BỘ CÔNG THƯƠNG
TRƯỜNG ĐH CÔNG NGHIỆP QUẢNG NINH

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

CHƯƠNG TRÌNH CHI TIẾT HỌC PHẦN
TRÌNH ĐỘ ĐẠI HỌC
Ngành/Chuyên ngành đào tạo: Công nghệ thông tin/ Mạng máy tính

1. Tên học phần: An toàn mạng

2. Loại học phần: Lý thuyết, thực hành

3. Số tin chỉ: 03tín chỉ. Trong đó LT 02 tín chỉ, TH 01 tín chỉ

4. Bộ môn quản lý học phần: Mạng và Công nghệ phần mềm.

5. Điều kiện tiên quyết:

Môn học trước: Mạng máy tính và Truyền thông; Đảm bảo và An toàn thông tin.

6. Phân bổ thời gian

- Thời gian trên lớp: 60 tiết

Số tiết lý thuyết: 30 tiết
Số tiết thực hành: 27 tiết
Số tiết kiểm tra: 03 tiết

- Thời gian tự học: 90 tiết

7. Mục tiêu của học phần

7.1. Kiến thức

- Nắm được các nguyên tắc cơ bản và nâng cao trong vấn đề an toàn hệthống mạng máy tính cũng như các mô hình ATM. Nắm bắt được các thông tin, cáchthức triển khai và phát triển các giải pháp an ninh hạ tầng mạng máy tính trong thực tế;

- Hiểu rõ các lỗ hổng của hệ thống trên nền tảng Microsoft Windows; nắm rõ các vấn đề an toàn, các mối đe dọa, mã hóa dữ liệu cũng như bảo mật trên các máy chủ;

- Hiểu rõ một số đặc tính cơ bản của mã độc, đồng thời cung cấp một số phương pháp phòng chống mã độc căn bản để giúp người học có nhận thức và hành động đúng dắn trong việc ngăn chặn các loại mã độc đối với hệ thống máy tính, mạng máy tính;

- Hiểu rõ về tấn công mạng, các hình thức tấn côngcác kỹ thuật tấn công trên mạng LAN, WLAN, các mô hình cũng như các phương thức tấn công mạng, các ứng dụng Web hiện nay cũng như biết một số hệ thống mạng riêng ảo, các mô hình điều khiển truy cập mạng cũng như cấu trúc bảo mật cơ sở hạ tầng mạng máy chủ;

- Biết các bước bảo mật trang web toàn diện nhằm phát hiện những cuộc tấn công nhằm vào website của các doanh nghiệp để làm tê liệt hệ thống, đánh cắp dữ liệu khách hàng của doanh nghiệp.Nắm được định nghĩa lỗ hổng bảo mật website là gì có thể dẫn đến việc website bị hack;

- Hiểu cách thức hoạt động của Hacker sử dụng các công cụ dò quét để phát hiện một loạt các website có cấu hình bảo mật kém hoặc website trên các nền tảng phổ

biến như PHP, WordPress hay Joomla có các lỗ hổng đã được công bố nhưng chưa được chủ website xử lý.Biết việc bảo mật hệ thống máy chủ Server trước những sự tấn công của tin tặc muốn lấy cắp thông tin hay phá hoại hệ thống;

Nắm rõ giải pháp ngăn ngừa xâm nhập nhằm mục đích bảo vệ tài nguyên, dữ liệu và mạng. Hiểu rõ những mối đe dọa tấn công lưu lượng mạng bất hợp pháp;phát hiện các cuộc tấn công nhanh và chính xác, đưa ra các cảnh báo giúp người quản trị xác định các lỗ hổng bảo mật trong hệ thống mạng máy tính.

7.2. Kỹ năng

Sinh viên sẽ giải thích được các nguyên nhân dẫn đến việc tấncông mạng máy tính, phân loại được các lỗ hổng trong hệ thống mạng. Ápdụng được các kỹ thuật Firewall, NAT, VPN, IDS/IPS vào hệ thống mạng;

- Khả năng triển khai các giải pháp an ninh, một số ứng dụng trong thực tế trên thực tế.Triển khai các kỹ thuật bảo vệ hạ tầng mạng.Giải pháp kỹ thuật trong lập kế hoạch an ninh mạng;

- Phân loại một số lỗ hổng trên Web cũng như kỹ thuật giám sát các giao thứ http, https;

- Bảo mật hệ thống máy chủ Server ở trong vùng DMZ;

- Thiết lập firewall không cho các kết nối tới máy chủ web trên toàn bộ các cổng, ngoại trừ cổng 80 (http), cổng 443 (https) và các cổng dịch vục khác;

- Cài đặt các bẫy macro để xem các tấn công vào máy chủ;

- Quét server theo định kỳ với các công cụ như ISS hay map để tìm kiếm lỗ hổng;

Cài đặt và sử dụng các thiết bị ngăn chặn và phát hiện xâm nhập trái phép vào hệ thống mạng.

