ĐỀ CƯƠNG CHI TIẾT

AN NINH MẠNG

(Networks Security)

Mã học phần: NETS33021 – Số tín chỉ: 03

Dùng cho (các) ngành: Công nghệ Thông tin

Điều kiện tiên quyết (nếu có): Mạng máy tính căn bản.

Hình thức đào tạo: Trực tiếp và trực tuyến

Đơn vị phụ trách: **Khoa Công nghệ thông tin**

1. Mô tả chung về học phần

Học phần An ninh mạng cung cấp kiến thức về nguyên lý của các kỹ thuật an ninh mạng gồm luận lý, kỹ thuật thông qua các công cụ phân tích về các lỗ hổng trong hệ thống mạng; các kỹ thuật bảo mật hạ tầng mạng. Ví dụ như Firewall, IDS/IPS; các kỹ thuật trong bảo mật ứng dụng: remote access security, web security, Email security, buffer overflow.

Đây là một môn học cần thiết trong lĩnh vực công nghệ thông tin giúp sinh viên có cái nhìn tổng quát để phát triển các ứng dụng xây dựng trên hệ thống mạng kết nối các thiết trong công nghiệp cũng như dân dụng.

2. Các chữ viết tắt (nếu có)

OSI model: Open Systems Interconnection- Mô hình kết nối mạng quy chuẩn

TCP/IP model: Transmission Control Protocol/Internet Protocol

IoT: Internet of Things in cloud: Dịch vụ nối kết đám mây

3. Chuẩn đầu ra của học phần

Mã	Chuẩn đầu ra học phần
plo10c	1. Vận dụng kiến thức về Quản trị và An ninh mạng máy tính để xây dựng giải pháp an ninh và xử lý các lỗi trong quá trình cài đặt và cấu hình
	2. Phân tích và hiện thực các giải giải pháp an ninh máy tính. Phân loại và trình bày đặc điểm cơ bản các lỗ hổng trong hệ thống mạng
	3. Vận dụng kiến thức về an ninh mạng để giải quyết vấn đề trong thực tế. Trình bày các nhóm giải pháp sử dụng để phát hiện và phòng chống xâm nhập mạng
plo11	4. Có ý thức trách nhiệm với cộng đồng, tuân thủ pháp luật và các chuẩn mực đạo đức nghề nghiệp

4. Giáo trình và tài liệu học tập

Giáo trình và tài liệu học tập:

1. Nei Daswani, Christoph Kern, Anita Kes avan, “Foundation of Security”, Apress, 2007.

Tài liệu tham khảo:

- Steve Manzuik, Ken Pfeil, Andre,”Network Security Assessment”, Syngress, 2007

- JieWang, Computer Network Security: Theory and Practice, Springer Berlin Heidelberg New York, 2009

5. Chiến lược học tập

Sinh viên cần tích cực và chủ động tham gia vào quá trình học tập; cần tham gia đầy đủ các giờ học theo quy định, không ngừng phấn đấu để duy trì sự tiến bộ liên tục trong học tập; hoàn thành nhiệm vụ học tập đúng tiến độ.

Để hoàn thành tốt học phần này, sinh viên cần:

+ Tích cực thực hiện các nhiệm vụ học tập do giảng viên giao cho.

+ Tích cực tìm hiểu các giáo trình, bài giảng, tài liệu tham khảo mà giảng viên yêu cầu.

Chủ động nghiên cứu mở rộng các tài liệu có liên quan đến bài học.

+ Chủ động và tích cực làm bài tập trước khi tham dự buổi học kế tiếp.

+ Chủ động và tích cực tham gia thảo luận; biết đặt các câu hỏi để trao đổi .

