CƠ SỞ AN TOÀN THÔNG TIN

I. THÔNG TIN CHUNG

Tên học phần	**Cơ sở an toàn thông tin**
Tên tiếng Anh	The Basics of Information Security
Số tín chỉ	3
Số giờ học ở lớp	45 (45 LT)
Số giờ tự học ở nhà	45
Học phần học trước:	Lập trình căn bản, Hệ quản trị cơ sở dữ liệu, Mạng máy tính

II. MỤC TIÊU HỌC PHẦN

2.1. Mục tiêu chung

Học phần này cung cấp cho sinh viên các kiến thức tổng thể về an toàn thông tin như các hiểm họa an toàn thông tin, các phương pháp, kỹ thuật, công nghệ quan trọng để đảm bảo an toàn thông tin. Hình thành cho sinh viên các kỹ năng triển khai và vận hành các công nghê an toàn thông tin đơn giản, kỹ năng phân tích, nhận diện các hiểm họa an toàn thông tin cơ bản, kỹ năng thảo luận nhóm.

2.2. Mục tiêu cụ thể

Mục tiêu	Mô tả	**Chuẩn đầu ra CTĐT**
M1	Hiểu được các khái niệm cơ bản về an toàn thông tin	R8
M2	Có kiến thức về các hiểm họa an toàn thông tin cơ bản	R8
M3	Có kiến thức cơ bản về xác thực và kiểm soát truy cập	R8
M4	Có kiến thức cơ bản về các cơ chế an toàn trên các hệ điều hành Linux và windows	R8
M5	Có kiến thức về các phương pháp cơ bản trong đảm bảo an toàn thông tin sử dụng mật mã	R8
M6	Có kiến thức về các công nghệ an toàn mạng cơ bản	R8
M7	Hiểu biết cơ bản về các tiêu chuẩn, chính sách, pháp lý trong quản lý an toàn thông tin	R8
M8	Có kiến thức cơ bản về an toàn vật lý	R8
M9	Nhận diện được các hiểm họa an toàn thông tin đơn giản và xác định các biện pháp đảm bảo an toàn thông tin tương ứng	R8, R14

III. MÔ TẢ HỌC PHẦN

Học phần này cung cấp cho sinh viên các kiến thức cơ bản và tổng thể về an toàn thông tin, bao gồm: Các khái niệm cơ bản về an toàn thông tin, các hiểm họa an toàn thông tin điển hình, các phương pháp xác thực và kiểm soát truy cập cơ bản, các phương pháp đảm bảo an toàn thông tin dựa trên mật mã, các công nghệ điển hình để đảm bảo an toàn mạng, các kiến thức về chính sách và pháp lý trong an toàn thông tin, các biện pháp an toàn vật lý

IV. CHƯƠNG TRÌNH CHI TIẾT HỌC PHẦN

Chương 1: Tổng quan về an toàn thông tin (3LT)

1.1. Khái niệm về an toàn thông tin
1.2. Các thuộc tính của thông tin
1.3. Một số thuật ngữ quan trọng
1.4. Mô hình CNNS
1.5. Các thành phần của hệ thống thông tin
1.6. Sự cân bằng giữa an toàn thông tin và truy cập
1.7. Các biện pháp đảm bảo an toàn thông tin
1.8. Các nguyên tắc trong đảm bảo an toàn thông tin
1.9. Vòng đời phát triển hệ thống tin an toàn

Chương2: Hiem hoa, tan cong, hiểm họa an toàn thông tin (6LT)

2.1. Phân loại về các hiểm họa an toàn thông tin
2.2. Hiểm họa tấn công bằng kỹ nghệ xã hội
2.3. Hiểm họa tấn công bằng mã độc
2.4. Hiểm họa tấn công khai thác lô hổng phần mềm
2.4. Hiểm họa tấn công người đứng giữa (Man in midle attacks)
2.5. Hiểm họa tấn công giả mạo
2.6. Hiểm họa tấn công dùng lại
2.7. Hiểm họa tấn công từ chối dịch vụ
2.9. Hiểm họa tấn công APT
2.9. Hiểm họa vật lý và từ thiên nhiên

Chương 3: Định danh và xác thực (6LT)

