BỘ CÔNG THƯƠNG
TRƯỜNG ĐH CÔNG NGHIỆP QUẢNG NINH

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

ĐỀ CƯƠNG CHI TIẾT HỌC PHẦN
TRÌNH ĐỘ ĐÀO TẠO: ĐẠI HỌC
NGÀNH/CHUYÊN NGÀNH: MẠNG MÁY TÍNH

1. Tên học phần:

Tiếng Việt: **An toàn và an ninh mạng**

Tiếng Anh: **Network safety and security**

Mã số học phần: ĐHCQ0003

Số tín chỉ học phần: 03 (lý thuyết, thực hành)

Số tiết học phần:

Lý thuyết: 30; Thực hành: 30

Tự học: 90

2. Đơn vị quản lý học phần:

2.1. Giảng viên giảng dạy:

1. ThS. Đặng Đình Đức
2. TS. Trần Văn Liêm

2.2. Bộ môn: Mạng và Công nghệ phần mềm

2.3. Khoa: Công nghệ thông tin

3. Điều kiện tiên quyết học phần

3.1. Học phần tiên quyết: Không

3.2. Học phần học trước: Mạng máy tính và truyền thông; Đảm bảo và an toàn thông tin.

4. Mục tiêu của học phần:

4.1. Kiến thức:

4.1.1. Hiểu biết rõ cơ sở luật pháp, luật an ninh mạng, quá trình xây dựng hệ thống an toàn, vấn đề an toàn hệ thống và an ninh mạng trong thực tiễn;

4.1.2. Nắm rõ các kiến thức cơ bản về an toàn và an ninh hệ thống mạng máy tính bao gồm các vấn đề an ninh dữ liệu, truyền thông, dịch vụ, thiết bị.

4.1.3. Nắm rõ tác hại của mã độc và các nguy cơ hiểm họa từ mã độc tác động đến an toàn và an ninh mạng trong vấn đề quản lý dữ liệu, an toàn khi truyền dữ liệu trong môi trường mạng máy tính.

4.1.4. Hiểu rõ tác động của việc đảm bảo an toàn an ninh cho các hệ thống mạng máy tính đối với sự vận hành, phát triển của các hệ thống máy tính, các kỹ thuật tấn công hệ thống máy tính, các phương pháp phòng chống.

4.1.5. Hiểu được các chiến lược an toàn hệ thống, các phương pháp an toàn mạng, một số lỗ hổng và cách thức tấn công mạng của hacker, một số kỹ phòng thủ trong an ninh mạng

4.1.6. Hiểu biết các kiến thức về an ninh mạng, những yêu cầu cơ bản cho một hệ thống mạng an toàn; những nguy cơ, các dạng tấn công vào hệ thống máy tính và mạng máy tính.

4.1.7. Nắm rõ cách thức hoạt động của các phần mềm có hại một hệ thống máy tính, mạng máy tính từ đó vận dụng các kỹ thuật để phòng chống và gia cố hệ thống.

4.1.8. Giải thích được các kiến thức nền tảng về bảo mật như: mật mã, các giải thuật dùng trong mã mật, khóa riêng và khóa chung, chữ ký điện tử, chứng chỉ số, các hệ thống xác thực.

4.1.9. Kiến thức về các mô hình mạng an toàn, vận dụng được các giải pháp an toàn cho dịch vụ Internet, một số kỹ thuật, giải pháp và công nghệ an ninh mạng phổ biến hiện nay như: xác thực, mã hóa, tường lửa, mạng riêng ảo, hệ thống phát hiện xâm nhập.

4.2. Kỹ năng:

4.2.1. Thành thạo đọc hiểu các kiến thức mở rộng của môn học an ninh mạng. Biết phân tích các giải pháp an ninh trong các hoạt động hệ thống, đánh giá, và đưa ra những nhận xét, giải pháp tăng cường an ninh cho hệ thống mạng.

