TRƯỜNG ĐẠI HỌC VĂN HIẾN
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

1. Thông tin về học phần

- Tên học phần: AN TOÀN MẠNG MÁY TÍNH NÂNG CAO (ADVANCED NETWORK SECURITY)
- Mã học phần: INT564
- Số tín chỉ: 03 (2/1/4)
- Bậc đào tạo: Đại học
- Loại học phần: Bắt buộc
- Học phần tiên quyết/ Học phần trước: An toàn mạng máy tính, Tổ chức và quản trị các dịch vụ mạng.
- Đơn vị phụ trách: Khoa Công nghệ thông tin
- Số giờ tín chỉ: 60, trong đó:
- Lý thuyết: 30 (1 tín chỉ LT = 15 tiết)
- Thực hành: 30 (1 tín chỉ TH = 30 tiết)
- Thực tập: 00 (1 tín chỉ TT = 60 giờ TT tại cơ sở)
- Đồ án/ Khóa luận 00 (1 tín chỉ ĐA/KL = 45 giờ làm ĐA/KL)

2. Thông tin về giảng viên

Giảng viên 1:

- Họ và tên: .....
- Chức danh, học vị: .....
- Thời gian làm việc: Giờ hành chính (8:00 -16:00)
- Địa điểm làm việc: Khoa ….. - Trường Đại học …..
- Điện thoại: .....
- Email: .....

Giảng viên 2:

- Họ và tên: .....
- Chức danh, học vị: .....
- Thời gian làm việc: Giờ hành chính (8:00 -16:00)
- Địa điểm làm việc: Khoa ….. - Trường Đại học …..
- Điện thoại: .....
- Email: .....

3. Tóm tắt nội dung học phần

Học phần gồm 06 chương, cung cấp cho người học kiến thức tổng quát về an toàn thông tin và được giải thích về những vị trí cần thiết để thiết lập phòng thủ nhằm giúp người học hiểu được sự cần thiết và chọn cơ chế phù hợp để nâng cao hiệu quả trong an

toàn mạng máy tính. Người học được giới thiệu cơ bản về các công nghệ và hệ thống cũng như các kỹ thuật an toàn mạng: tường lửa, mạng riêng ảo, hệ thống phát hiện và ngăn chặn xâm nhập, … Ngoài ra, học phần còn giới thiệu thêm về hệ thống Honeynet.

4. Mục tiêu của học phần

Học phần có những mục tiêu:

- Cung cấp cho người học những kiến thức chung về an toàn thông tin.
- Cung cấp cho người học kiến thức về các công nghệ, hệ thống và kỹ thuật an toàn mạng.
- Trang bị kiến thức cần thiết về việc triển khai, cấu hình và sử dụng tường lửa, mạng riêng ảo, hệ thống phát hiện và ngăn chặn xâm nhập, hệ thống quản lý sự kiện và thông tin an toàn, hệ thống Honeynet.
- Phát triển kỹ năng phân tích, lập luận và thuyết trình hiệu quả.

5. Chuẩn đầu ra của học phần:

Mã CĐR	**Nội dung chuẩn đầu ra** (Bắt đầu bằng động từ theo thang Bloom)
Kiến thức	
CLO1	Trình bày được tầm quan trọng của việc đảm bảo an toàn mạng máy tính
CLO2	Hiểu được vai trò và chức năng của các công nghệ và hệ thống an toàn trong mạng máy tính
CLO3	Giải thích được vị trí triển khai của các công nghệ và hệ thống an toàn trong mạng máy tính
Kỹ năng	
CLO4	Triển khai, cấu hình và sử dụng được các công nghệ, hệ thống an toàn trong mạng máy tính
CLO5	Tham gia làm việc nhóm, trao đổi và đóng góp ý kiến
Mức độ tự chủ và trách nhiệm	
CLO6	Có ý thức đóng góp để xây dựng các biện pháp an toàn mạng và có thói quen học tập suốt đời