3.1. Khái niệm định danh và xác thức
3.2. Định danh và xác thực dựa trên username và password
3.3. Xác thực dựa trên password
3.4. Xác thực dựa trên mật mã
3.5. Các phương pháp xác thực khác

Chương 4: Kiểm soát truy cập (6LT)

4.1. Các khái niệm chung
4.2. Mô hình kiểm soát truy cập tùy ý (DAC)
4.3. Mô hình kiểm soát truy bắt buộc (MAC)
4.4. Mô hình kiểm soát truy cập dựa trên vai trò (RBAC)
4.5.Một số mô hình kiểm soát truy cập khác

Chương 5: Cơ chế an toàn hệ điều hành (6LT)

5.1. Các cơ chế chung
5.2. Cơ chế an toàn hệ điều hành Linux
5.3. Cơ chế an toàn hệ điều hành windows

Chương 6. Đảm bảo an toàn thông tin bằng mật mã (6LT)

6.1. Mã hóa thông tin

6.2. Xác thực thông tin

6.3. Chứng chỉ số và hạ tầng khóa công khai

6.4. Bảo mật truyền thông

6.5. Công nghệ VPN

Chương 7. An toàn mạng (9LT)

7.1. Tổng quan về an toàn mạng

7.2. An toàn trên thiết bị Switch

7.3. An toàn trên thiết bị Router

7.4. Công nghệ tường lửa

7.5. Công nghệ phát hiện xâm nhập trái phép

7.6. Công nghệ giám sát an toàn mạng

Chương 8. Quản lý an toàn thông tin (6LT)

8.1. Bộ tiêu chuẩn quản lý an toàn thông tin ISO 27001

8.2. Quản lý rủi ro an toàn thông tin

8.3. Chính sách an toàn thông tin

8.4. Quy trình an toàn thông tin

8.5. Pháp lý an toàn thông tin

Chương 9. An toàn vật lý (3LT)

9.1. Kiểm soát truy cập

9.2. Môi trường vật lý an toàn

9.3. Phục hồi thảm họa

9.4. Liên tục hoạt động

9.5. Quản lý đặc quyền

V. KẾ HOẠCH GIẢNG DẠY

Giải thích ký hiệu: LT – lý thuyết; BT – bài tập/thảo luận; TH – Thực hành; ON – tự học ở nhà

TT	Nội dung và phương pháp dạy học	Mục tiêu	LT	BT	TH	ON
1	***Chương 1. Tổng quan về an toàn thông tin*** **Giảng dạy trên lớp** - Khái niệm về an toàn thông tin - Một số thuật ngữ quan trọng (Điểm yếu, hiểm họa, tấn công, rủi ro) - Các thuộc tính của thông tin - Mô hình CNNS - Các thành phần của hệ thống thông tin - Sự cân bằng giữa an toàn thông tin và truy cập - Các biện pháp đảm bảo an toàn thông tin - Các nguyên tắc trong đảm bảo an toàn thông tin	M1	3	0	0	6

TT	Nội dung và phương pháp dạy học	Mục tiêu	LT	BT	TH	ON
	- Vòng đời phát triển hệ thống tin an toàn **Phương pháp giảng dạy chính** - Thuyết giảng - Trình chiếu Powerpoint - Tương tác với sinh viên **Tài liệu tham khảo** [1, Chapter 3]; [5, Chapter 1] **Tự học ở nhà** - Đọc thêm: Tình hình an toàn thông tin tại Việt Nam và thế giới trong thời gian gần đây [6] - Độc thêm: Các khái niệm liên quan đến an toàn thông tin [6]					
2	***Chương 2. Các hiểm họa an toàn thông tin*** **Giảng dạy trên lớp** - Hiểm họa tấn công bằng kỹ nghệ xã hội - Tấn công bằng mã độc - Tấn công khai thác lô hổng phần mềm - Tấn công người đứng giữa (Man in midle attacks) - Tấn công giả mạo - Tấn công dùng lại - Tấn công từ chối dịch vụ - Tấn công APT - Hiểm họa vật lý và từ thiên nhiên **Phương pháp giảng dạy chính** - Trình chiếu Powerpoint - Thuyết giảng - Minh họa, thảo luận về một số tấn công cơ bản - Làm mẫu **Tài liệu tham khảo** [1, Chapter 2]; [5, Chapter 2] **Tự học ở nhà** - Tìm hiểu thêm về các tấn công [7] - Thực hành, thử nghiệm một số tấn công: SQL Injection, Buffer Overflow [7]	M2, M9	6	0	0	12
3	***Chương 3. Định danh và xác thực***	M3, M9	6	0	0	12

