BỘ GIÁO DỤC VÀ ĐÀO TẠO
TRƯỜNG ĐẠI HỌC CẦN THƠ

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

ĐỀ CƯƠNG CHI TIẾT HỌC PHẦN

1. Tên học phần: An ninh mạng (Network Security)

- **Mã số học phần:** CT211
- **Số tín chỉ học phần: 03** tín chỉ
- **Số tiết học phần:** 30 tiết lý thuyết + 30 tiết thực hành + 90 tiết tự học

2. Đơn vị phụ trách học phần:

- **Bộ môn:** Mạng máy tính và truyền thông
- **Khoa:** Công nghệ thông tin và truyền thông

3. Điều kiện:

- **Điều kiện tiên quyết:** Thiết kế và cài đặt mạng (CT335)
- **Điều kiện song hành:** Giải quyết sự cố mạng (CT344)

4. Mục tiêu của học phần:

Mục tiêu	Nội dung mục tiêu	CĐR CTĐT
4.1	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 và một số kỹ thuật xâm nhập hệ thống máy tính và mạng máy tính.	2.1.3c 2.2.1a
4.2	Kiến thức về 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.	2.1.3c 2.2.1a
4.3	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.	2.1.3c 2.2.1a
4.4	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.	2.1.3c 2.2.1a 2.3a; 2.3b

5. Chuẩn đầu ra của học phần:

CĐR HP	Nội dung chuẩn đầu ra	Mục tiêu	CĐR CTĐT
	Kiến thức		
CO1	Trình bày được tổng quan về an ninh mạng.	4.1	2.1.3c
CO2	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	4.1	2.1.3c

CĐR HP	Nội dung chuẩn đầu ra	Mục tiêu	CĐR CTĐT
	tính.		
CO3	Diễn giải 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.	4.2	2.1.3c
CO4	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.	4.3	2.1.3c
CO5	Trình bày được các mô hình mạng an toàn	4.3	2.1.3c
CO6	Trình bày được các giải pháp an toàn cho dịch vụ Internet	4.3	2.1.3c
CO7	Lựa chọn 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		2.1.3c
CO8	Diễn giải hoạt động của hệ thống phát hiện xâm nhập và hệ thống ngăn ngừa xâm nhập mạng		2.1.3c
	Kỹ năng		
CO9	Xác định được mục đích và các yêu cầu của an ninh mạng	4.4	2.2.1a
CO10	Vận dụng kiến thức để thực nghiệm các kỹ thuật tấn công, quét để xác định điểm yếu của hệ thống mạng		2.2.1a
CO11	Lựa chọn và thực hiện được các kỹ thuật gia cố hệ thống		2.2.1a
CO12	Diễn giải và vận dụng các kỹ thuật 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		2.2.1a
CO13	Chọn lựa được các mô hình mạng an toàn và chọn lựa được các giải pháp an toàn cho các dịch vụ	4.4	2.2.1a
CO14	Sử dụng 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		2.2.1a
CO15	So sánh và đánh giá được sự khác biệt giữa hệ thống phát hiện xâm nhập và hệ thống ngăn ngừa xâm nhập mạng		2.2.1a
	Thái độ/Mức độ tự chủ và trách nhiệm		
CO16	Nghiêm túc trong học tập, nghiên cứu tìm tòi, thông tin liên quan về an ninh mạng. Tự tổ chức thực nghiệm để trải nghiệm thực tế, rèn luyện kỹ năng chuyên môn để tích lũy kinh nghiệm và làm giàu kiến thức bản thân.	4.4	2.3a; 2.3b
CO17	Rèn luyện tính chuyên nghiệp trong việc lập kế hoạch, triển khai hệ thống, phân tích đánh giá và linh động trong		2.3a; 2.3b

CĐR HP	Nội dung chuẩn đầu ra	Mục tiêu	CĐR CTĐT
	xử lý tình huống liên quan đến an ninh mạng		
CO18	Ý thức tự học nâng cao trình độ, cập nhật kiến thức mới để thức khai thác các thế mạnh của công nghệ mạng máy tính, an ninh mạng vào lĩnh vực khác nhau của đời sống kinh tế xã hội		2.3a; 2.3b

6. Mô tả tóm tắt nội dung học phần:

Học phần này cung cấp cho sinh viên một khối lượng kiến thức tương đối hoàn chỉnh về phương pháp xây dựng một hệ thống an toàn cho máy tính và mạng máy tính. Sau khi học xong môn này, sinh viên có được những khả năng sau:

- Giải thích được thế nào là an ninh mạng
- Trình bày được những nguy cơ, các dạng tấn công và một số kỹ thuật xâm nhập hệ thống máy tính và mạng máy tính.
- Trình bày được các yêu cầu cơ bản cho một hệ thống mạng an toàn.
- Trình bày 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.
- 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.
- Trình bày và cài đặt được các cơ chế an toàn cho các thiết bị mạng.
- Xây dựng được các mô hình mạng an toàn.
- Vận dụng được các giải pháp an toàn cho dịch vụ Internet.
- Lựa chọn được 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.
- Trình bày được cách quản lý và điều hành một hệ thống mạng an toàn.