4.2.2. Sử dụng thành thạo một số phần mềm tiện ích và phần mềm công cụ để phục hồi, bảo vệ cho hệ thống thông tin; cũng như áp dụng một cách thích hợp các kỹ thuật căn bản đảm bảo an toàn truyền thông và an toàn hệ thống khi bị tấn công trên mạng;

4.2.3. Thành thạo kỹ năng phòng chống xâm nhập trong mạng máy tính, làm việc độc lập, làm việc nhóm, tư duy, áp dụng các kỹ thuật để phân tích phương án và triển khai phát hiện xâm nhập và phòng thủ trong an ninh mạng

4.2.4. Có khả năng thích ứng với sự thay đổi của công nghệ mạng máy tính nói riêng và các công nghệ khác nói chung

4.2.5. Có kỹ năng thực hiện mô phỏng các kỹ thuật tấn công hệ thống máy tính thông dụng, từ đó xây dựng chiến lược, quy trình phòng chống các cuộc tấn công hệ thống máy tính.

4.3. Năng lực tự chủ và trách nhiệm:

4.3.1. 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;

4.3.2. 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;

4.3.3. 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.

4.3.4. Có tính thần và thái độ nghiêm túc và có khả năng đọc hiểu và nghiên cứu chuyên sâu trong lĩnh vực an ninh mạng máy tính. Có năng lực định hướng, lập kế hoạch,

điều phối, quản lý, hướng dẫn, giám sát, đánh giá và đưa ra kết luận các công việc thuộc chuyên môn nghề nghiệp

4.3.5. Có thái độ tích cực trong học tập và chịu trách nhiệm với các nhiệm vụ được phân công

5. Chuẩn đầu ra học phần

Sau khi hoàn thành việc học học phần này, sinh viên có thể:

1. Nắm rõ cơ sở luật pháp, chính sách, luật an ninh mạng, quản lý rủi ro, quá trình xây dựng hệ thống an toàn, vấn đề an toàn hệ thống và an ninh mạng;

2. Trình bày và phân tích được sự an toàn và an ninh mạng trong việc quản lý dữ liệu, truyền dữ liệu trong môi trường mạng máy tính

3. Phân tích và vận dụng được cách thức hoạt động của các phần mềm có hại một hệ thống máy tính, mạng máy tính từ đó vận dụng các kỹ thuật đề phòng chống và gia cố hệ thống mạng máy tính.

4. Làm chủ được những luận điểm quan trọng trong việc kiểm tra và triển khai được phương án phòng chống xâm nhập trong mạng máy tính, làm việc độc lập, làm việc nhóm, tư duy, áp dụng các kỹ thuật để phát hiện xâm nhập và phòng thủ trong an ninh mạng.

5. Hiểu rõ các phương pháp an toàn mạng, một số lỗ hổng và cách thức tấn công mạng của hacker cũng như chọn lựa được các mô hình mạng an toàn và chọn lựa được các giải pháp an toàn cho các dịch vụ

6. Sử dụng thành thạo một số kỹ thuật, giải pháp và công nghệ an ninh mạng phổ biến hiện nay như: xác thực, mã hóa, tường lửa, mạng riêng ảo

7. Phân tích và đánh giá được sự khác biệt giữa hệ thống phát hiện xâm nhập và hệ thống ngăn ngừa xâm nhập mạng

8. Hiểu và trình bày được những yêu cầu cơ bản cho một hệ thống mạng an toàn; những nguy cơ, các dạng tấn công và một số kỹ thuật xâm nhập hệ thống máy tính và mạng máy tính

6. Tóm tắt nội dung học phần

Học phần An toàn và an ninh mạng gồm các nội dung khái lược về an toàn và thông tin dữ liệu, những nội dung cơ bản trong an ninh mạng; lỗ hổng bảo mật và các loại tấn công phổ biến; an ninh mạng mức giao vận; an ninh thư điện tử; an toàn và an ninh mạng máy tính; một số kỹ thuật phát hiện xâm nhập và phòng thủ trong an ninh mạng. Thông qua học phần giúp sinh viên ghi nhớ, phân loại, thực hiện cũng như đánh giá mức độ an toàn của hệ thống mạng

7. Cấu trúc nội dung học phần

Đề mục	Nội dung	Số tiết			Mục tiêu
		Tổng	LT	TH/TN	
Chương 1	**Tổng Quan về An toàn và an ninh mạng**	**4**	**2**	**2**	
1.1	Các khái niệm cơ bản	2	1	1	4.1.1