TT	Nội dung và phương pháp dạy học	Mục tiêu	LT	BT	TH	ON
	Giảng dạy trên lớp - Khái niệm định danh và xác thức - Định danh và xác thực dựa trên username và password - Xác thực dựa trên password - Xác thực dựa trên mật mã - Các phương pháp xác thực khác **Phương pháp giảng dạy chính** - Trình chiếu Powerpoint - Thuyết giảng - Thảo luận nhóm **Tài liệu tham khảo** [1, Chapter 4] **Tự học ở nhà** - Xem lại và tóm tắt ngắn ngọn nội dung của chương - Đọc thêm về các giao thức xác thực Kerborose, PAP, CHAP [3]					
4	***Chương 4. Kiểm soát truy cập*** **Giảng dạy trên lớp** - Các khái niệm chung - Mô hình kiểm soát truy cập tùy ý (DAC) - Mô hình kiểm soát truy bắt buộc (MAC) - Mô hình kiểm soát truy cập dựa trên vai trò (RBAC) - Một số mô hình kiểm soát truy cập khác **Phương pháp giảng dạy chính** - Thuyết giảng - Minh họa các mô hình kiểm soát truy cập trên công nghệ cụ thể - Trình chiếu Powerpoint **Tài liệu tham khảo** [1, Chương 5] **Tự học ở nhà** - Xem lại và tóm tắt ngắn ngọn nội dung của chương - Thực hiện bài Lab: Role-Based Access Control [7] - Thực hiện bài Lab: DAC LAB [7]	M3, M9	6	0	0	12
5	***Chương 5. Các cơ chế an toàn hệ điều hành***	M4, M9	6	0	0	12

TT	Nội dung và phương pháp dạy học	Mục tiêu	LT	BT	TH	ON
	Giảng dạy trên lớp - Các cơ chế chung - Cơ chế an toàn hệ điều hành Linux - Cơ chế an toàn hệ điều hành windows **Phương pháp giảng dạy chính** - Thuyết giảng - Minh họa các cơ chế an toàn trên hệ điều hành Linux - Trình chiếu Powerpoint - Thảo luận nhóm **Tài liệu tham khảo** [1, Chapters 6, 7,8] **Tự học ở nhà** - Đọc thêm về các dịch vụ an toàn trên hệ điều hành Windows [4] - Thực hiện bài Lab: Linux Capability Exploration [7]					
6	***Chương 6.*** *Đảm bảo an toàn thông tin bằng mật mã* **Giảng dạy trên lớp** - Mã hóa thông tin - Xác thực thông tin - Chứng chỉ số và hạ tầng khóa công khai - Bảo mật truyền thông - Công nghệ VPN **Phương pháp giảng dạy chính** - Trình chiếu Powerpoint - Thuyết giảng - Minh họa, thảo luận về việc sử dụng chứng chỉ số - Làm mẫu **Tài liệu tham khảo** [1, Chapters 15,16] **Tự học ở nhà** - Đọc và thử nghiệm dịch vụ mã hóa EFS của windows[4] - Đọc và thử nghiệm công cụ BoxCryptor - Cài đặt chứng chỉ số để bảo mật web[4]	M5,M9	6	0	0	12
7	***Chương 7.*** *An toàn mạng*	M6, M9	9	0	0	18