+ Cần ghi những chú ý và vẽ sơ đồ thiết kế

6. Nội dung, kế hoạch giảng dạy và đánh giá

Nội dung và kế hoạch giảng dạy, đánh giá	**Hoạt động học tập của người học**				**Chuẩn đầu ra**
	Trên lớp	**ST**	**Tự học**	**SG**	
Mở đầu					
Chương 1: **Tổng quan về bảo mật mạng** 1.1 Tổng quan về bảo mật mạng máy tính 1.2 Các thiết bị và sự kiện có thể làm thiết bị thay đổi 1.3 Phân loại các lỗ hổng bảo mật 1.4 Các thành phần của hệ thống mạng 1.5 Các kiểu tấn công mạng 1.6 Các giải pháp phát hiện và phòng chống tấn công mạng	Nghe giảng Thuyết trình Trình chiếu Powerpoint Thảo luận	09	Xem tham các cuộc tấn công mạng máy tính lớn trong lịch sử	18	plo10c.1, plo10c.2
Đánh giá 1: 30% Nhận biết được các thiết bị có thể kết nối Internet	Trình bày được các thiết bị mạng máy tính		Các giải pháp hạn chế mức độ nguy hại của các loại tấn công		plo10c.1, plo11

Chương 2: **Công cụ phân tích, đánh giá an ninh mạng** 2.1 Thiết lập tường lửa-Firewall 2.1.1 Chặn và nhận biết các tấn công 2.1.2 Giới hạn truy cập tới sites đen 2.2 Thiết lập đảo ngược Reverse firewall: 2.2.1 Ngăn ngừa mất dữ liệu 2.2.2 Hiện hành vi bất thường. 2.3 Mạng riêng ảo VPN/edge service 2.3.1 Phân luồng truy cập internet 2.3.2 Lập máy proxy 2.4 Phát hiện mã độc và hành vi tương tác 2.5 Giám sát, đánh hơi và quét mặt/thẻ	Nghe giảng: Trình chiếu Powerpoint Thuyết trình Thực hành: Làm mẫu	09	Đọc thêm: các nội dung liên quan VLAN WIFI Security Mô phỏng	18	plo10c.2, plo11
Chương 3:**Mã hóa Cryptography** 3.1 Các loại board nhúng thông dụng: Cấu hình 3.2 Căn bản về mã hóa 3.3 Một số kỹ thuật mã hóa 3.4 Ứng dụng của các kỹ thuật mã hóa trong các ứng dụng trên mạng 3.5 Các interface giao tiếp	Nghe giảng Thực hành: Trình chiếu Thuyết trình - Làm mẫu	09	Làm bài thực hành Mô phỏng Ứng dụng của các kỹ thuật mã hóa trong các ứng dụng trên mạng	18	plo10c.1, plo10c.2, plo10c.3
Chương 4: **Bảo mật hạ tầng mạng và phòng chống xâm nhập** 4.1 Thiết lập các chính sách an ninh 4.1.1 Thiết bị cứng 4.1.2 Phần mềm 4.1.3. Quản lý khu vực 4.2 Xây dựng tường lửa phân cấp Switch firewall 4.3 Dịch lại địa chỉ mạng- NAT 4.4 IDS/IPS 4.4.1 Hệ thống phát hiện xâm nhập 4.4.2 Hệ thống ngăn chặn xâm nhập	Nghe giảng: Trình chiếu - Thuyết trình Thực hành: - Làm mẫu	09	Cài đặt IDS/IPS mã nguồn mở Mô phỏng	18	plo10c.2, plo10c.3,

Đánh giá 2: 30% Thao tác như cài đặt, kết nối, và vận hành: thành công hay không	Trên thiết bị Switches and Routers				plo10c.2, plo10c.3,
Chương 5: **Sử dụng các ứng dụng bảo mật** 5.1 Dịch vụ IoT: broker, API gateway, các loại hệ cơ sở dữ liệu 5.2 Bảo mật truy cập từ xa 5.3 Bảo mật IoT: xác thực, Mã hóa TLS/SSL 5.4 Bảo mật bằng web: ngăn/ hạn chế tracks 5.5 Bảo mật thư điện tử 5.6 Tràn bộ đệm	Nghe giảng Thực hành	09	Thiết lập chế độ hoạt động Lập trình mã	18	plo10c.1, plo10c.2, plo10c.3,
Tổng kết-dự án	Thực hành	2		4	…
Đánh giá 3: 40% An ninh ứng dụng liên kết: dò tìm điểm đã thông, mức độ thành công					plo10c.1plo10 c.2, plo10c.3
Tổng số tiết/giờ học		**45**		**90**	

ST-Số tiết chuẩn SG-Số giờ

7. Đánh giá kết quả học tập

Hoạt động đánh giá của học phần gồm:

Phân loại	**Phương pháp đánh giá**	**Tỷ trọng**	**Chuẩn đầu ra**			
			plo10c.1	**plo10c.2**	**plo10c.3**	**plo11**
Quá trình	ĐG1. Báo cáo	30%	x		x	x
	ĐG2. Báo cáo	30%	x	x	x	
Kết thúc học phần	ĐG3. Báo cáo, đề mô	40%	x	x	x	
	Tổng cộng:	100%				

7.1 Hoạt động đánh giá 1 (ĐG1) - Chuẩn đầu ra: **plo10c.1, plo10c.3, plo11 -** Tỷ lệ: **30%** điểm học phần

- Hình thức đánh giá: Báo cáo trực tiếp
- Mô tả bài đánh giá:Trình bày được tổng quan về bảo mật mạng máy tính, các thành phần của hệ thống mạng, xây dựng giải pháp an ninh và xử lý các lỗi trong quá trình cài đặt và cấu hình, có ý thức trách nhiệm với cộng đồng, tuân thủ pháp luật và các chuẩn mực đạo đức nghề nghiệp khi tương tác trên mạng.
- Ma trận đánh giá:

Tiêu chí đánh giá	**Khung điểm**				
	A	**B**	**C**	**D**	**F**
	8,5 ÷ 10	**7,0 ÷ 8,4**	**5,5 ÷ 6,9**	**4,0 ÷ 5,4**	**< 4,0**

Tiêu chí đánh giá	Khung điểm				
	A	**B**	**C**	**D**	**F**
	8,5 ÷ 10	**7,0 ÷ 8,4**	**5,5 ÷ 6,9**	**4,0 ÷ 5,4**	**< 4,0**
TC1: Trình bày các thiết bị có thể kết nối Internet và các hình thức tấn công. Phân tích và đưa ra giải pháp hạn chế mức độ nguy hại của các loại tấn công (80%)	Trình bày các thiết bị có thể kết nối và các hình thức tấn công, phân tích đưa ra được giải pháp đạt hiệu quả	Trình bày các thiết bị có thể kết nối và các hình thức tấn công, phân tích và đưa ra được giải pháp	Trình bày các thiết bị có thể kết nối và các hình thức tấn công, đưa ra được giải pháp nhưng chưa phân tích được	Trình bày các thiết bị có thể kết nối và các hình thức tấn công, chưa đưa ra được giải pháp	Trình bày còn thiếu và chưua đưa ra được giải pháp
TC2: Có ý thức trách nhiệm với cộng đồng, tuân thủ pháp luật và các chuẩn mực đạo đức nghề nghiệp. (20%)	Trình bày và giải thích rõ ràng các quy định pháp lý và chuẩn mực đạo đức và ý thức trách nhiệm khi tương tác trên mạng.	Trình bày và giải thích được các quy định pháp lý và chuẩn mực đạo đức và ý thức trách nhiệm khi tương tác trên mạng.	Trình bày nhưng chưa giải thích rõ ràng các quy định pháp lý và chuẩn mực đạo đức và ý thức trách nhiệm khi tương tác trên mạng.	Trình bày còn thiếu các quy định pháp lý và chuẩn mực đạo đức và ý thức trách nhiệm khi tương tác trên mạng.	Trình bày sơ sài các quy định pháp lý và chuẩn mực đạo đức và ý thức trách nhiệm khi tương tác trên mạng.

Đánh giá 1 = TC1 × 30% + TC2 × 30% + TC3 × 40%

7.2 Hoạt động đánh giá 2 (ĐG2)- Chuẩn đầu ra: plo10c.1, plo10c.2, plo10c.3

- Hình thức đánh giá: Báo cáo trực tiếp
- Mô tả bài đánh giá: Thiết lập hệ thống với công cụ phân tích, đánh giá an ninh mạng
- Ma trận đánh giá:

Tiêu chí đánh giá	Khung điểm				
	A	**B**	**C**	**D**	**F**
	8,5 ÷ 10	**7,0 ÷ 8,4**	**5,5 ÷ 6,9**	**4,0 ÷ 5,4**	**< 4,0**
TC1: Mạng LAN Các chính sách an toàn (40%)	Mô hình OSI Các thiết bị an ninh mạng	Công cụ phân tích mạng	Công cụ đánh giá an ninh mạng	Quản lý khu vực vật lý	Nhân viên vào ra
TC2:	Mã hóa	Network	Thu thập	Dữ liệu	Lưu

