TRƯỜNG ĐẠI HỌC CÔNG NGHỆ
KHOA CÔNG NGHỆ THÔNG TIN
------📖------

CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM
Độc lập - Tự do - Hạnh phúc
==========

ĐỀ CƯƠNG CHI TIẾT
HỌC PHẦN: THỰC HÀNH AN NINH MẠNG

(Ban hành kèm theo Quyết định số /QĐ-ĐHCN ngày tháng năm 20.....
của Hiệu trưởng Trường Đại học Công nghệ)

1. Thông tin về các giảng viên học phần

STT	Họ và tên	Chức danh, học vị	Địa chỉ liên hệ	Điện thoại/Email	Ghi chú
1	Nguyễn Đại Thọ	TS	Khoa CNTT	nguyendaitho@vnu.edu.vn	Trưởng học phần
2	Lê Thị Hợi	TS	Khoa CNTT	hoi.le@vnu.edu.vn	Giảng viên

2. Thông tin chung về học phần

- Tên học phần:
  + Tiếng Việt: Thực hành an ninh mạng
  + Tiếng Anh: Practical Network Security
- Mã số môn học: INT3317
- Số tín chỉ: 3
- Giờ tín chỉ đối với các hoạt động (LT/ThH/TH): 30/30/0
- Môn học tiên quyết: INT2213 – Mạng máy tính
- Các yêu cầu đối với môn học (nếu có):
- Bộ môn, Khoa phụ trách môn học: Bộ môn M&TTMT, Khoa CNTT

3. Mục tiêu học phần

Học phần cung cấp cho học viên những kiến thức và kỹ năng sau đây:

- Mô tả các vấn đề an ninh chung có thể phát sinh khi sử dụng các mạng viễn thông và dữ liệu để truyền thông tin
- Phân tích các vấn đề an ninh mạng, nhận biết và xác định các yêu cầu cần phải đáp ứng
- Nhận biết và giải quyết các vấn đề an ninh mạng trên cơ sở áp dụng các kiến thức đã học, sử dụng các công cụ và kỹ thuật phù hợp

- Sử dụng các kỹ thuật, kỹ năng và công cụ tiên tiến cần thiết để đảm bảo an ninh mạng, hiểu rõ những hạn chế của chúng

4. Chuẩn đầu ra

Mục tiêu / Nội dung	Bậc 1	Bậc 2	Bậc 3	Bậc 4
1. Kiến thức				
1.3 Kiến thức chung của khối ngành (M3)				
1.3.2 Hiểu được đặc thù chuyên nghiệp trong công nghệ, phân biệt được những nét đặc trưng của yêu cầu chuyên nghiệp trong công nghệ	X			
1.4 Kiến thức chung của nhóm ngành (M4)				
1.4.6 Hiểu các khái niệm cơ bản về mạng máy tính, các bộ phận, các giao thức, cách thức truyền dữ liệu trên mạng			X	
1.5 Kiến thức của ngành và bổ trợ (M5)				
1.5.3 Vận dụng được các kiến thức trong lĩnh vực quản trị mạng			X	
1.5.4 Hiểu và vận dụng được kiến thức chuyên sâu theo định hướng "Mạng máy tính" bao gồm các chuyên đề về quản trị mạng, thực hành an ninh mạng, mạng không dây, truyền thông đa phương tiện, lập trình mạng, …			X	
1.5.5 - Hiểu và vận dụng được kiến thức chuyên sâu theo định hướng "Truyền thông", bao gồm các chuyên đề về mạng không dây, mạng quang, thiết kế và quản trị mạng viễn thông, mã hóa, …			X	
2. Kỹ năng				
2.1 Kỹ năng cứng				
2.1.1 Các kỹ năng nghề nghiệp				
2.1.1.1 Vận dụng các kiến thức cơ bản về Toán và Vật lý trong khoa học công nghệ và đời sống	X			
2.1.1.5 Biết tìm kiếm, cập nhật, tổng hợp, khai thác thông tin		X		
2.1.1.6 Đọc hiểu tài liệu tiếng Anh chuyên ngành		X		
2.1.1.8 Biết sử dụng các kiến thức chuyên môn một cách linh hoạt		X		
2.1.2 Kỹ năng lập luận tư duy và giải quyết vấn đề				
2.1.2.1 Có kỹ năng phát hiện vấn đề		X		
2.1.2.2 Có kỹ năng đánh giá và phân tích vấn đề		X		
2.1.2.3 Có kỹ năng giải quyết vấn đề chuyên môn		X		
2.1.2.4 Có kỹ năng mô hình hóa		X		
2.1.3 Kỹ năng nghiên cứu và khám phá kiến thức				
2.1.3.2 Có kỹ năng dùng thực nghiệm để khám phá kiến thức		X		
2.1.3.4 Có kỹ năng áp dụng kiến thức vào thực tế		X		
2.1.4 Kỹ năng tư duy theo hệ thống				
2.1.4.1 Có tư duy logic		X		
2.1.4.2 Có tư duy phân tích, tổng hợp		X		
2.1.4.3 Có tư duy toàn cục		X		
2.1.5 Hiểu bối cảnh xã hội và ngoại cảnh				

