ĐẠI HỌC QUỐC GIA TP. HỒ CHÍ MINH
TRƯỜNG ĐẠI HỌC CÔNG NGHỆ THÔNG TIN

ĐỀ CƯƠNG MÔN HỌC
NHẬP MÔN BẢO ĐẢM VÀ AN NINH THÔNG TIN

1. THÔNG TIN CHUNG (General information)

Tên môn học (tiếng Việt):	Nhập môn bảo đảm và an ninh thông tin
Tên môn học (tiếng Anh):	Introduction to Information Assurance and Security
Mã môn học:	IE105
Thuộc khối kiến thức:	Đại cương ☐; Cơ sở nhóm ngành ☐;
	Cơ sở ngành ☑; Chuyên ngành ☐; Tốt nghiệp ☐
Khoa, Bộ môn phụ trách:	Khoa học và Kỹ thuật Thông tin
Giảng viên biên soạn:	ThS. Nguyễn Duy
	Email: duyn@uit.edu.vn
Số tín chỉ:	4
Lý thuyết:	3
Thực hành:	1
Tự học:	8
Môn học tiên quyết:	Không
Môn học trước:	Nhập môn mạng máy tính

2. MÔ TẢ MÔN HỌC (Course description)

Môn Nhập môn bảo đảm và an ninh thông tin gồm các nội dung cơ bản như sau: Tổng quan về các nguyên tắc an ninh Mạng máy tính, xây dựng một tổ chức an toàn, quyền truy cập và kiểm soát truy cập, phương thức ngăn chặn việc tấn công hệ thống, bảo vệ chống lại việc tấn công Botnet, các vấn đề bảo vệ hệ thống mạng chống phần mềm độc hại, an ninh mạng Windows và Unix / Linux, bảo mật mạng truyền dẫn; bảo mật mạng LAN, mạng không dây và mạng di động.

3. MỤC TIÊU MÔN HỌC (Course goals)

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

Bảng 1.

Mục tiêu môn học	Chuẩn đầu ra trong CTĐT
Có kiến thức về cơ bản về an ninh thông tin	1.2.8
Xác định chức năng, các thành phần và kiến trúc hệ thống công nghệ	4.3.2

thông tin	
Mô hình hoá hệ thống và kết nối hệ thống	4.3.3

4. CHUẨN ĐẦU RA MÔN HỌC (Course learning outcomes)

Bảng 2.

CĐRMH	Mô tả CĐRMH (Mục tiêu cụ thể)	Mức độ giảng dạy
G1 (1.2.8.1)	Có kiến thức về hạ tầng công nghệ thông tin	T
G2 (1.2.8.5)	Có kiến thức về an toàn thông tin	T
G3 (4.3.2.1)	Biết cách xác định vai trò của các thiết bị trong hệ thống	I
G4 (4.3.2.2)	Biết cách xác định nguyên lý hoạt động của hệ thống	I
G5 (4.3.3.2)	Sự cân đối giữa các mục tiêu, chức năng, nguyên lý và cấu trúc khác nhau của hệ thống	U
G6 (4.3.3.3)	Biết các lên kế hoạch quản lý hệ thống	U

5. NỘI DUNG MÔN HỌC, KẾ HOẠCH GIẢNG DẠY (Course content, lesson plan)

a. Lý thuyết

Bảng 3.

Buổi học (30 tiết)	Nội dung	CĐR MH	Hoạt động dạy và học	Thành phần đánh giá
Buổi 1,2 (6 tiết)	**Chương 1: Tổng quan về an toàn thông tin** 1. An toàn thông tin là gì? 2. Những tác nhân ảnh hưởng đến thông tin 3. Qui trình xây dựng ATTT trong doanh nghiệp 4. Mối quan hệ giữa các khái niệm ATTT 5. Phân loại kiểm soát 6. Phân loại dữ liệu 7. Mô hình phòng thủ theo chiều sâu 8. Khuôn khổ an ninh (security framework) 9. Quản lý rủi ro (risk management)	G1, G2	**Dạy:** GV thuyết giảng **Học ở lớp:** Trao đổi những vấn đề chưa rõ hoặc chưa hiểu trong buổi học **Học ở nhà:** Tham khảo slide và nguồn internet.	A1, A4
Buổi 3,4	**Chương 2: Các kĩ thuật tấn công cơ bản** 1. Eavesdropping (Nghe lén)	G2	**Dạy:** GV	

(6 tiết)	2. Data Modification (Thay đổi dữ liệu) 3. Identity Spoofing (Giả mạo danh tính) 4. Password-Based Attacks 5. Denial-of-Service Attack (tấn công từ chối dịch vụ) 6. Malicious Software		thuyết giảng **Học ở lớp:** Trao đổi những vấn đề chưa rõ hoặc chưa hiểu trong buổi học **Học ở nhà:** Tham khảo slide và nguồn internet.	
Buổi 5 (3 tiết)	**Chương 3: Mã hoá đối xứng** 1. Giới thiệu về mật mã học 2. Lịch sử của mật mã học 3. Giải thuật mã hoá cổ điển 4. Giải thuật mã hoá hiện đại 5. Phá mã một hệ thống mật mã	G2	**Dạy:** GV thuyết giảng **Học ở lớp:** Trao đổi những vấn đề chưa rõ hoặc chưa hiểu trong buổi học **Học ở nhà:** Đọc sách 1, chương 2.	A1, A4
Buổi 6,7 (6 tiết)	**Chương 4. Mã hoá bất đối xứng** 1. Số nguyên tố 2. Hệ mã hoá khoá công khai 3. Giao thức trao đổi khoá Diffie-Hellman 4. RSA 5. Quản lý khoá 6. Hàm băm 7. Chữ kí điện tử	G2	**Dạy:** GV thuyết giảng **Học ở lớp:** Trao đổi những vấn đề chưa rõ hoặc chưa hiểu trong buổi học **Học ở nhà:** Đọc sách 1,	