Ma trận liên kết giữa Chuẩn đầu ra chương trình đào tạo và Chuẩn đầu ra học phần

Chuẩn đầu ra	**PLO1**	**PLO2**	**PLO3**	**PLO4**	**PLO5**	**PLO6**	**PLO7**	**PLO8**	**PLO9**	**PLO10**
CLO1	X	X								
CLO2	X	X	X	X						
CLO3	X	X	X	X						
CLO4			X	X	X	X	X	X		
CLO5					X	X	X			
CLO6									X	X

***Ghi chú: PLOs** (ProgrammeLearningOutcomes): Chuẩn đầu ra cấp CTĐT*
***CLOs** (CourseLearningOutcomes): Chuẩn đầu ra học phần*

6. Nội dung chi tiết của học phần

6.1. Lý thuyết

Chương	Nội dung	Đáp ứng CLOs
Chương 1	**Tổng quan về đảm bảo an toàn mạng máy tính**	**CLO1, CLO5**
1.1	An toàn mạng máy tính là gì?	
1.2	Những gì cần được bảo vệ	
1.3	Mục đích và cách đánh giá mức độ an toàn mạng	
1.4	Sự cần thiết của việc viết lại chính sách và người chịu trách nhiệm của an toàn mạng máy tính	
1.5	Một số vấn đề về mạng nội bộ và mạng bên ngoài	
1.6	Những thành phần an toàn mạng thường được sử dụng để giảm thiểu các mối đe dọa	
Chương 2	**Công nghệ tường lửa**	**CLO2, CLO3, CLO5**
2.1	Định nghĩa về tường lửa	
2.2	Tầm quan trọng của tường lửa trong an toàn mạng máy tính	
2.3	Cơ chế hoạt động của tường lửa	
2.4	Phân loại tường lửa	
2.5	Các phương pháp lọc lưu lượng của tường lửa	
2.6	Các luật tường lửa	
Chương 3	**Công nghệ mạng riêng ảo – VPN**	**CLO2, CLO3, CLO5**
3.1	Định nghĩa về VPN	
3.2	Lợi ích của việc triển khai VPN	
3.3	Giới hạn của VPN	
3.4	Mô hình triển khai và kiến trúc VPN	
3.5	Mối quan hệ giữa mã hóa và VPN	
3.6	Chứng thực trong VPN	
3.7	Các giao thức được sử dụng trong VPN	
Chương 4	**Hệ thống phát hiện và ngăn chặn xâm nhập**	**CLO2, CLO3, CLO5**
4.1	Định nghĩa về xâm nhập, phát hiện xâm nhập và ngăn chặn xâm nhập	
4.2	Phát hiện xâm nhập và hệ thống phát hiện xâm nhập	
4.3	Phân loại hệ thống phát hiện xâm nhập	

Chương	Nội dung	Đáp ứng CLOs
4.4	Phản ứng với hành động xâm nhập hệ thống	
4.5	Những thách thức đối với hệ thống phát hiện xâm nhập	
4.6	Thế nào là hệ thống phát hiện xâm nhập hoàn thiện	
4.7	Hệ thống ngăn chặn xâm nhập	
4.8	Các công cụ phát hiện xâm nhập	
Chương 5	**Hệ thống quản lý sự kiện và thông tin an toàn – SIEM**	**CLO2, CLO3, CLO5**
5.1	Định nghĩa về SIEM	
5.2	Giám sát thời gian thực	
5.3	Phản ứng sự cố	
5.4	Giám sát người dùng	
5.5	Thông tin tình báo về mối đe dọa	
5.6	Phân tích và phát hiện mối đe dọa nâng cao	
Chương 6	**Hệ thống Honeynet**	**CLO2, CLO3, CLO5**
6.1	Giới thiệu về Honeynets và Honeypots	
6.2	Hệ thống Trap-and-Trace	
6.3	Phòng chống xâm nhập chủ động	