Mục tiêu / Nội dung	Bậc 1	Bậc 2	Bậc 3	Bậc 4
2.1.5.1 Hiểu biết bối cảnh xã hội và cơ quan	X			
2.1.5.2 Nhận thức được vai trò và trách nhiệm của cá nhân với xã hội và cơ quan công tác	X			
2.1.5.3 Biết nắm bắt nhu cầu xã hội đối với kiến thức khoa học chuyên ngành	X			
2.1.7 Năng lực vận dụng kiến thức, kỹ năng vào thực tiễn				
2.1.7.1 Có năng lực phân tích yêu cầu	X			
2.1.7.2 Có năng lực thiết kế giải pháp	X			
2.2 Kỹ năng mềm				
2.2.1. Các kỹ năng cá nhân				
2.2.1.1 Có tư duy sáng tạo	X			
2.2.1.2 Có tư duy phản biện		X		
2.2.1.3 Biết đề xuất sáng kiến		X		
2.2.4. Kỹ năng giao tiếp				
2.2.4.1 Biết cách lập luận, sắp xếp ý tưởng		X		
3. Về phẩm chất đạo đức				
3.1 Phẩm chất đạo đức cá nhân				
3.1.1 Trung thực		X		
3.1.4 Nhiệt tình		X		

5. Tóm tắt nội dung học phần

Môn học cung cấp kiến thức tổng quan và chuyên sâu về các hiểm họa đối với các hệ thống máy tính kết nối với mạng Internet, giới thiệu các giải pháp, các công cụ an ninh, các khuyến nghị và các thông lệ có thể áp dụng để đảm bảo an toàn thông tin. Các bài giảng định hướng ứng dụng và các bài thực hành theo các tình huống giả định sát với thực tiễn chuẩn bị cho sinh viên các kiến thức và kỹ năng cần thiết để sẵn sàng đối phó với bất kỳ thách thức nào đối với an ninh các hệ thống mạng và máy tính. Sinh viên được hướng dẫn sử dụng các công cụ phần cứng, phần mềm an ninh theo hình thức thực nghiệm quy trình dễ hiểu và dễ thực hiện.

6. Nội dung chi tiết học phần

Chương 1. Giới thiệu

1.1. Khái niệm an toàn thông tin
1.2. Các tác nhân gây ra các hiểm họa an ninh
1.3. Các lỗ hổng và các tấn công

Chương 2. Các hiểm họa và tấn công phía đầu cuối

2.1. Các tấn công sử dụng mã độc
2.2. Các tấn công mức ứng dụng
2.3. Trí tuệ nhân tạo đối địch

Chương 3. An ninh đầu cuối và phát triển ứng dụng

3.1. Các nguồn tình báo hiểm họa
3.2. Đảm bảo an toàn các máy tính đầu cuối
3.3. Tạo lập và triển khai SecDevOps

Chương 4. Mật mã học cơ bản

4.1. Định nghĩa mật mã học
4.2. Các giải thuật mật mã
4.3. Các tấn công và phòng thủ mật mã
4.4. Sử dụng mật mã học

Chương 5. Cơ sở hạ tầng khóa công khai và các giao thức mật mã

5.1. Các chứng thực số
5.2. Cơ sở hạ tầng khóa công khai
5.3. Các giao thức mật mã
5.4. Cài đặt mật mã học

Chương 6. Các hiểm họa, đánh giá và phòng thủ mạng

6.1. Các tấn công mạng
6.2. Các công cụ đánh giá và phòng thủ
6.3. Các điều khiển an ninh vật lý

Chương 7. Các thiết bị và công nghệ an ninh mạng

7.1. Các thiết bị an ninh
7.2. Các công nghệ an ninh

Chương 8. An ninh đám mây và an toàn ảo hóa

8.1. An ninh đám mây
8.2. An toàn ảo hóa
8.3. Các giao thức mạng an toàn

Chương 9. Xác thực

9.1. Các kiểu chủ thể xác thực
9.2. Các giải pháp xác thực

Chương 10. Chuẩn bị, phản ứng và điều tra sự cố

10.1. Chuẩn bị trước sự cố
10.2. Phản ứng với sự số
10.3. Điều tra sự cố

7. Học liệu

7.1. Học liệu bắt buộc

[1] Mark Ciampa, *CompTIA Security+ Guide to Network Security Fundamentals, Seventh Edition*, Cengage, 2022.