7. Cấu trúc nội dung học phần:

7.1. Lý thuyết

	Nội dung	Số tiết	CĐR HP
Chương 1.	Tổng quan về an ninh mạng	**3**	CO1
1.1.	Giới thiệu		
1.2.	Các kiểu tấn công mạng		
1.3.	Phần mềm có hại		
1.4.	Các yêu cầu của một hệ thống an ninh mạng – Kiến trúc AAA		
Chương 2.	An toàn cho các thiết bị mạng	**3**	CO2
2.1.	An ninh mạng ở tầng vật lý		
2.2.	An ninh mạng ở tầng liên kết dữ liệu		

	Nội dung	Số tiết	CĐR HP
2.3.	An ninh mạng ở tầng mạng		
2.4.	An ninh mạng ở tầng vận chuyển và các tầng trên		
Chương 3.	Gia cố hệ thống (system hardening)	**6**	CO3
3.1.	Khái niệm		
3.2.	Gia cố hệ điều hành và hệ điều hành mạng		
3.3.	Gia cố ứng dụng		
3.4.	Tổ chức chính sách an ninh mạng		
3.5.	Điều tra xâm nhập mạng		
3.6.			
Chương 4.	Căn bản về mật mã (Cryptography)	**6**	CO4
4.1.	Khái niệm		
4.2.	Ứng dụng của mật mã		
4.3.	Các thuật toán mã hóa		
4.4.	Khóa bí mật và khóa công khai		
4.5.	Hạ tầng khóa công khai		
4.6.	Chữ ký số và chứng chỉ số		
	Quản lý khóa và chứng chỉ số		
Chương 5.	An toàn trong truyền thông	**3**	CO5-CO7
5.1.	Truy cập từ xa		
5.2.	Truy cập liên mạng		
Chương 6.	Các mô hình mạng an toàn	**3**	CO5
6.1.	Khái niệm về các vùng an ninh		
6.2.	Mạng cục bộ ảo (VLANs)		
6.3.	Dịch vụ NAT & PAT		
Chương 7.	Tường lửa (Firewall)	**6**	CO7
7.1.	Giới thiệu tổng quan		
7.2.	Tường lửa		
7.3.	Phân loại tường lửa		
Chương 8.	Hệ thống phát hiện xâm nhập (IDS-Intrusion Detection Systems) và Hệ thống ngăn ngừa xâm nhập mạng (IPS-Intrusion Prevention Systems)	**6**	CO8
8.1.	Giới thiệu tổng quan		
8.2.	Hệ thống phát hiện xâm nhập (IDS-Intrusion Detection Systems)		
8.3.	Hệ thống ngăn ngừa xâm nhập mạng (IPS-Intrusion Prevention Systems)		
8.4.	Đánh giá ưu – nhược điểm của hai hệ thống IDS và IPS		

7.2. Thực hành

	Nội dung	Số tiết	CĐR HP

	Nội dung	Số tiết	CĐR HP
Bài 1.	Syslog-SSH-NTP, PAP, CHAP	**5**	CO1-CO4 CO9-CO14
Bài 2.	Layer 2 và VLAN-Security	**5**	CO2-CO3 CO11, CO13
Bài 3.	AAA, DHCP, NAT, Wireless	**5**	CO1-CO2, CO5
Bài 4.	Site-to-Site-IPsec-VPN, CBAC	**5**	CO4-CO7, CO12-CO14
Bài 5.	Secure network	**5**	CO5-CO6, CO13-CO14
Bài 6.	Cấu hình cơ bản tường lửa và hệ thống ngăn chặn xâm nhập	**5**	CO7-C08 CO14-CO15

8. Phương pháp giảng dạy:

- Giảng viên trình bày lý thuyết, có ví dụ minh họa.
- Giảng viên cung cấp thông tin về tài liệu liên quan đến học phần
- Giảng viên cung cấp các yêu cầu thực hành, giới thiệu và hướng dẫn sử dụng các ứng dụng liên quan để thực hiện các bài thực hành

9. Nhiệm vụ của sinh viên:

Sinh viên phải thực hiện các nhiệm vụ như sau:

- Tham dự tối thiểu 80% số tiết học lý thuyết.
- Tham gia đầy đủ 100% giờ thực hành và thực hiện được tất cả các yêu cầu của bài thực hành
- Tham dự kiểm tra giữa kỳ và cuối kỳ đầy đủ.
- Chủ động tổ chức thực hiện giờ tự học.