7.3. Thái độ

+ Có ý thức và tinh thần trách nhiệm, thái độ và đạo đức đúng đắn, ý thức kỷ luật và tác phong công nghiệp để đáp ứng yêu cầu thực tế mà công việc đòi hỏi;

+ Có phương pháp làm việc khoa học, khả năng làm việc độc lập, làm việc theo nhóm, khả năng tự nghiên cứu và nâng cao chất lượng học tập;

+ Có tinh thần trách nhiệm với bản thân và tập thể, tinh thần học hỏi, ý trí vươn lên để hoàn thiện bản thân để tiếp tục học tập ở các trình độ cao hơn.

8. Nội dung học phần

8.1. Mô tả vắn tắt

Học phần gồm 6 chương: Chương 1. Giúp sinh viên hiểu rõ về tổng quan về An toàn mạng; Chương 2. Giúp sinh viên biết rõ hơn về mã độc và cách phân tích mã độc; Trong Chương 3. Giới thiệu một số mô hình tấn công mạng; chương 4. Giới thiệu cho sinh viên hiểu về An toàn hạ tầng mạng; Chương 5. Giúp sinh viên nắm rõ về An toàn cho Web/Webserver; cuối cùng là Chương 6. Giúp sinh viên hiểu rõ hơn các phương pháp an toàn cho một hệ thống mạng hiện nay.

8.2. Nội dung chi tiết học phần

Tuần	NỘI DUNG	LT (tiết)	TH (tiết)	Tài liệu đọc trước	Nhiệm vụ của sinh viên
1	**Chương 1. Tổng quan về An toàn mạng máy tính** 1.1. Nguyên tắc cơ bản về ATM và Internet 1.2. Thông tin cơ bản về ATM, các mô hình ATM 1.3. Các vấn đề an toàn, các mối đe dọa và tấn công Mã hóa và cơ sở hạ tầng khóa công khai 1.4. Các mục tiêu an ninh mạng 1.5. Bảo mật trên các lớp khác nhau	2	2	Tài liệu [1] Chương 1 (Từ 1.1 đến 1.5)	- Chuẩn bị và đọc trước nội dung trong tài liệu [1]Chương 1 từ 1.6 – 1.8 - Thực hành theo nội dung trong tài liệu [2] tuần 1
2	1.6. Bảo mật 2 lớp và BGP 1.7. Hoạt động bảo mật trên các máy chủ 1.8. Điều khiển truy cập và xác thực	2	2	Tài liệu [1] Chương 1 (Từ 1.6 đến 1.8)	- Chuẩn bị và đọc trước nội dung trong tài liệu [1] Chương 2 từ 2.1 – 2.3 - Thực hành theo nội dung trong tài liệu [2] tuần 2
3	**Chương 2. Mã độc, phân tích mã độc** 2.1. Tổng quan mã độc 2.2. Các loại mã độc 2.3. Hiểm họa của mã độc đối với ATM	2	2	Tài liệu [1] Chương 2 (Từ 2.1 đến 2.3)	- Chuẩn bị và đọc trước nội dung trong tài liệu [1] Chương 2 từ 2.4 – 2.6 - Thực hành theo nội dung trong tài liệu [2] tuần 3
4	2.4. Nhận biết mã độc và cách phòng tránh 2.5. Phương pháp phân tích mã độc 2.6. Kỹ thuật PE&COFF file trong phân tích mã độc	2	2	Tài liệu [1] Chương 2 (Từ 2.4 đến 2.6)	- Chuẩn bị và đọc trước nội dung trong tài liệu [1] Chương 3 từ 3.1 – 3.3 - Thực hành theo nội dung trong tài liệu [2] tuần 4
5	**Chương 3. Tấn công xâm nhập hệ thống mạng** 3.1. Giới thiệu 3.2. Các phương thức Hacker tấn công mạng 3.3. Các mô hình tấn công mạng	2	1	Tài liệu [1] Chương 3 (Từ 3.1 đến 3.3)	- Chuẩn bị và đọc trước nội dung trong tài liệu [1] Chương 3 từ 3.4 – 3.5 - Thực hành theo nội dung