6.2. Thực hành

	Nội dung	Đáp ứng CLOs
6.2.1.	**Bài tập cá nhân**	**CLO2, CLO3, CLO5, CLO6**
	Người học làm bài tập trong từng chương.	
6.2.2.	**Bài tập nhóm**	**CLO2, CLO3, CLO4, CLO5, CLO6**
Lab 1	- Đề xuất và triển khai hệ thống mạng theo mô hình Client – Server có năng lực để thực hiện các công nghệ, hệ thống đảm bảo an toàn mạng máy tính như: Firewall, VPN, IDS/IPS, SIEM,... - Kiểm tra hoạt động của mô hình và lưu trữ làm tiền đề cho các bài Lab tiếp theo	
Lab 2	- Dựa vào mô hình đã triển khai ở bài Lab 1, hãy đề xuất vị trí phù hợp cho tường lửa và triển khai để nâng cao tính an toàn mạng máy tính của mô hình	

	Nội dung	Đáp ứng CLOs
	- Triển khai các luật tường lửa cho phép các máy khách được bảo vệ bởi tường lửa truy cập một số ứng dụng hoặc dịch vụ cụ thể. - Các thành viên trong nhóm thực hiện kiểm tra hoạt động của các luật tường lửa đã triển khai	
Lab 3	- Dựa vào mô hình đã triển khai ở bài Lab 1, hãy đề xuất vị trí phù hợp cho VPN và triển khai để nâng cao tính an toàn mạng máy tính của mô hình - Kiểm tra hoạt động của VPN - Các thành viên trong nhóm thực hiện kiểm tra hoạt động của VPN đã triển khai	
Lab 4	- Dựa vào mô hình đã triển khai ở bài Lab 1, hãy đề xuất vị trí phù hợp cho Hệ thống phát hiện & ngăn chặn xâm nhập và triển khai để nâng cao tính an toàn mạng máy tính của mô hình - Triển khai luật để phát hiện một số hoạt động xâm nhập - Các nhóm thực hiện kiểm thử chéo hệ thống của nhau để đánh giá khả năng phát hiện và ngăn chặn xâm nhập của hệ thống	
Lab 5	- Dựa vào mô hình đã triển khai ở bài Lab 1, hãy đề xuất vị trí phù hợp cho hệ thống SIEM và triển khai để nâng cao tính an toàn mạng máy tính của mô hình - Triển khai luật để thu thập thông tin nhật ký và cảnh báo - Các thành viên trong nhóm thực hiện kiểm tra hoạt động của hệ thống SIEM đã triển khai	
Lab 6	- Triển khai hệ thống mạng là tổng hợp các công nghệ, hệ thống của các bài lab trước mà có thêm hệ thống Honeynet. - Các nhóm thực hiện kiểm thử chéo hệ thống và đánh giá khả năng phòng thủ của từng nhóm với nhau.	

7. Phân bổ thời gian theo tiết và điều kiện thực hiện:

Chương	Tên chương	Số tiết tín chỉ					Ghi chú
		Lý thuyết	Bài tập	Thực hành	Tự học	Tổng	
1	Tổng quan về đảm bảo an toàn mạng máy tính	05	0	0	10	15	
2	Công nghệ tường lửa	05	0	05	10	20	
3	Công nghệ mạng riêng ảo – VPN	05	0	05	10	20	
4	Hệ thống phát hiện và ngăn chặn xâm nhập	05	0	10	10	25	
5	Hệ thống quản lý sự kiện và thông tin an toàn – SIEM	05	0	05	10	20	
6	Hệ thống Honeynet	05	0	05	10	20	
Tổng		**30**	**0**	**30**	**60**	**120**	

CÁC CHỦ ĐỀ THẢO LUẬN VÀ TIỂU LUẬN

1. .....
2. .....

