

ĐỀ CƯƠNG CHI TIẾT HỌC PHẦN

1. Tên học phần: An toàn hệ thống (System Security)

- Mã số học phần: CT222
- Số tín chỉ học phần: 3 tín chỉ
- Số tiết học phần: 30 tiết lý thuyết, 30 tiết thực hành, 75 tiết tự học.

2. Đơn vị phụ trách học phần:

- Bộ môn: Công nghệ thông tin
- Khoa: Công nghệ thông tin & Truyền thông

3. Điều kiện:

- Điều kiện tiên quyết:
- Điều kiện song hành:

4. Mục tiêu của học phần:

Mục tiêu	Nội dung mục tiêu	CĐR CTĐT
4.1	Có kiến thức nền tảng về tác động của việc đảm bảo an toàn cho các hệ thống 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.	2.1.3.a,b,c
4.2	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.	2.2.1.a
4.3	Có khả năng làm việc độc lập cũng như làm việc theo nhóm để hoàn thành các dự án về an toàn hệ thống.	2.2.1.a

5. Chuẩn đầu ra của học phần:

CĐR HP	Nội dung chuẩn đầu ra	Mục tiêu	CĐR CTĐT
	Kiến thức		
CO1	Mô tả các khái niệm cơ bản liên quan đến an toàn thông tin và an toàn hệ thống máy tính.	4.1	2.1.3.a,b,c
CO2	Mô tả được những khái niệm liên quan đến mã hóa dữ liệu, nêu được những ứng dụng cơ bản của mã hóa dữ liệu.	4.1	2.1.3.a,b,c
CO3	Mô tả được khái niệm về phần mềm độc hại, virus máy	4.1	2.1.3.a,b,c

CĐR HP	Nội dung chuẩn đầu ra	Mục tiêu	CĐR CTĐT
	Kiến thức		
	tính, Trojan Horse, và sâu máy tính.		
CO4	Mô tả được khái niệm cơ bản về tấn công ứng dụng, hệ điều hành và mạng máy tính.	4.1	2.1.3.a,b,c
CO5	Mô tả được các mô hình bảo mật và chính sách về an toàn hệ thống máy tính.	4.1	2.1.3.a,b,c
CO6	Mô tả được một số hình thức tấn công trên dịch vụ web.	4.1	2.1.3.a,b,c
	Kỹ năng		
CO7	Giải thích được nguyên tắc vận hành của các giải thuật mã hóa dữ liệu, vận dụng được những ứng dụng cơ bản của mã hóa dữ liệu.	4.2	2.2.1.a
CO8	Giải thích được cách thức hoạt động phần mềm độc hại, virus máy tính, Trojan Horse, và sâu máy tính.	4.2	2.2.1.a
CO9	Giải thích được cách thức tấn công ứng dụng, hệ điều hành và mạng máy tính.	4.2	2.2.1.a
CO10	Giải thích và vận dụng được các mô hình bảo mật và chính sách về an toàn hệ thống máy tính.	4.2	2.2.1.a
CO11	Vận dụng các chính sách bảo mật, và mô hình bảo mật để bảo đảm an toàn hệ thống máy tính.	4.2	2.2.1.a
CO12	Giải thích cách thức tấn công dịch vụ web và phương thức phòng chống.	4.2	2.2.1.a
	Thái độ/Mức độ tự chủ và trách nhiệm		
CO13	Có ý thức kỷ luật học tập, biết làm việc theo nhóm và có tinh thần khám phá kiến thức có liên quan đến hệ điều hành.	4.3	2.2.1.a
CO14	Có ý thức sưu tầm các ứng dụng thực tiễn trong lĩnh vực an toàn hệ thống và an ninh thông tin.	4.3	2.2.1.a

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 An toàn hệ thống máy tính. Các nội dung chủ yếu bao gồm: Các khái niệm cơ bản về an toàn thông tin và máy tính, An ninh hệ điều hành, Phần mềm độc hại, An ninh mạng, An ninh dịch vụ Web, Mã hóa dữ liệu, Các mô hình an ninh và an toàn thông tin.