					trong tài liệu [2] tuần 5
	Kiểm tra bài số 1		**1**		
6	3.4. Những hình thức tấn công phổ biến 3.5. Một số kỹ thuật tấn công mạng	**2**	**2**	Tài liệu [1] Chương 3 (Từ 3.4 đến 3.5)	- Chuẩn bị và đọc trước nội dung trong tài liệu [1] Chương 3 từ 3.6 – 3.7 - Thực hành theo nội dung trong tài liệu [2] tuần 6
7	3.6. Một số công cụ tấn công mạng 3.7. Một số phương thức tấn công ứng dụng web	**2**	**2**	Tài liệu [1] Chương 3 (Từ 3.6 đến 3.7)	- Chuẩn bị và đọc trước nội dung trong tài liệu [1] Chương 4 từ 4.1 – 4.3.3 - Thực hành theo nội dung trong tài liệu [2] tuần 7
8	**Chương 4. An toàn hạ tầng mạng** 4.1. Phân tích các hiểm hoạ nguy cơ mất an toàn trong cơ sở hạ tầng mạng 4.2. Bảo mật truy cập các thiết bị mạng 4.3. Các mô hình điều khiển truy nhập 4.3.1. MAC 4.3.2. RBAC 4.3.3. DAC	**2**	**2**	Tài liệu [1] Chương 4 (Từ 4.1 đến 4.3.3)	- Chuẩn bị và đọc trước nội dung trong tài liệu [1] Chương 4 từ 4.4 – 4.5 - Thực hành theo nội dung trong tài liệu [2] tuần 8
9	4.4. Công nghệ mạng riêng ảo 4.5. Bảo mật máy chủ và cơ sở hạ tầng	**2**	**2**	Tài liệu [1] Chương 4 (Từ 4.4 đến 4.5)	- Chuẩn bị và đọc trước nội dung trong tài liệu [1] Chương 4 từ 4.6 – 4.7 - Thực hành theo nội dung trong tài liệu [2] tuần 9

10	4.6. Giám sát An toàn mạng 4.7. An toàn cho mạng WLAN	**2**	**1**	Tài liệu [1] Chương 4 (Từ 4.6 đến 4.7)	- Chuẩn bị và đọc trước nội dung trong tài liệu [1] Chương 5 từ 5.1 – 5.4 - Thực hành theo nội dung trong tài liệu [2] tuần 10
	Kiểm tra bài số 2		**1**		
11	**Chương 5. An toàn cho Web/Webserver** 5.1. Công nghệ Web 5.1.1. Cấu trúc 1 trang web 5.1.2. Ứng dụng web hoạt động như thế nào? 5.2. Bảo mật máy chủ Web 5.3. Bảo mật lưu lượng Web 5.4. An toàn cho IP, IPSec, SSL	**2**	**2**	Tài liệu [1] Chương 5 (Từ 5.1 đến 5.4)	- Chuẩn bị và đọc trước nội dung trong tài liệu [1] Chương 5 từ 5.5 – 5.7 - Thực hành theo nội dung trong tài liệu [2] tuần 11
12	5.5. Một số hình thức tấn công website: 5.5.1. Khai thác lỗ hổng của những phần mềm có trên web server. 5.5.2. Tấn công DDOS 5.5.3. Khai tác dữ liệu từ back-end 5.5.4. Thay đổi(deface) giao diện website. 5.5.5. Dùng web server đã bị tấn công để phát tán malware. 5.6. Phân loại các lỗ hổng bảo mật Website phổ biến hiện nay 5.6.1. Giám sát các giao thức http/s 5.6.2. Bảo vệ các ứng dụng và dữ liệu trước các loại tấn công trái phép. 5.6.3. Phân tích sâu các gói tin di chuyển trong các lưu lượng đi ra/ vào từ máy chủ dịch vụ Web. 5.7. Các bước bảo mật Web	**2**	**2**	Tài liệu [1] Chương 5 (Từ 5.5 đến 5.7)	- Chuẩn bị và đọc trước nội dung trong tài liệu [1] Chương 6 từ 6.1 – 6.4 - Thực hành theo nội dung trong tài liệu [2] tuần 12
13	**Chương 6. Phương pháp bảo vệ hệ thống mạng** 6.1. Mối đe dọa mạng máy tính doanh nghiệp 6.2. Các cơ chế chính bảo vệ hệ thống máy tính	**2**	**2**	Tài liệu [1] Chương 6 (Từ 6.1 đến 6.4)	- Chuẩn bị và đọc trước nội dung trong tài liệu [1] Chương 6 từ 6.5 – 6.8 - Thực hành