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	CĐR HP
1	Điểm chuyên cần	Đánh giá mức độ tham dự các buổi học lý thuyết và thực hành	10%	CO17-CO18
2	Điểm kiểm tra giữa kỳ	Hình thức trắc nghiệm	30%	CO1-CO4 CO9-CO12
3	Điểm thi kết thúc học phần	- Thi trắc nghiệm - Tham dự tối thiểu 80% số tiết lý thuyết và tối thiểu 5/6 buổi thực hành	60%	CO1-CO15

10.2. Cách tính điểm

- Điểm đánh giá thành phần và điểm thi kết thúc học phần được chấm theo thang điểm 10 (từ 0 đến 10), làm tròn đến một chữ số thập phân.

- Điểm học phần là tổng điểm của tất cả các điểm đánh giá thành phần của học phần nhân với trọng số tương ứng. Điểm học phần 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 định về công tác học vụ của Trường.

11. Tài liệu học tập:

Thông tin về tài liệu	Số đăng ký cá biệt
[1] Michael Cross, Jeremy Faircloth, Eli Faskha, Michael Gregg, Alun Jones, Marc Perez, *Security+ : Study Guide and Practice Exam*, 2nd edition, Syngress, 2007.	
[2] William Stallings, *Network security essentials*, 2nd edition, Prentice Hall, 2003.	
[3] Cisco networking academy, *Network security v2.0,* 2004.	
[4] Eric Maiwald, *Network security: A beginner's guide*, 2nd edition, McGraw-Hill, 2003	

12. Hướng dẫn sinh viên tự học:

Tuần	Nội dung	Lý thuyết (tiết)	Thực hành (tiết)	Nhiệm vụ của sinh viên
1+2	Chương 1	12		+ Tham khảo trước các slides bài giảng cho GV cung cấp + Ghi nhận các vấn đề chưa rõ để trao đổi với GV trên lớp
3	Chương 2	6		+ Tham khảo trước các slides bài giảng cho GV cung cấp + Ghi nhận các vấn đề chưa rõ để trao đổi với GV trên lớp
4	Chương 3 Kiến thức để thực hành Syslog-SSH-NTP, PAP, CHAP	6	5	+ Tham khảo trước các slides bài giảng cho GV cung cấp + Chủ động thực hiện các yêu cầu của bài thực hành do GV cung cấp + Ghi nhận các vấn đề chưa rõ để trao đổi với GV trên lớp
5	Chương 4 Kiến thức để thực hành Layer 2 và VLAN-Security	6	5	+ Tham khảo trước các slides bài giảng cho GV cung cấp + Chủ động thực hiện các yêu cầu của bài thực hành do GV cung cấp + Ghi nhận các vấn đề chưa rõ để trao đổi với GV trên lớp

Tuần	Nội dung	Lý thuyết (tiết)	Thực hành (tiết)	Nhiệm vụ của sinh viên
6+7	Chương 5 Kiến thức để thực hành kiến trúc AAA, DHCP, NAT, Wireless	12	5	+ Tham khảo trước các slides bài giảng cho GV cung cấp + Chủ động thực hiện các yêu cầu của bài thực hành do GV cung cấp + Ghi nhận các vấn đề chưa rõ để trao đổi với GV trên lớp + Tham gia nghiêm túc buổi kiểm tra giữa kỳ
7	Chương 6 Site-to-Site-IPsec-VPN, CBAC	6	5	+ Tham khảo trước các slides bài giảng cho GV cung cấp + Chủ động thực hiện các yêu cầu của bài thực hành do GV cung cấp + Ghi nhận các vấn đề chưa rõ để trao đổi với GV trên lớp
8	Chương 7 Kiến thức để thực hành mô an ninh mạng	6	5	+ Tham khảo trước các slides bài giảng cho GV cung cấp + Chủ động thực hiện các yêu cầu của bài thực hành do GV cung cấp + Ghi nhận các vấn đề chưa rõ để trao đổi với GV trên lớp
9	Chương 8 Kiến thức để thực hành cấu hình cơ bản tường lửa và hệ thống ngăn chặn xâm nhập	6	5	+ Tham khảo trước các slides bài giảng cho GV cung cấp + Chủ động thực hiện các yêu cầu của bài thực hành do GV cung cấp + Ghi nhận các vấn đề chưa rõ để trao đổi với GV trên lớp
14				+ Cũng cố toàn bộ kiến thức đã học phần lý thuyết và thực hành + Thực hiện nghiêm túc qui chế kiểm tra

Cần Thơ, ngày 15 tháng 6 năm 2019

TL. HIỆU TRƯỞNG
TRƯỞNG KHOA

Nguyễn Hữu Hòa

TRƯỞNG BỘ MÔN

Đỗ Thanh nghị