[2] Jonathan S. Weissman, *Principles of Computer Security: CompTIA Security+ and Beyond Lab Manual (Exam SY0-601)*, McGraw-Hill, 2021.

7.2 Học liệu tham khảo

[3] William Stallings. *Cryptography and Network Security: Principles and Practice, Eighth Edition*. Pearson, 2019.

[4] Andrew Hurd, *CompTIA Security+ Guide to Network Security Fundamentals, Lab Manual, Sixth Edition*, Cengage, 2018.

[5] CTFtime team, *https://ctftime.org*, All about CTF (Capture The Flag).

8. Hình thức tổ chức dạy học

8.1. Phân bổ lịch trình giảng dạy trong 1 học kỳ (15 tuần)

Hình thức dạy	Số tiết/tuần	Từ tuần …đến tuần…	Địa điểm
Lý thuyết	2	1 - 15	Giảng đường
Thực hành	2	1 - 15	Giảng đường
Tự học bắt buộc			

8.2 Lịch trình dạy cụ thể

Tuần	***Nội dung giảng dạy lý thuyết/thực hành***	***Nội dung sinh viên tự học***
1	Chương 1	• Đọc thêm Module 1 (Introduction to Security) trong giáo trình [1] • Làm các bài tập thực hành Lab Exercise 1.04 (Building the Virtual Lab), Lab Exercise 2.02 (Linux File System Management), Lab Exercise 2.03 (Linux Systems Administration) và Lab Exercise 2.04 (Linux System Security) trong tài liệu [2]
2	Chương 2	• Đọc thêm Module 3 (Threats and Attacks on Endpoints) trong giáo trình [1] • Làm các bài tập thực hành Chapter 15 (Types of Attacks and Malicious Software) trong tài liệu [2]
3, 4	Chương 3	• Đọc thêm Module 4 (Endpoint and Application Development Security) trong giáo trình [1] • Làm các bài tập thực hành Chapter 14 (System Hardening and Baselines) và Chapter 19 (Secure Software Development) trong tài liệu [2]
5	Chương 4	• Đọc thêm Module 6 (Basic Cryptography) trong giáo trình [1] • Làm các bài tập thực hành Project 6-1 (Using OpenPuff Steganography), Project 6-2 (Running an RSA Cipher Demonstration), Project 6-3 (Installing GUI Hash Generator and Comparing Digests), Project 6-4 (Using Microsoft's Encrypting File System) và Project 6-6 (Blockchain Tutorial) trong giáo trình [1] • Làm bài tập thực hành Lab Exercise 6.04 (E-mail Cryptography) trong tài liệu [2]

6	Chương 5	• Đọc thêm Module 7 (Public Key Infrastructure and Cryptographic Protocols) trong giáo trình [1] • Làm các bài tập thực hành Lab Exercise 7.01 (DNSSEC for Security) và Lab Exercise 7.02 (DNSSEC for Exploiting)
7, 8	Chương 6	• Đọc thêm Module 8 (Networking Threats, Assessments, and Defenses) trong giáo trình [1] • Làm các bài tập thực hành Chapter 13 (Intrusion Detection Systems and Network Security) và Chapter 16 (Security Tools and Techniques) trong tài liệu [2]
9, 10	Chương 7	• Đọc thêm Module 9 (Network Security Appliances and Technologies) trong giáo trình [1] • Làm các bài tập thực hành Chapter 9 (Network Fundamentals) và Chapter 10 (Infrastructure Security) trong tài liệu [2]
11	Chương 8	• Đọc thêm Module 10 (Cloud and Virtualization Security) trong giáo trình [1] • Làm các bài tập thực hành Chapter 17 (Web Components, E-mail, and Instant Messaging) trong tài liệu [2]
12, 13	Chương 9	• Đọc thêm Module 12 (Authentication) trong giáo trình [1] • Làm các bài tập thực hành Chapter 11 (Authentication and Remote Access) trong tài liệu [2]
14, 15	Chương 10	• Đọc thêm Module 13 (Incident Preparation, Response, and Investigation) trong giáo trình [1] • Làm các bài tập thực hành Lab Exercise 22.02 (Metasploit Framework), Lab Exercise 22.03 (Metasploit's Meterpreter), Lab Exercise 22.04 (Armitage) và Chapter 23 (Computer Forensics) trong tài liệu [2]