7. Cấu trúc nội dung học phần:

7.1. Lý thuyết

	Nội dung	Số tiết	CĐR HP
Chương 1.	GIỚI THIỆU	3	
1.1.	Các khái niệm cơ bản	1	CO1
1.2.	Mô hình truy cập	0.5	CO1
1.3.	Mô hình mã hóa	0.5	CO1;CO2;CO7
1.4.	Những vấn đề an toàn hệ thống và bảo mật	1	CO1
Chương 2.	AN NINH HỆ ĐIỀU HÀNH	4	
2.1.	Các khái niệm liên quan	0.5	CO4;CO9
2.2.	An ninh tiến trình	1	CO4;CO9
2.3.	An ninh tập tin và bộ nhớ	1	CO4;CO9
2.4.	An ninh ứng dụng chạy trên hệ điều hành	1.5	CO4;CO9
Chương 3.	PHẦN MỀM ĐỘC HẠI	4	
3.1.	Các khái niệm cơ bản	0.5	CO3;CO8
3.2.	Những tấn công bên trong	0.5	CO3;CO8
3.3.	Virus máy tính	1	CO3;CO8
3.4.	Phần mềm độc hại khác	0.5	CO3;CO8
3.5.	Những ứng dụng đe dọa thông tin người dùng	0.5	CO3;CO8
3.6.	Giải pháp hiện hữu	1	CO3;CO8 CO5;CO11
Chương 4.	AN NINH MẠNG	4	
5.1.	Những khái niệm cơ bản	0.5	CO4;CO9 CO4;CO11
5.2.	Mối đe dọa	1	CO4;CO9 CO4;CO11
5.3.	Các loại tấn công mạng	1.5	CO4;CO9 CO4;CO11
4.4.	Một số giải pháp hiện hữu	1	CO4;CO9 CO4;CO11
Chương 5.	AN NINH DỊCH VỤ WEB	6	
5.1.	Các khái niệm cơ bản	1	CO6;CO12
5.2.	Tấn công ứng dụng máy khách	2	CO6;CO12
5.3.	Tấn công ứng dụng máy chủ	2	CO6;CO12
5.4.	Các giải pháp hiện hữu	1	CO6;CO12
Chương 6.	MÃ HÓA	5	
6.1.	Các khái niệm cơ bản	0.5	CO2; CO7
6.2.	Mã hóa đối xứng	1	CO2; CO7
6.3.	Mã hóa bất đối xứng	1.5	CO2; CO7
6.4.	Các hàm băm trong mã hóa	1	CO2; CO7
6.5.	Chữ ký số và chứng chỉ số	1	CO2; CO7
Chương 7.	CÁC MÔ HÌNH BẢO MẬT	4	
7.1.	Chính sách, mô hình và niềm tin	0.5	CO5;CO11
7.2.	Mô hình điều khiển truy cập	0.5	CO5;CO11
7.3.	Đánh giá và các chuẩn an ninh	0.5	CO5;CO11
7.4.	Đánh giá bảo mật phần mềm	0.5	CO5;CO11

	Nội dung	Số tiết	CĐR HP
7.5.	Kiểm soát và quản trị	1	CO5;CO11
7.6.	Mô hình Kerberos	1	CO5;CO11

7.2. Thực hành

	Nội dung	Số tiết	CĐR HP
Bài 1	Làm quen với môi trường VMs, Unix, lập trình C	5	CO1;CO13; CO14
Bài 2	Tấn công mật khẩu, gia cố bảo mật	5	CO4; CO9; CO13;CO14
Bài 3	Mã hóa và tấn công liên quan	5	CO2; CO7; CO13;CO14
Bài 4	Tấn công web và phòng chống	5	CO6;CO12; CO13;CO14
Bài 5	Tấn công stack-overflows và phòng chống	5	CO3;CO9; CO13;CO14
Bài 6	Tường lửa	5	CO9; CO4; CO13;CO14

8. Phương pháp giảng dạy:

- Lý thuyết: Giảng viên thuyết trình, đặt vấn đề trao đổi với SV
- Thực hành: Giảng viên giao bài thực hành để SV chuẩn bị ở nhà và hướng dẫn SV thực hành lập trình trong phòng máy tính

9. Nhiệm vụ của sinh viên:

Sinh viên phải thực hiện các nhiệm vụ như sau:

- Tự đọc những nội dung và giảng viên yêu cầu.
- Tham dự tối thiểu 80% số tiết học lý thuyết.
- Tham gia đầy đủ 100% giờ thực hành/thí nghiệm/thực tập và có báo cáo kết quả.
- Thực hiện đầy đủ các bài tập nhóm/bài tập và được đánh giá kết quả thực hiện.
- Tham dự kiểm tra giữa học kỳ.
- Tham dự thi kết thúc học phần.
- 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 thực hành	- Bài kiểm tra thực hành	20%	CO13; CO14
2	Điểm kiểm tra giữa kỳ	- Tham dự bài kiểm tra giữa kỳ	30%	CO13; CO14
3	Điểm kiểm tra kết thúc học phần	- Tham dự bài kiểm tra cuối kỳ - Bắt buộc dự kiểm tra	50%	CO13; CO14

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] Computer security : Art and science / Matt Bishop.- Boston: Aindison Wesley, 2003.- 1084 p.; 24 cm, 0201440997.- 005.8/ B622	MON.021342
[2] Introduction to computer security / Matt Bishop.- Boston: Addison-Wesley, 2005.- xxxii, 747 p.: ill.; 24 cm, 0321247442.- 005.8/ B622	MON.064219

12. Hướng dẫn sinh viên tự học:

Tuần	Nội dung	Lý thuyết (tiết)	Thực hành (tiết)	Nhiệm vụ của sinh viên
1-15	Hoạt động tự học	30	45	<ul style="list-style-type: none"> - Xem lại bài giảng. - Làm bài tập khi có yêu cầu. - Tham khảo thêm tài liệu khi được yêu cầu hoặc cần tìm hiểu thêm

Cần Thơ, ngày 30 tháng 5 năm 2019

TRƯỞNG BỘ MÔN

TL. HIỆU TRƯỞNG
TRƯỜNG KHOA
TRƯỜNG ĐẠI HỌC
CẦN THƠ
Nguyễn Hữu Hòa

Phạm Thế Phi