8. Phương pháp giảng dạy:

Giảng viên giảng dạy với sự kết hợp của một số phương pháp sau:

Gợi ý:

- Thuyết trình
- Phát vấn
- Hỏi lại hoặc vấn đáp
- Đọc và tóm lược nội dung tài liệu
- Động não nhanh (bài tập tư duy cá nhân)
- Giao bài đọc về nhà
- Hướng dẫn tự học
- Thảo luận nhóm

Ma trận liên kết giữa Chuẩn đầu ra với phương pháp giảng dạy

Phương pháp giảng dạy	CLO1	CLO2	CLO3	CLO4	CLO5	CLO6	CLO7	CLO8	CLO9	CLO10	CLO11	CLO12
	X	X								X		
	X									X		
			X							X		

Phương pháp giảng dạy	CLO1	CLO2	CLO3	CLO4	CLO5	CLO6	CLO7	CLO8	CLO9	CLO10	CLO11	CLO12
				X						X	X	
					X	X	X	X	X	X	X	X
					X	X	X	X	X	X	X	X
					X	X	X	X	X	X	X	X

9. Phương pháp học tập

Sinh viên học tập với sự kết hợp của một số phương pháp sau:

Gợi ý:

- Thuyết trình
- Làm việc nhóm
- Tự học, tự nghiên cứu
- ….

Ma trận liên kết giữa Chuẩn đầu ra với phương pháp học tập

Phương pháp học tập	CLO1	CLO2	CLO3	CLO4	CLO5	CLO6	CLO7	CLO8	CLO9	CLO10	CLO11	CLO12
	X	X								X		
	X									X		
			X							X		
				X						X	X	

10. Nhiệm vụ của sinh viên

Gợi ý:

- Chủ động tổ chức thực hiện giờ tự học.
- Tham gia đầy đủ các giờ lên lớp và giờ thuyết trình (sinh viên chỉ được vắng mặt tối đa 20% thời gian lên lớp của học phần).
- Đọc tài liệu tham khảo bắt buộc và bổ trợ do giảng viên giới thiệu.
- Hoàn thành đầy đủ các bài tập cá nhân, bài tập nhóm.
- Tham gia kỳ thi kết thúc học phần.
- ....

11. Thang điểm đánh giá: Điểm đánh giá quá trình và điểm thi kết thúc học phần được chấm theo thang điểm 10 (từ 0 đến 10), làm tròn đến 1 chữ số thập phân.

12. Phương pháp kiểm tra, đánh giá kết quả học tập

Sinh viên được đánh giá kết quả học tập trên cơ sở hai điểm thành phần như sau:

1. *Điểm đánh giá quá trình: trọng số 40% bao gồm:*

a. Điểm chuyên cần: …., trọng số …%
b. Điểm kiểm tra thường xuyên: …., trọng số …%

2. Điểm thi kết thúc học phần: trọng số 60%

Hình thức thi: Tiểu luận

Ma trận quan hệ giữa Chuẩn đầu ra và phương pháp kiểm tra, đánh giá

Hình thức đánh giá	**CLO1**	**CLO2**	**CLO3**	**CLO4**	**CLO5**	**CLO6**	**CLO7**	**CLO8**	**CLO9**	**CLO10**	**CLO11**	**CLO12**
Tiểu luận	X	X	X	X	X	X	X	X	X	X	X	X
Thuyết trình	X		X		X	X	X	X	X	X	X	X
Trắc nghiệm	X	X	X	X	X	X	X	X	X	X	X	X
Dự lớp									X			
...												

13. Tài liệu phục vụ cho học phần (các tài liệu xuất bản trong 05 năm trở lại đây và cung cấp được cho Trung tâm Học liệu nơi đặt tài liệu)

13.1. Tài liệu chính

- Joseph Migga Kizza, Guide to Computer Network Security, Fifth Edition, Springer, 2020.

13.2. Tài liệu tham khảo

- Michael E. Whitman and Herbert J. Mattord, Principles of Information Security, 7th Edition, 2022.
- James F. Kurose & Keith W. Ross, Computer Networking A Top-Down Approach, Eighth Edition, PEARSON, 2020.
- R.Achary, Cryptography and Network Security an Introduction, Mercury Learning and Information LLC, 2021.

TP.Hồ Chí Minh, ngày ... tháng ... năm ……

Hiệu trưởng **Duyệt**	**Trưởng Bộ môn** (Ký và ghi rõ họ tên)	**Giảng viên biên soạn** (Ký và ghi rõ họ tên)