hệ mật mã trong các giao thức mạng như WPA/WPA2, IPSec, SSL/ TLS, SSH; các giao thức xác thực người dùng như CHAP, EAP. Bên cạnh đó, học phần cũng bao gồm nội dung phân tích lỗ hổng và các nguy cơ bảo mật trên bộ giao thức TCP/IP; các nguy cơ an toàn bảo mật đối với mạng LAN và WLAN, lỗ hổng và các nguy cơ của các dịch vụ mạng như Web, thư điện tử (email), phân giải tên miền (DNS).

Học phần cũng cung cấp cho sinh viên các kỹ năng phân tích, nhận diện các hành vi tấn công trong mạng, quét và rà roát lỗ hổng an toàn bảo mật trên các dịch vụ mạng.

3. MỤC TIÊU VÀ CHUẨN ĐẦU RA CỦA HỌC PHẦN

Sinh viên hoàn thành học phần này có khả năng:

Mục tiêu/CĐR	Mô tả mục tiêu/Chuẩn đầu ra của học phần	CĐR được phân bổ cho HP/ Mức độ (I/T/U)
[1]	[2]	[3]
M1	**Xác định các mối đe dọa tấn công an toàn bảo mật trong mạng máy tính và cách thức nhận biết, phòng tránh**	1.2.4, 1.2.5, 1.3.6, 1.4.2, 2.1.1, 2.1.3, 2.2.1, 2.2.3, 3.1 1.4.4, 4.1.1, 4.1.2
M1.1	Trình bày được các mục tiêu và các mối đe dọa an toàn bảo mật trong mạng máy tính	[1.2.4, 1.2.5] (U) [1.3.6, 1.4.2] (T) [4.1.1, 4.1.2](I)
M1.2	Giải thích được về các lỗ hổng trong chồng giao thức TCP/IP và kỹ thuật tấn công khai thác.	[1.2.4, 1.2.5] (U) [1.3.6, 1.4.2] (T) [2.1.1, 2.1.3] (T)
M1.3	Sử dụng công cụ để phân tích và nhận biết đặc điểm của các hành vi tấn công trong mạng	[1.2.4, 1.2.5, 2.5.1, 3.1] (U)

		[1.3.6, 1.4.2] (T) [2.2.1, 2.2.3] (T)
M1.4	Biết đến các giải pháp phòng chống và giảm thiểu tấn công vào mạng TCP/IP	[1.4.4] (I)
M2	**Hiểu biết về các kỹ thuật tấn công vào dịch vụ Web**	1.2.2, 1.2.6, 1.3.6, 1.4.2, 1.4.4, 2.2.1, 2.2.3, 3.1
M2.1	Giải thích được các lỗ hổng an toàn bảo mật của ứng dụng Web và các kỹ thuật tấn công khai thác	[1.2.2, 1.2.6] (U) [1.3.6, 1.4.2, 1.4.4](T)
M2.2	Phát hiện được các lỗ hổng an toàn bảo mật trên ứng dụng Web	[2.5.1, 3.1] (U) [1.3.6, 1.4.2] (T) [2.2.1, 2.2.3] (T)
M2.3	Biết đến các giải pháp phòng chống và giảm thiểu tấn công vào ứng dụng Web	[1.3.6, 1.4.2, 1.4.4] (T) [1.2.6] (U)
M3	**Hiểu biết về các phương thức bảo vệ quá trình truyền tin trong mạng**	1.2.6, 1.3.6, 1.3.7, 1.4.1, 1.4.2,
M3.1	Trình bày được hoạt động của các giao thức an toàn bảo mật trong mạng TCP/IP	[1.2.6, 1.4.1] (U) [1.3.6, 1.4.2] (T) [1.3.7] (I)
M3.2	Ứng dụng các cơ chế mật mã để bảo vệ dữ liệu trong mạng	[1.2.6, 1.4.1] (U) [1.3.6, 1.4.2] (T) [1.3.7] (I)

4. TÀI LIỆU HỌC TẬP

Giáo trình

[1] Nguyễn Khanh Văn(2014). *Giáo trình Cơ sở an toàn thông tin*. NXB Bách khoa - Hà Nội.