TT	Nội dung và phương pháp dạy học	Mục tiêu	LT	BT	TH	ON
	Giảng dạy trên lớp - Tổng quan về an toàn mạng - An toàn trên thiết bị Switch - An toàn trên thiết bị Router - Công nghệ tường lửa - Công nghệ phát hiện xâm nhập trái phép - Công nghệ giám sát an toàn mạng **Phương pháp giảng dạy chính** - Trình chiếu Powerpoint - Thuyết giảng - Minh họa hoạt động của các công nghệ - Làm mẫu **Tài liệu tham khảo** [1, Chapter17]; [4, Chương 2] **Tự học ở nhà** - Nghiên cứu tập luật của Snort, cài đặt thử nghiệm - Nghiên cứu hoạt động của Iptable, cài đặt thử nghiệm - Cài đặt thử nghiệm các ACL cho Router sử dụng công cụ mô phỏng GNS3					
8	***Chương 8.*** *Quản lý an toàn thông tin* **Giảng dạy trên lớp** - Bộ tiêu chuẩn quản lý an toàn thông tin ISO 27001 - Quản lý rủi ro an toàn thông tin - Chính sách an toàn thông tin - Quy trình an toàn thông tin - Pháp lý an toàn thông tin **Phương pháp giảng dạy chính** - Trình chiếu Powerpoint - Thuyết giảng - Minh họa, thảo luận về việc sử dụng chứng chỉ số - Làm mẫu **Tài liệu tham khảo** [1, Chapter 2]; [4, Chapters 3,4,5] **Tự học ở nhà** - Đọc thêm về bộ tiêu chuẩn TCVN 10295: 2014	M7, M9	6	0	0	12

TT	Nội dung và phương pháp dạy học	Mục tiêu	LT	BT	TH	ON
	- Đọc Luật An toàn thông tin mạng năm 2016 - Độc Luật an An ninh mạng năm 2018					
9	***Chương 9.*** *An toàn vật lý* **Giảng dạy trên lớp** - Kiểm soát truy cập - Môi trường vật lý an toàn - Phục hồi thảm họa - Liên tục hoạt động - Quản lý đặc quyền **Phương pháp giảng dạy chính** - Trình chiếu Powerpoint - Thuyết giảng - Minh họa, thảo luận về một số cơ chế an toàn vật lý **Tài liệu tham khảo** [4, Chapter 9] **Tự học ở nhà** - Đọc thêm về các kỹ thuật tấn công vật lý [6] - Củng cố các kiến thức đã học trên lớp [4, Chapter 9]	M8, M9	3	0	0	6
	Tổng		**45**	**0**	**0**	**90**

VI. GIÁO TRÌNH VÀ TÀI LIỆU THAM KHẢO

6.1. Giáo trình và tài liệu tham khảo chính:

[1] Dieter Gollmann, Computer Security, Hamburg Uninersity of Technology

6.2. Tài liệu tham khảo khác:

[2] Lê Đình Vinh, Trần Đức Sự, Vũ Thị Vân, Giáo trình Cơ sở an toàn thông tin, NXB Thông tin & Truyền thông, 2013.
[3] Nguyễn Quốc Toàn, Hoàng Sỹ Tương, Giáo trình Giao thức an toàn mạng, NXB Thông tin & Truyền thông, 2013.
[4] Lương Thế Dũng, Cao Minh Tuấn, Giáo trình Quản trị an toàn hệ thống, NXB Thông tin & Truyền thông, 2013.
[5] Michael Whitman, Principles of Information Security, Cengage Learning; 4 edition (January 1, 2011)
[6]. http://antoanthongtin.vn
[7]. http://www.cis.syr.edu/~wedu/seed/

6.3. Giảng đường cho các buổi học lý thuyết

- Máy chiếu
- Bảng viết

6.4. Phòng máy cho các buổi học thực hành

- Máy chiếu

– Máy tính chạy hệ điều hành Windows, cài đặt bộ công cụ mã nguồn mở weka

VII. ĐÁNH GIÁ KẾT QUẢ HỌC TẬP

7.1. Chấm điểm

Điểm đánh giá	Căn cứ đánh giá	Công thức tính
Điểm chuyên cần	Đi học đầy đủ, tham gia xây dựng bài; Kết quả các bài thực hành	(1)
Điểm thi giữa kỳ	Bài thi giữa kỳ	(2)
Điểm quá trình	(1), (2)	(3) = 0,3×(1) + 0,7×(2)
Điểm thi kết thúc học phần	Bài thi kết thúc học phần	(4)
Điểm học phần	(3), (4)	(5) = 0,3×(3) + 0,7×(4)

7.2. Điều kiện để được thi kết thúc học phần

– Dự lớp tối thiểu 75% số giờ học

– Điểm quá trình đạt tối thiểu 4,0 (thang điểm 10)

7.3. Hình thức thi kết thúc học phần

Tự luận hoặc Trắc nghiệm (Lý thuyết + Bài tập)