1.2	Mục tiêu an toàn an ninh mạng				4.1.2
1.3	Các mô hình an ninh mạng	2	1	1	
1.4	Các chính sách an ninh mạng				
1.5	Các yêu cầu của một hệ thống an ninh mạng - Kiến trúc AAA				
Chương 2	**An toàn và an ninh hạ tầng mạng**	**8**	**4**	**4**	
2.1	An ninh mạng trong mô hình OSI	4	2	2	4.1.3 4.1.4
2.2	Các lỗ hổng bảo mật của mạng máy tính				
2.3	Các giao thức và dịch vụ truy nhập từ xa (RADIUS, TACACS)				
2.4	Các mô hình điều khiển truy nhập (MAC, RBAC, DAC)	4	2	2	
2.5	Điều khiển truy nhập mạng (NAC)				
2.6	Mạng riêng ảo VPN				
2.7	An toàn cho mạng WLAN				
	Kiểm tra bài 1				
Chương 3	**Mã độc, phân tích mã độc**	**16**	**8**	**8**	
3.1	Tổng quan mã độc	4	2	2	4.1.5
3.2	Các loại mã độc				
3.3	Hiểm họa của mã độc đối với ATM	4	2	2	
3.4	Nhận biết mã độc và cách phòng tránh	4	2	2	
3.5	Phương pháp phân tích mã độc	4	2	2	
Chương 4	**Tấn công xâm nhập hệ thống mạng**	**16**	**8**	**8**	
4.1	Phương pháp luận tấn công	4	2	2	4.1.5 4.1.6 4.1.7
4.2	Định nghĩa, khái niệm tấn công				
4.3	Phân loại tấn công				
4.4	Các mô hình thực hiện tấn công	4	2	2	
4.5	Các phương pháp phòng chống tấn công				
4.6	Một số công cụ tấn công mạng	4	4	4	
4.7	Tấn công mạng qua lỗ hổng				
4.8	An toàn dịch vụ WEB	4	2	2	
	Kiểm tra bài 2				
Chương 5	**Công nghệ tường lửa (Firewall)**	**8**	**4**	**4**	
5.1	Giới thiệu tổng quan	4	2	2	4.1.6 4.1.7
5.2	Nguyên lý làm việc				
5.3	Phân loại firewall				
5.4	Một số mô hình firewall	4	2	2	

5.5	Đánh giá firewall				
Chương 6	**Hệ thống phát hiện và phòng chống xâm nhập (IDS&IPS)**	**8**	**4**	**4**	
6.1	Khái niệm chung về IDS và IPS	4	2	2	4.1.7 4.1.8 4.1.9
6.2	Hệ thống phát hiện xâm nhập IDS				
6.3	Hệ thống phòng chống xâm nhập IPS				
6.4	Xây dựng các mô hình trong thực tế				
6.5	Đánh giá về các hệ thống				
6.6	Đánh giá ưu - nhược điểm của hai hệ thống IDS và IPS	4	2	2	
	Kiểm tra bài 3				
	Tổng cộng	**60**	**30**	**30**	

8. Phương pháp giảng dạy

- Giảng dạy lý thuyết kết hợp thảo luận theo nhóm
- Phương pháp Suy nghĩ - Chia sẻ.
- Phương pháp thực hành

9. Nhiệm vụ của sinh viên:

Sinh viên phải thực hiện các nhiệm vụ sau:

- Có mặt tối thiểu 70% số tiết học lý thuyết.
- Tham gia và hoàn thành đầy đủ các buổi thao luận, bài tập nhóm/bài tập và được đánh giá kết quả thực hiện.
- Tham dự kiểm tra giữa học kỳ.
- Chủ động chuẩn bị các nội dung và thực hiện giờ tự học theo mục 12
- Thực hiện các hoạt động khác theo yêu cầu của giảng viên.

