IT4831 PHÒNG CHỐNG TẤN CÔNG MẠNG

Phiên bản:

1. THÔNG TIN CHUNG

Tên học phần: Phòng chống tấn công mạng
(Computer Network Defense)

Mã số học phần: IT4831

Khối lượng: 2(2-0-1-4)
- Lý thuyết: 30 tiết
- Bài tập/BTL: 0 tiết
- Thí nghiệm: 15 tiết

Học phần tiên quyết: -

Học phần học trước: - IT4263: An ninh mạng

Học phần song hành: Không

2. MÔ TẢ HỌC PHẦN

Học phần này giới thiệu cho sinh viên các kiến thức cơ bản về các mô hình tấn công và phòng chống tấn công trên mạng máy tính. Học phần cung cấp các kiến thức về các giải pháp công nghệ trong các hệ thống phòng chống tấn công như mạng riêng ảo (VPN), hệ thống hạ tầng khóa công khai (PKI) và các ứng dụng; hệ thống tường lửa (firewall); hệ thống phát hiện và đánh chặn tấn công (IDPS). Bên cạnh đó, học phần cũng giới thiệu các nội dung kiến thức về phát triển và triển khai các tác vụ vận hành an toàn bảo mật cho hệ thống công nghệ thông tin như thiết kế an toàn bảo mật cho hệ thống mạng, xây dựng và triển khai chính sách an toàn bảo mật, quy trình ứng phó sự cố an toàn bảo mật, gia cố hệ thống, sao lưu dự phòng hệ thống.

Học phần cung cấp cho sinh viên các kỹ năng triển khai và vận hành các sản phẩm giải pháp công nghệ phổ biến trong các hệ thống phòng chống tấn công mạng như VPN, tường lửa, hệ thống phát hiện xâm nhập IDS.

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	**Hiểu và có khả năng xây dựng giải pháp phòng chống các hành vi tấn công vào hệ thống mạng máy tính**	1.2.4; 1.2.5; 1.4.2; 1.4.4; 1.4.7; 2.1.1, 2.1.3, 2.1.4, 2.1.1, 2.1.3, 2.1.4, 2.3.1, 2.3.2, 3.3.3
M1.1	Hiểu và mô tả được các hệ thống phòng chống tấn công mạng, vai trò của chúng trong giải pháp chung	[1.2.4; 1.2.5] (U) [1.4.2](T, U) [1.4.4; 1.4.7] (I) [4.1.2](I) [3.3.3](U)

M1.2	Phân tích và lựa chọn được các hệ thống đáp ứng yêu cầu phòng chống tấn công mạng trong ngữ cảnh cụ thể	[1.2.4, 1.2.5](U) [1.4.2](T, U) [2.1.1, 2.1.3, 2.1.4](T, U)
M1.3	Thiết kế và tích hợp các hệ thống phòng chống tấn công mạng	[1.2.4, 1.2.5] (U) [1.4.2](T, U) [2.1.4, 2.3.1, 2.3.2](T, U)
M2	**Hiểu và có khả năng xây dựng các tác vụ cần thiết để vận hành hệ thống mạng một cách an toàn bảo mật**	1.2.4, 1.2.5; 1.4.5
M2.1	Hiểu và trình bày được nội dung công việc cần thực hiện trong các tác vụ an toàn bảo mật mạng	[1.2.4, 1.2.5] (U) [1.4.5](I, T) [2.1.4, 2.3.1, 2.3.2](T, U) [4.1.2](I) [3.3.3](U)
M2.2	Lập kế hoạch triển khai các tác vụ	[1.2.4, 1.2.5] (U)
M3	**Có khả năng triển khai và vận hành các hệ thống phòng chống tấn công mạng**	1.2.4, 1.2.5, 1.4.2
M3.1	Phân tích và lựa chọn các thông số cài đặt, triển khai các hệ thống phòng chống tấn công mạng	[1.2.4, 1.2.5] (U) [1.4.2](T, U)
M3.2	Vận hành và lý giải được hoạt động của các hệ thống	[1.2.4, 1.2.5] (U) [1.4.2](T, U)

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.

Sách tham khảo

[1] William Stallings (2005). *Cryptography and Network Security Principles and Practices*. Prentice Hall.