9. Chính sách đối với môn học và các yêu cầu khác của giảng viên

- Sinh viên làm bài tập trên lớp theo sự hướng dẫn của giáo viên, nếu còn bài tập nào chưa hoàn thành thì phải tiếp tục thực hiện ở nhà.
- Kết quả các bài tập thực hành hoàn thành trên lớp được giáo viên đánh giá thông qua quan sát trực tiếp.
- Kết quả thực hiện các bài tập ở nhà được đánh giá thông qua báo cáo viết nộp qua Website môn học.
- Sinh viên nào sao chép hoặc cố ý cho bạn sao chép bài tập thực hành sẽ bị 0 điểm cho phần đánh giá này.

- Các sinh viên bị 0 điểm bài tập thực hành sẽ bị cấm thi học kỳ đồng nghĩa với nhận 0 điểm tổng kết môn học.

10. Phương pháp, hình thức kiểm tra, đánh giá kết quả học tập môn học

10.1. Mục đích và trọng số kiểm tra, đánh giá

Hình thức	Phương pháp	Mục đích	Trọng số
Bài tập thực hành	Làm trên lớp theo hướng dẫn của giáo viên và tiếp tục hoàn thành ở nhà	Đánh giá khả năng vận dụng kiến thức môn học vào thực tế của sinh viên	40%
Thi kết thúc môn học	Thi trắc nghiệm trên máy tính	Đánh giá kiến thức, kỹ năng sinh viên đạt được khi kết thúc môn học	60%
Tổng			**100%**

10.2. Tiêu chí đánh giá

- Tiêu chí đánh giá chung:

TT	***Yêu cầu***	***Điểm đạt được***	***Ghi chú***
1	Hoàn thành tốt các yêu cầu đề ra, thể hiện khả năng vận dụng thành thạo các kiến thức đã học	9-10	
2	Hoàn thành cơ bản các yêu cầu đề ra, thể hiện khả năng vận dụng cơ bản các kiến thức đã học	7-8	
3	Hoàn thành khoảng 50-60% các yêu cầu đề ra, mới dừng lại ở mức mô tả lại kiến thức đã học	5-6	
4	Hoàn thành dưới 50% yêu cầu đề ra, trên 50% yêu cầu quan trọng chưa đạt	1-4	

- Tiêu chí đánh giá cụ thể với từng đầu điểm của môn học:

+ Bài tập thực hành: Sinh viên thực hiện đầy đủ các bước thực hành theo hướng dẫn trong đề bài của mỗi bài tập, trả lời tất cả các câu hỏi bao gồm các câu hỏi trong phần hướng dẫn, các câu hỏi tự luận và điền từ cuối mỗi bài tập.

+ Kết thúc môn: Sinh viên hiểu và vận dụng được các kiến thức và kỹ năng đã học, chú trọng vào 4 chương nội dung chính về an toàn và an ninh mạng, đặc biệt theo các dạng bài tập đã được hướng dẫn và rèn luyện thông qua các buổi chữa bài tập trên lớp

- Cụ thể việc đánh giá kiến thức, kỹ năng của sinh viên theo các mức đáp ứng được chuẩn đầu ra, mức khá, mức giỏi:

Tùy vào mức độ hoàn thành các bài tập và thi cuối kỳ mà sinh viên sẽ được phân loại thành trung bình, khá, và giỏi.

- Giỏi: Hoàn thành hết các bài tập thực hành (hoặc tích cực tham gia các hoạt động trên lớp để tích lũy số điểm thưởng tương ứng) và giải quyết tốt câu hỏi thi với mức độ hoàn thiện cao

- Khá: Hoàn thành được các bài tập thực hành và làm được các câu hỏi thi cơ bản, chưa giải quyết được một số nội dung khó hoặc chưa hoàn thiện
- Trung bình: Còn một số nội dung chưa làm được.

10.3. Lịch thi và kiểm tra

Hình thức thi và kiểm tra	**Thời gian**
Bài tập thực hành	Nộp báo cáo thực hành vào tuần 13
Thi cuối kỳ	Theo lịch của Trường

Duyệt **Chủ nhiệm Khoa** **Chủ nhiệm bộ môn**