BỘ GIÁO DỤC VÀ ĐÀO TẠO
TRƯỜNG ĐẠI HỌC CẦN THƠ

ĐỀ CƯƠNG CHI TIẾT HỌC PHẦN

Học phần: An toàn hệ thống và an ninh mạng
(*System and Network Security*)

- Mã số: **CT434** ; Số tín chỉ: **3**
- Cấu trúc học phần: Số tiết: 60; gồm (LT: 30, TN: 30)

1. Thông tin giảng viên

Tên giảng viên: Thạc sĩ Nguyễn Công Huy
Đơn vị : Khoa Công Nghệ Thông Tin và Truyền Thông
Điện thoại : (84) 710 - 3734720 E-mail: nchuy@cit.ctu.edu.vn
Tên người cùng tham gia giảng dạy: Thạc sĩ Phạm Hữu Tài
Đơn vị : Khoa Công Nghệ Thông Tin và Truyền Thông
Điện thoại : (84) 710 - 3734721 E-mail: phtai@cit.ctu.edu.vn

2. Mã số HP tiên quyết: CT112

3. Nội dung:

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

- Giải thích được thế nào là an toàn hệ thống và an ninh mạng.
- Mô tả được các yêu cầu cơ bản cho 1 hệ thống mạng an toàn
- Trình bày được những nguy cơ, các đối tượng tấn công, các dạng tấn công và một số kỹ thuật xâm nhập hệ thống máy tính và mạng máy tính. Sử dụng được 1 số công cụ quét và kiểm tra hệ thống.
- Trình bày cách thức hoạt động của các phần mềm có hại 1 hệ thống máy tính, từ đó vận dụng các kỹ thuật để phòng chống và gia cố hệ thống.
- Hiểu được các kiến thức nền tảng về bảo mật như: mật mã, các thuật toán băm và thuật toán mã hóa, khóa bí mật và khóa công khai, chữ ký số, chứng chỉ số, hạ tầng khóa công khai...
- Trình bày và cài đặt được các cơ chế an toàn cho các thiết bị mạng. Cấu hình được các tính năng an toàn cơ bản cho các thiết bị mạng.
- Hiểu và xây dựng được các mô hình mạng an toàn.
- Hiểu và vận dụng được các giải pháp an toàn cho đường truyền mạng và các dịch vụ mạng trên Internet.
- Hiểu, vận dụng và cài đặt được một số kỹ thuật, giải pháp và công nghệ an ninh mạng phổ biến hiện nay như: chứng thực, mã hóa, tường lửa, mạng riêng ảo, hệ thống phát hiện xâm nhập.
- Hiểu được cách quản lý và điều hành một hệ thống mạng an toàn.

3.2. Phương pháp giảng dạy: giảng dạy 30 tiết lý thuyết trên lớp, thực hành 30 tiết trên các mô hình mạng giả lập.

3.3. Đánh giá học phần: Kiểm tra giữa kỳ : 40 %; Thi cuối kỳ: 60 %

4. Đề cương chi tiết: **Số tiết**

Chương I – Tổng quan về an toàn hệ thống và an ninh mạng 8

- Khái niệm an toàn mạng, sự cần thiết của an toàn mạng
- Các tiêu chí của 1 hệ thống mạng an toàn
- Các hình thức tấn công trên mạng
- Một số kỹ thuật tấn công trên mạng

- Các phần mềm có hại
- Mô hình AAA trong thiết kế hệ thống mạng an toàn.

Chương II – An toàn cho các thiết bị mạng 2

- Tầng vật lý
- Tầng liên kết dữ liệu
- Tầng mạng
- Tầng vận chuyển và tầng ứng dụng.

Chương III – Gia cố hệ thống 4

- Gia cố hệ điều hành mạng
- Gia cố ứng dụng
- Tổ chức chính sách an ninh mạng, có bước điều tra xâm nhập.

Chương IV – Căn bản về mật mã 2

- Kái niệm mật mã
- Các thuật toán mã hóa thông dụng hiện nay
- Khái niệm khóa bí mật và khóa công khai
- Ứng dụng của mật mã trong việc xây dựng dịch vụ mạng
- Chữ ký số và chứng chỉ số
- Quản lý khóa và chứng chỉ số, hạ tầng khóa công khai.

Chương V – An toàn trong truyền thông 6

- Giải pháp trong truy cập từ xa
- Giải pháp trong mạng không dây, mạng riêng ảo
- Các truy cập liên mạng.

Chương VI – Các mô hình mạng an toàn 2

- DMZ
- VLAN
- NAT

Chương VII – Tường lửa 2

- Khái niệm
- Phân loại tường lửa, các quy tắc, bộ lọc
- Giới thiệu một số tường lửa phổ biến hiện nay.

Chương VIII – Hệ thống phát hiện và ngăn ngừa xâm nhập 2

- Khái niệm - Phương thức hoạt động
- Giới thiệu một số hệ thống ngăn ngừa xâm nhập phổ biến hiện nay

Chương IX – Quản lý hệ thống an ninh mạng 2

- Phân quyền
- Quản lý rủi ro
- Tập huấn và lập tài liệu cho 1 hệ thống mạng an toàn.

Thực tập: Gồm 6 buổi theo các chủ đề sau 30

- Tấn công trên mạng
- Gia cố hệ thống
- Chữ ký số và chứng chỉ số
- An toàn cho các thiết bị mạng
- Tường lửa và hệ thống phát hiện xâm nhập
- VPN.

5. Tài liệu của học phần

1. Cisco networking academy program, *CCNA security*, 2009.
2. Michael Cross, Jeremy Faircloth, Eli Faskha, Michael Gregg, Alun Jones, Marc Perez, *Security+ : Study Guide and Practice Exam*, 2nd edition, Syngress, 2007.
3. Eric Maiwald, *Network security: A beginner's guide*, 2nd ed, McGraw-Hill, 2003.
4. Joseph Migga Kizza, *Computer network security*, Springer, 2005.
5. William Stallings, *Network security essentials: Applications and standards* , 2nd edition, Prentice Hall, 2003.