[2] Randy Weaver, Dawn Weaver, Dean Farwood (2013), *Guide to Network Defense and Countermeasures*. Cengage Learning

5. CÁCH ĐÁNH GIÁ HỌC PHẦN

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

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. Mở đầu** 1. An toàn bảo mật và các nguy cơ an toàn bảo mật 2. Khái niệm chung về phòng chống tấn công mạng 3. Phòng thủ theo chiều sâu	M1.1, M1.3	Giảng bài	A2.1
2	**Bài 2. Mạng riêng ảo – VPN** 1. Giới thiệu chung về VPN 2. Các giao thức VPN 2.1. Các giao thức VPN tầng 2	M1.1, M1.2, M3.1, M3.2	Đọc trước tài liệu; Giảng bài	A2.1
3	2.2. IPSec VPN	M1.2, M3.1, M3.2	Đọc trước tài liệu; Giảng bài;	A2.1
4	2.3. SSL VPN 3. Triển khai VPN	M1.2, M1.3, M3.1, M3.2	Đọc trước tài liệu; Giảng bài;	A2.1
5	**Bài 3. Hệ thống tường lửa (firewall)** 1. Giới thiệu chung về tường lửa 2. Các công nghệ tường lửa	M1.1, M1.2, M3.1, M3.2	Đọc trước tài liệu; Giảng bài;	A2.1
6	3. Các kiến trúc triển khai *Bài thực hành số 1: Cấu hình và vận hành dịch vụ VPN*	M1.2, M1.3, M3.1, M3.2	Đọc trước tài liệu; Giảng bài; Thực hành trên phòng thí nghiệm	A2.1
7	4. Xây dựng tập luật cho tường lửa	M1.2 M3.1 M3.2	Đọc trước tài liệu; Giảng bài;	A1.1 A2.1
8	**Bài 4. Hệ thống phát hiện và ngăn chặn tấn công (IDPS)** 1. Giới thiệu chung về hệ thống IDPS 2. Cơ sở lý thuyết về phát hiện xâm nhập *Bài thực hành số 2: Cấu hình và vận hành hệ thống tường lửa*	M1.1, M1.2, M3.1, M3.2	Đọc trước tài liệu; Giảng bài Thực hành trên phòng thí nghiệm	A2.1
9	3. Các phương pháp phát hiện tấn công 3.1. Phát hiện dựa trên dấu hiệu	M1.2, M3.1, M3.2	Đọc trước tài liệu;	A2.1

	3.2. Phát hiện dựa trên bất thường 4. Các kiến trúc IDPS 4.1. Host-based IDPS		Giảng bài;	
10	4.2. Network-based IDPS 4.3. Kiến trúc lai	M1.2, M3.1, M3.2	Đọc trước tài liệu; Giảng bài;	A2.1
11	**Bài 5. Một số tác vụ trong công tác phòng chống tấn công mạng** 1. Gia cố hệ thống 1.1. Gia cố hạ tầng mạng 1.2. Gia cố hệ điều hành *Bài thực hành số 3: Cấu hình và vận hành hệ thống phát hiện xâm nhập*	M1.3, M2.1, M2.2	Đọc trước tài liệu; Giảng bài; Thực hành trên phòng thí nghiệm	A1.1 A2.1
12	1.3. Gia cố cơ sở dữ liệu 1.4. Gia cố máy chủ dịch vụ Web	M1.3, M2.1, M2.2	Đọc trước tài liệu; Giảng bài;	A1.1 A2.1
13	2. Sao lưu và khôi phục hệ thống 3. Quy trình ứng phó sự cố	M2.1, M2.2	Đọc trước tài liệu; Giảng bài;	A2.1
14	**Bài 6. Xây dựng chính sách an toàn bảo mật** 1. Tổng quan về chính sách an toàn bảo mật 1.1. Khái niệm cơ bản 1.2. Phân loại 2. Quy trình xây dựng chính sách an toàn bảo mật 3. Chính sách bảo mật thông tin trong hệ thống 4. Chính sách toàn vẹn thông tin trong hệ thống	M2.1, M2.2	Đọc trước tài liệu; Giảng bài;	A2.1
15	**Bài 7. Thiết kế an toàn bảo mật cho hệ thống mạng** 1. Tổng quan về quy trình thiết kế hệ thống mạng 2. Thiết kế an toàn bảo mật hệ thống mạng	M1.1, M1.2, M1.3	Đọc trước tài liệu; Giảng bài;	A2.1
16	***Tổng kết và ôn tập***			

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**