

1. THÔNG TIN VỀ GIẢNG VIÊN

Họ tên: Nguyễn Thế Cường
Chức danh, học hàm, học vị: Giảng viên, Tiến sĩ ngành Khoa học máy tính
Thời gian, địa điểm làm việc: Các ngày trong tuần, phòng 212 A2, CC3.
Địa chỉ liên hệ: Khoa CNTT&TT, trường ĐHHĐ
Điện thoại: 0975.008.134 Email: nguyenthecuong@hdu.edu.vn

Họ tên: **Lê Việt Nam**
Chức danh, học hàm, học vị: Giảng viên, Thạc sĩ ngành CNTT
Thời gian, địa điểm làm việc: Các ngày trong tuần, phòng 103 A2, CSC.
Địa chỉ liên hệ: Khoa CNTT&TT, trường ĐHHĐ
Điện thoại: 0916.537.333 Email: levietnam@hdu.edu.vn

Họ tên: **Hoàng Văn Quý**
Chức danh, học hàm, học vị: Giảng viên, ThS ngành CNTT
Thời gian, địa điểm làm việc: Các ngày trong tuần, phòng 103 A2, CSC.
Địa chỉ liên hệ: Khoa CNTT&TT, trường ĐHHĐ
Điện thoại: 0915.393.636 Email: hoangvanquy@hdu.edu.vn

2. THÔNG TIN CHUNG VỀ HỌC PHẦN

Tên ngành/khoá đào tạo: Đại học công nghệ thông tin

Tên học phần: An toàn mạng máy tính

Số tín chỉ: 3

Học phần: Tự chọn

Các môn tiên quyết: Mạng máy tính, LT mật mã

Các môn học kế tiếp:

Giờ tín chỉ đối với các hoạt động:

Lý thuyết	Bài tập/Thảo luận	Thực hành	Tự học
25	20	20	135

Địa chỉ bộ môn phụ trách học phần: Bộ môn Mạng máy tính & Ứng dụng, Khoa Công nghệ thông tin & Truyền thông, phòng 203 nhà A2, cơ sở 2, Đại học Hồng Đức.

3. NỘI DUNG CỦA HỌC PHẦN

Những khái niệm, công cụ, công nghệ, biện pháp căn bản về an ninh mạng như đảm bảo an toàn thiết bị mạng bằng Cisco IOS, AAA server, hệ thống firewall, hệ thống phát hiện tấn công và chống tấn công, các phương pháp chứng thực, mã hóa, toàn vẹn dữ liệu cũng như cách thức triển khai hệ thống mạng VPN.

4. MỤC TIÊU CỦA HỌC PHẦN

Mục tiêu		Mô tả	Chuẩn đầu ra CTĐT
1. Kiến thức	1.1	Có kiến thức tổng quan về an toàn mạng máy tính. những chính sách liên quan đến đảm bảo an toàn mạng máy tính	C13
	1.2	Có kiến thức về các phương pháp triển khai đối phó các tấn công mạng, mã hóa, toàn vẹn dữ liệu	C13
	1.3	Có kiến thức về các vấn đề đảm bảo an toàn truyền thông dữ liệu và các chứng chỉ an toàn mạng.	C13
2. Kỹ năng	2.1	Có kỹ năng Mô tả được một số nguy cơ và đe dọa tiềm ẩn đối với hệ thống mạng; ứng dụng được các chính sách về quản lý theo dõi an toàn hệ thống mạng	C13
	2.2	Có kỹ năng quản lý việc truy cập thiết bị mạng bằng Cisco IOS và AAA; Triển khai được các biện pháp chống tấn công mạng LAN và các biện pháp chống xâm nhập và kiểm soát, lọc lưu lượng mạng bằng Cisco IOS firewall như CBAC, Zone-based firewall, Cisco IOS IPS	C13
	2.3	Có kỹ năng về các vấn đề về đảm bảo an toàn truyền thông dữ liệu; sử dụng được chứng chỉ số; Triển khai hệ thống mạng site-to-site VPN	C13, C16
3. Thái độ	3.1	Có thái độ học tập tích cực, chịu khó tìm hiểu về an toàn mạng máy tính và các lĩnh vực liên quan	C16, C21
	3.2	Có khả năng làm việc độc lập và khả năng làm	C16, C21