Tiêu chí đánh giá	Khung điểm				
	A	B	C	D	F
	8,5 ÷ 10	7,0 ÷ 8,4	5,5 ÷ 6,9	4,0 ÷ 5,4	< 4,0
Internet (30%)	Phân tích thiết kế	security	Logs monitoring	Analyses Data	Data tore
CT3: Setting (30%)	Phân tích Nhu cầu	Thiết kế mạng subnet	Gắn kết thiết bị	Quản lý hệ thống	Cấu hình

Đánh giá 2 = TC1 × 40% + TC2 × 30% + TC3 × 30%

7.3 Hoạt động đánh giá 3 (ĐG3)- Chuẩn đầu ra: plo10c.1, plo10c.2, plo10c.3

- Hình thức đánh giá: Báo cáo trực tiếp
- Mô tả bài đánh giá: Trình bày được các các chính sách an ninh trong cơ quan áp dụng mạng - Network security policy
- Ma trận đánh giá:

Tiêu chí đánh giá	Khung điểm				
	A	B	C	D	F
	8,5 ÷ 10	7,0 ÷ 8,4	5,5 ÷ 6,9	4,0 ÷ 5,4	< 4,0
TC1: Cơ sở hạ tầng mạng (40%)	Tài nguyên Internet	Thu thập dữ liệu Các chính sách an ninh	Web security	Email security	Độ phủ
TC2: Đánh giá (40%)	Kết nối: Phân tích Dữ liệu	Buffer overflow	Remote access security	Lớp ứng dụng Mã hóa TLS/SSL	IoT security: xác thực,
TC3: Khai thác an toàn mạng (20%)	An ninh ứng dụng	Thiết kế an ninh mạng	Gắn kết thiết bị	Quản lý hệ thống	Chuyển giao Và an ninh hệ thống

Đánh giá 3 = TC1 × 40% + TC2 × 40% + TC3 × 20%

7.4 Cách tính kết quả học tập chung của học phần

Kết quả đánh giá chung: Đánh giá= ĐG1× 30% +ĐG2× 40% +ĐG3× 40%

8. Các phương tiện, trang thiết bị dạy và học

Phòng học có máy chiếu, phấn bảng, thiết bị mạng, thiết bị đề mo

Sinh viên có máy tính laptop, trình mô phỏng

9. An toàn của sinh viên và giảng viên

Giảng viên và sinh viên phải tuân thủ các quy định về việc sử dụng các trang thiết bị điện tại phòng học.

Trong trường hợp phát sinh các vấn đề có thể dẫn đến mất an toàn, sinh viên cần kịp

thời báo cáo với giảng viên để phối hợp giải quyết.

10. Kỷ luật, khiếu nại và hỗ trợ

- Sinh viên chỉ được công nhận hoàn thành môn học nếu có đủ các điều kiện sau:

+ Có mặt trên lớp đủ thời gian theo quy định của nhà trường.

+ Điểm học phần từ 5,5 trở lên và điểm các bài đánh giá đạt từ 5,5 trở lên.

- Nếu có gian lận trong hoạt động đánh giá nào thì sẽ hủy kết quả đánh giá đó.10/10

- Sinh viên chưa đạt đánh giá nào vẫn tiếp tục học các học phần tiếp theo và sẽ được trả

nợ trong quá trình học.

- Sinh viên có quyền khiếu nại trực tiếp giáo viên về kết quả đánh giá ngay sau khi kết quả được công bố.

- Sinh viên gặp bất kỳ khó khăn gì trong quá trình học tập có thể liên hệ trực tiếp với giảng viên, Trưởng khoa/bộ môn, Văn phòng hỗ trợ sinh viên, Phòng Đào tạo & NCKH, Ban Thanh tra của Nhà trường để được hướng dẫn, hỗ trợ

Chủ tịch Hội đồng **xây dựng CTĐT ngành**	*Hải Phòng, ngày tháng năm 2022* **Người biên soạn**
	Nguyễn Thị Xuân Hương