[2]

Sách tham khảo

[1] Michael Goodrich, Roberto Tamassia (2010). *Introduction to Computer Security, 1st Edition*. Pearson.

[2]

[3]

5. CÁCH ĐÁNH GIÁ HỌC PHẦN

Điểm thành phần	Phương pháp đánh giá	Mô tả	CĐR được	Tỷ

	cụ thể		đánh giá	trọng
[1]	[2]	[3]	[4]	[5]
A1. Điểm quá trình (*)	**Đánh giá quá trình**			**40%**
	A1.1. Thực hành	Báo cáo thực hành	M1.2, M1.3, M2.1, M2.2	40%
A2. Điểm cuối kỳ	A2.1. Thi cuối kỳ	Thi viết	M1.2, M1.2, M1.3, M2.1, M2.2, M2.3, M3.1, M3.2	**60%**

** Điểm quá trình sẽ được điều chỉnh bằng cách cộng thêm điểm chuyên cần. Điểm chuyên cần có giá trị từ –2 đến +1, theo Quy chế Đào tạo đại học hệ chính quy của Trường ĐH Bách khoa Hà Nội.*

6. KẾ HOẠCH GIẢNG DẠY

Tuần	Nội dung	CĐR học phần	Hoạt động dạy và học	Bài đánh giá
[1]	[2]	[3]	[4]	[5]
1	**Bài 1. Tổng quan về an toàn thông tin trên hệ thống mạng** 1. Khái niệm chung về an toàn bảo mật thông tin 2. Chính sách và các cơ chế an toàn bảo mật 3. Lỗ hổng và nguy cơ an toàn bảo mật 4. Xây dựng hệ thống an toàn bảo mật cho mạng máy tính	M1.1	Giảng bài	A2.1
2	**Bài 2. An toàn bảo mật quá trình truyền tin** 1. Các yêu cầu an toàn bảo mật cho quá trình truyền tin 2. Bảo mật truyền tin với các hệ mật mã 2.1. Hệ mật mã khóa đối xứng 2.2. Hệ mật mã khóa công khai 3. Xác thực thông điệp 2.1. Mã xác thực thông điệp 2.2. Hàm băm và chữ ký số 4. Giao thức phân phối khóa 4.1. Các giao thức phân phối khóa đối xứng 4.2. Các giao thức phân phối khóa công khai	M3.2	Đọc trước tài liệu; Giảng bài	A2.1
3	**Bài 3. Tổng quan về mạng máy tính** 1. Các khái niệm cơ bản	M1.1	Đọc trước tài liệu;	A2.1