			chương 2.	
Buổi 8 (3 tiết)	**Chương 5: Tưởng lửa** 1. Tường lửa là gì? 2. Phân loại tường lửa? 3. Tính năng của tường lửa thế hệ mới? 4. Mô hình triển khai tường lửa	G3, G4, G6	**Dạy:** GV thuyết giảng **Học ở lớp:** Trao đổi những vấn đề chưa rõ hoặc chưa hiểu trong buổi học **Học ở nhà:** Đọc sách 2	A1, A4
Buổi 9 (3 tiết)	**Chương 6: Proxy** 1. Proxy Server là gì? 2. Mục đích của Proxy Server 3. Phân loại Proxy Server 4. Cơ chế hoạt động của Proxy Server **5.** Mô hình triển khai Proxy Server	G3, G4, G6	Dạy: Thuyết giảng Học ở nhà: Đọc sách 1, chương 3	A1, A4
Buổi 10 (3 tiết)	**Chương 7. Hệ thống phát hiện và phòng chống xâm nhập (IDS/IPS)** 1. Tổng quan IDS/IPS 2. Thành phần chính của hệ thống IDS/IPS 3. Phân loại IDS/IPS. 4. Các kĩ thuật phát hiện xâm nhập 5. Snort	G3, G4, G6	**Dạy:** GV thuyết giảng **Học ở lớp:** Trao đổi những vấn đề chưa rõ hoặc chưa hiểu trong buổi học **Học ở nhà:** Đọc sách 1, chương 3.	
Buổi 11, 12 (6 tiết)	**Chương 8: Các giao thức bảo mật** 1. IP Security 2. Secure Socket Layer /Transport Layer Security 3. Pretty Good Privacy 4. Secure Shell	G3, G4, G5	**Dạy:** GV thuyết giảng **Học ở lớp:** Trao đổi những vấn đề chưa rõ hoặc chưa	A1, A4

			hiểu trong buổi học **Học ở nhà:** Đọc sách 3, chương 16,18,19.	
Buổi 13, 14 (6 tiết)	**Chương 9: Tìm hiểu Botnet** 1. Tìm hiểu về botnet, botnet topology và giao thức 2. Tìm hiểu về chu kì điển hình sống của Bot. 3. Mô hình phát tán Botnet, phòng chống Botnet và Botmaster Traceback	G3, G4, G5	**Dạy:** GV thuyết giảng **Học ở lớp:** Trao đổi những vấn đề chưa rõ hoặc chưa hiểu trong buổi học **Học ở nhà:** Đọc sách 1, chương 8.	A1, A4
Buổi 15 (3 tiết)	**Ôn tập – dự trữ**			

b. Thực hành

Bảng 4.

Buổi học (*30 tiết*)	**Nội dung**	**CĐRMH**	**Thành phần đánh giá**
Buổi 1 (5 tiết)	Bài thực hành 1:Tìm hiểu và triển khai giải pháp Endpoint Security	G2, G3, G6	A3
Buổi 2 (5 tiết)	Bài thực hành 2: Tìm hiểu và triển khai giải pháp Gateway Security	G2, G3, G6	A3
Buổi 3 (5 tiết)	Bài thực hành 3: Tìm hiểu và triển khai công cụ dò tìm lỗ hổng trong hệ thống máy chủ và mạng.	G2, G3, G6	A3

Ghi chú: Hình thức thực hành đối với môn này là hình thức 2.

6. ĐÁNH GIÁ MÔN HỌC (Course assessment)

Bảng 5.

Thành phần đánh giá	**CĐRMH**	**Tỷ lệ (%)**
A1. Quá trình (Kiểm tra trên	G3, G4, G5, G6	20%

lớp, bài tập, đồ án, …)		
A2. Giữa kỳ		0%
A3. Thực hành	G3, G4	30%
A4. Cuối kỳ	G1, G2, G3, G4, G5	50%

7. QUY ĐỊNH CỦA MÔN HỌC (Course requirements and expectations)

- Quy định về giờ giấc, chuyên cần, kỷ luật trong khóa học: sinh viên đến lớp theo quy định chung của trường.
- Quy định liên quan đến các sự cố có thể xảy ra với bài thi, bài tập: theo quy định chung của trường.
- Quy định sử dụng phương tiện học tập: theo quy định chung của trường và của giáo viên.
- Sinh viên nghỉ quá 15% số buổi sẽ cấm thi.

8. TÀI LIỆU HỌC TẬP, THAM KHẢO

Tài liệu tham khảo

1. John A.Vacca (2010). *Network and system security*.
2. Brian Komar, Ronald Beekelaar and Joern Wettern (2003), Firewall for Dummies, 2nd edition.
3. Willam Stallings, Cryptography and network security, 5th edition.

9. PHẦN MỀM HAY CÔNG CỤ HỖ TRỢ THỰC HÀNH

1. VMWare workstation.

Tp.HCM, ngày 05 tháng 12 năm 2016

Trưởng khoa/bộ môn	**Giảng viên biên soạn**
(Ký và ghi rõ họ tên)	(Ký và ghi rõ họ tên)
TS. Nguyễn Gia Tuấn Anh	ThS. Nguyễn Duy