	6.3. Các phương pháp khai thác bảo vệ thông tin 6.4. Kiểm soát lưu lượng mạng				theo nội dung trong tài liệu [2] tuần 13
14	6.5. Các dịch vụ an toàn mạng 6.6. Công nghệ tường lửa, ASA 6.7. Các mô hình bảo vệ, phòng thủ, chống tấn công 6.8. Các kỹ thuật xâm nhập, kỹ thuật phát hiện xâm nhập	**2**	**2**	Tài liệu [1] Chương 6 (Từ 6.5 đến 6.8)	- Chuẩn bị và đọc trước nội dung trong tài liệu [1] Chương 6 từ 6.9 – 6.9.5 - Thực hành theo nội dung trong tài liệu [2] tuần 14
	Kiểm tra bài số 3		**1**		
15	6.9. Các công cụ bảo vệ hệ thống mạng 6.9.1. Giới thiệu công cụ Essential NetTools 6.9.2. Giới thiệu công cụ Microsoft Baseline Security Analyzer 6.9.3. Sử dụng công cụ Tenable NeWT Scanner 6.9.4. IDS/IPS 6.9.5. Open Source Filter lọc nội dung cho HTTP, FTP, SMTP	**2**	**1**	Tài liệu [1] Chương 6 (Từ 6.9 đến 6.9.5)	- Thực hành theo nội dung trong tài liệu [2] tuần 15
	Tổng cộng	**30**	**30**		

9. Nhiệm vụ của sinh viên

- Dự lớp: Tối thiểu 70% số giờ học trên lớp có sự hướng dẫn của giảng viên
- Bài tập, thực hành:

+ Làm bài tập đầy đủ

+ Đọc thêm tài liệu giảng viên yêu cầu

+ Đi thực hành trên máy tính đầy đủ

+ Thi kiểm tra giữa kỳ và thi kiểm tra kết thúc học phần

- Dụng cụ học tập: ổ lưu trữ USB
- Khác:

10. Thang điểm và hình thức đánh giá:

- **Thang điểm:** Thang điểm 10 (từ 0 - 10)
- **Hình thức đánh giá:**

- Sinh viên không tham gia đủ 70% số tiết học trên lớp không được dự thi kết thúc học phần và nhận điểm 0.

- Điểm thành phần để điểm lẻ đến một chữ số thập phân
- Điểm học phần làm tròn đến phần nguyên

11. Tiêu chuẩn đánh giá sinh viên

TT	Điểm thành phần	Quy định	Trọng số	Ghi chú
1	Điểm thường xuyên, đánh giá nhận thức, thái độ thảo luận, chuyên cần, làm bài tập ở nhà,…	- Số tiết dự học/tổng số tiết: 5% - Số bài tập đã làm/tổng số bài tập được giao và tham gia thảo luận trên lớp: 5%	10%	
2	Điểm kiểm tra giữa kỳ	- Hình thức KT: Thực hành trên máy tính. - Số bài kiểm tra: 03	30%	50 phút/bài
3	Thi kết thúc học phần	Hình thức thi hỗn hợp (Vấn đáp+ thực hành)	60%	60 phút

12. Tài liệu học tập

- Giáo trình bắt buộc

[1] Bài giảng An toàn mạng, Bộ môn Mạng & CNPM biên soạn và cập nhật

[2] Tài liệu thực hành, Bộ môn Mạng & CNPM biên soạn và cập nhật

- Tài liệu tham khảo

[1] William Stallings. Network Security Essentials: Applications and Standards, Third Edition. Prentice Hall, 2007.

13. Các yêu cầu khác (nếu có) của học phần:

Quảng Ninh,ngày 02 tháng 3 năm 2020

HIỆU TRƯỞNG	TRƯỞNG BỘ MÔN	GIẢNG VIÊN BIÊN SOẠN
TS. Hoàng Hùng Thắng	ThS. Đặng Đình Đức	ThS. Nguyễn Huy Hoàng