	2. Kiến trúc phân tầng 3. Chuyển tiếp dữ liệu trong mạng 4. Hoạt động của ứng dụng mạng 5. Một số hoạt động quan trọng trong mạng		Giảng bài;	
4	**Bài 4. An toàn an ninh trên hạ tầng mạng** 1. An toàn bảo mật tầng vật lý và tầng liên kết dữ liệu 1.1. Các nguy cơ an toàn bảo mật tầng vật lý 1.2. An toàn bảo mật mạng WLAN 1.3. An toàn bảo mật trong mạng cục bộ	M1.2, M1.4	Đọc trước tài liệu; Giảng bài;	A2.1
5	2. An toàn bảo mật tầng mạng 2.1. Các nguy cơ an toàn bảo mật của giao thức IP 2.2. Các nguy cơ an toàn bảo mật trong quá trình định tuyến *Bài thực hành số 1: Phân tích các kỹ thuật do thám hệ thống mạng*	M1.2, M1.3, M1.4	Đọc trước tài liệu; Giảng bài; Thực hành trên phòng thí nghiệm	A1.1 A2.1
6	**Bài 5. An toàn an ninh cho ứng dụng mạng** 1. An toàn an ninh trên tầng giao vận 2. An toàn bảo mật tầng ứng dụng 2.1. An toàn bảo mật dịch vụ phân giải tên miền 2.2. An toàn bảo mật dịch vụ thư điện tử	M1.2, M1.4	Đọc trước tài liệu; Giảng bài	A2.1
7	**Bài 6. Tấn công từ chối dịch vụ - DoS** 1. Khái niệm chung về DoS 2. Một số kỹ thuật tấn công DoS 2.1. Tấn công DoS L3/4 *Bài thực hành số 2: Phân tích một số kỹ thuật tấn công trong mạng LAN*	M1.2, M1.3, M1.4	Đọc trước tài liệu; Giảng bài; Thực hành trên phòng thí nghiệm	A1.1 A2.1
8	2.2. Tấn công DoS L7 3. Phòng chống và giảm thiểu tấn công DoS	M1.2, M1.4	Đọc trước tài liệu; Giảng bài;	A2.1
9	**Bài 7. An toàn dịch vụ Web – Tổng quan** 1. Tổng quan về dịch vụ Web 2. Chính sách SOP 2. Giao thức HTTPS 2.1. Giới thiệu chung về HTTPS 2.2. Các nguy cơ an toàn bảo mật của HTTPS *Bài thực hành số 3: Phân tích một số kỹ*	M1.3, M2.1, M2.3	Đọc trước tài liệu; Giảng bài; Thực hành trên phòng thí nghiệm	A1.1 A2.1

	thuật tấn công giao thức DNS			
10	**Bài 8. An toàn dịch vụ Web – Tấn công Sqli và XSS** 1. Tấn công Command Injection 2. Tấn công SQL Injection *Bài thực hành số 4: Phân tích một số kỹ thuật tấn công DoS*	M1.3, M2.1, M2.3	Đọc trước tài liệu; Giảng bài; Thực hành trên phòng thí nghiệm	A1.1 A2.1
11	3. Tấn công XSS	M2.1, M2.3	Đọc trước tài liệu; Giảng bài;	A2.1
12	**Bài 9. An toàn dịch vụ Web – Quản lý phiên** 1. Quản lý phiên dịch vụ Web 2. Ứng dụng của cookie và các mối đe dọa 3. Tấn công CSRF *Bài thực hành số 5: Kiểm thử lỗ hổng SQL Injection trên dịch vụ Web*	M2.1, M2.2, M2.3	Đọc trước tài liệu; Giảng bài; Thực hành trên phòng thí nghiệm	A1.1 A2.1
13	**Bài 10. An toàn dịch vụ Web – Một số dạng tấn công khác** 1. Tấn công Clickjacking 2. Một số dạng tấn công khác	M2.1, M2.3	Đọc trước tài liệu; Giảng bài	A2.1
14	**Bài 11. Một số giao thức bảo mật trong TCP/IP** 1. IPSec 2. Giao thức SSL/TLS 3. Giao thức SSH 4. Các giao thức bảo mật của WLAN *Bài thực hành số 6: Kiểm thử lỗ hổng XSS và CSRF trên dịch vụ Web*	M2.2, M3.1, M3.2	Đọc trước tài liệu; Giảng bài; Thực hành trên phòng thí nghiệm	A1.1 A2.1
15	**Bài 12. Các hệ thống phòng chống và ngăn chặn tấn công** 1. Hệ thống tường lửa 2. Hệ thống phát hiện và ngăn chặn tấn công	M1.4	Đọc trước tài liệu; Giảng bài	A2.1

7. QUY ĐỊNH CỦA HỌC PHẦN

(Các quy định của học phần nếu có)

8. NGÀY PHÊ DUYỆT: ……..

Chủ tịch Hội đồng **Nhóm xây dựng đề cương**

9. QUÁ TRÌNH CẬP NHẬT

Lần cập nhật	Nội dung điều chỉnh	Ngày tháng được phê duyệt	Áp dụng từ kỳ/khóa	Ghi chú
1	Sắp xếp lại nội dung bài giảng Đề xuất thêm giáo trình			
2	……			