10. Đánh giá kết quả học tập của sinh viên

10.1. Cách đánh giá

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

TT	Điểm thành phần	Quy định	Trọng số	Ghi chú
1	Điểm chuyên cần	Số tiết sinh viên tham dự học/tổng số tiết quy định. Ý thức, thái độ học tập trên lớp, ý thức chuẩn bị bài, làm bài tập … của sinh viên.	10%	Sinh viên không tham dự đủ 70% số tiết học trên lớp thì không được dự thi kết thúc học phần
2	Điểm quá trình	Bài tập lớn/thực hành	30%	
3	Điểm thi kết thúc học phần	Vấn đáp + Thực hành	60%	

10.2. Cách tính điểm:

Điểm học phần bao gồm điểm kiểm tra thường xuyên trong quá trình học tập; điểm đánh giá nhận thức và thái độ tham gia thảo luận; điểm đánh giá phần thực hành; điểm chuyên cần; điểm thi giữa học phần; điểm tiểu luận và điểm thi kết thúc học phần thực hiện theo công thức sau:

Điểm học phần	=	Điểm chuyên cần x 0.1	+	Điểm quá trình x 0.3	+	Điểm thi kết thúc học phần x 0.6

Điểm học phần tính theo thang điểm 10 làm tròn đến một chữ số thập phân, sau đó được quy đổi sang điểm chữ và điểm số theo thang điểm 4 theo quy chế đào tạo của Nhà trường.

11. Tài liệu học tập, tham khảo:

- Giáo trình học tập chính:

[1]. Giáo trình An toàn và an ninh mạng - Trường Đại học Công nghiệp Quảng Ninh. 2022

[2]. Lab thực hành An toàn và an ninh mạng, Trường Đại học Công nghiệp Quảng Ninh, 2022

- Tài liệu tham khảo:

[3] Giáo trình An toàn và bảo mật dữ liệu, Trường Đại học Công nghiệp Quảng Ninh, 2022

[4] PGS.TS. Thái Hồng Nhị, TS. Phạm Minh Việt, An toàn thông tin, NXB Khoa học và Kỹ thuật, 2011;

[5] PGS.TS. Hoàng Đăng Hải, Bài giảng An ninh mạng, Học viện Bưu chính viễn thông, 2018;

12. Hướng dẫn tự học của học phần

Chương	Nội dung	LT (tiết)	BT (tiết)	TH (tiết)	Sinh viên cần tham khảo và chuẩn bị
1	1. Các mô hình an ninh mạng 2. Các chính sách an ninh mạng 3. Các yêu cầu của một hệ thống an ninh mạng - Kiến trúc AAA	5	2	5	Tài liệu [1] chương 1 Tài liệu [2] chương 1
2	1. Các giao thức và dịch vụ truy nhập từ xa (RADIUS, TACACS) 2. Các mô hình điều khiển truy nhập (MAC, RBAC, DAC)	10	3	10	Tài liệu [1] chương 2 Tài liệu [2] chương 2 Tài liệu [3] chương 3

Chương	Nội dung	LT (tiết)	BT (tiết)	TH (tiết)	Sinh viên cần tham khảo và chuẩn bị
	3. Điều khiển truy nhập mạng (NAC) 4. Mạng riêng ảo 5. An toàn cho mạng WLAN				
3	3.1. Các loại mã độc 3.2. Hiểm họa của mã độc đối với ATM 3.3. Phương pháp phân tích mã độc	5	3	5	Tài liệu [1] chương 3 Tài liệu [2] chương 3 Tài liệu [3] chương 4
4	1. Các mô hình thực hiện tấn công 2. Các phương pháp phòng chống tấn công 3. Một số công cụ tấn công mạng 4. Tấn công mạng qua lỗ hổng 5. An toàn dịch vụ WEB	5	2	10	Tài liệu [1] chương 4 Tài liệu [2] chương 4 Tài liệu [3] chương 4
5	1. Phân loại firewall 2. Một số mô hình firewall	5	2	5	Tài liệu [1] chương 5 Tài liệu [2] chương 5
6	1. Hệ thống phát hiện xâm nhập IDS 2. Hệ thống phòng chống xâm nhập IPS 3. Xây dựng các mô hình trong thực tế	5	3	5	Tài liệu [1] chương 6 Tài liệu [2] chương 6
	Tổng cộng	**35**	**15**	**40**	

Quảng Ninh, ngày 21 tháng 10 năm 2022

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