		việc nhóm	
--	--	-----------	--

5. CHUẨN ĐẦU RA CỦA HỌC PHẦN

TT	KẾT QUẢ MONG MUỐN ĐẠT ĐƯỢC	MỤC TIÊU	CHUẨN ĐẦU RA CTĐT
A	Trình bày được các kiến thức tổng quan về an toàn mạng máy tính; các chính sách liên quan đến đảm bảo an toàn mạng máy tính; triển khai được các PP đối phó các tấn công mạng; sử dụng các kiến thức để đảm bảo an toàn truyền thông dữ liệu và các chứng chỉ an toàn mạng.	1.1, 1.2, 1.3	C13
B	Phân loại và mô tả được một số nguy cơ và đe dọa tiềm ẩn đối với hệ thống mạng; ứng dụng được các chính sách về quản lý theo dõi an toàn hệ thống mạng	1.1, 2.1	C13
C	Trình bày được các vấn đề về quản lý việc truy cập thiết bị mạng bằng Cisco IOS và AAA; Trình bày và Triển khai được các biện pháp chống tấn công mạng LAN và các biện pháp chống xâm nhập và kiểm soát, lọc lưu lượng mạng bằng Cisco IOS firewall như CBAC, Zone-based firewall, Cisco IOS IPS	1.3, 2.1, 2.2, 2.3	C13
D	Trình bày được các vấn đề về đảm bảo an toàn truyền thông dữ liệu; sử dụng được chứng chỉ số; Triển khai hệ thống mạng site-to-site VPN; thiết kế và hỗ trợ trong việc xây dựng được một hệ thống mạng đảm bảo an toàn.	1.3, 2.1, 2.2, 2.3	C13, C16
E	Vận dụng được các kiến thức về An toàn mạng máy tính để giải quyết các bài toán thực tế liên quan đến lĩnh vực an ninh mạng máy tính.	2.3, 3.1, 3.2	C16, C21

6. NỘI DUNG CHI TIẾT HỌC PHẦN

CHƯƠNG 1: CÁC NGUY CƠ VỀ AN TOÀN MẠNG HIỆN ĐẠI

1.1 Giới thiệu

1.2 Các nguyên tắc căn bản về an toàn mạng

- 1.3 Virus, Worm và Trojan
- 1.4 Các hình thức tấn công và phòng chống thông dụng
- 1.5 Tóm tắt chương
- 1.6 Trắc nghiệm ôn tập

CHƯƠNG 2: AN TOÀN THIẾT BỊ MẠNG CISCO

- 2.1 Giới thiệu
- 2.2 Quản lý truy cập thiết bị mạng
- 2.3 Cấu hình
- 2.4 Theo dõi giám sát thiết bị
- 2.5 Tính năng an toàn tự động
- 2.6 Tóm tắt chương
- 2.7 Trắc nghiệm ôn tập

Chương 3: AAA

- 3.1 Giới thiệu
- 3.2 Mục đích và các hình thức AAA
- 3.3 Cấu hình local AAA
- 3.4 Cấu hình server AAA
- 3.5 Tóm tắt chương
- 3.6 Trắc nghiệm ôn tập

CHƯƠNG 4: CÔNG NGHỆ FIREWALL

- 4.1 Giới thiệu
- 4.2 Access Control List
- 4.3 Các công nghệ về firewall
- 4.4 Context-based Access Control
- 4.5 Cấu hình CBAC
- 4.6 Zone-based Policy
- 4.7 Cấu hình ZPF
- 4.8 Tóm tắt chương
- 4.9 Trắc nghiệm ôn tập

CHƯƠNG 5: HỆ THỐNG CHỐNG XÂM NHẬP

- 5.1 Giới thiệu
- 5.2 Các công nghệ IPS
- 5.3 Cấu hình
- 5.4 Tóm tắt chương
- 5.5 Trắc nghiệm ôn tập

CHƯƠNG 6: AN TOÀN TRÊN MẠNG LAN

- 6.1 Giới thiệu
- 6.2 An toàn trên thiết bị đầu cuối
- 6.3 An toàn trên mạng LAN
- 6.4 An toàn trên mạng không dây, VoIP và hệ thống SAN
- 6.5 Cấu hình
- 6.6 SPAN và RSPAN
- 6.7 Tóm tắt chương
- 6.8 Trắc nghiệm ôn tập

CHƯƠNG 7: MẬT MÃ HỌC

- 7.1 Giới thiệu
- 7.2 Các dịch vụ về mật mã học
- 7.3 Hash, chữ ký điện tử và chứng thực
- 7.4 Mã hóa đối xứng và bất đối xứng
- 7.5 Chứng chỉ số
- 7.6 Hạ tầng PKI
- 7.7 Tóm tắt chương
- 7.8 Trắc nghiệm ôn tập

CHƯƠNG 8: TRIỂN KHAI MẠNG VPN

- 8.1 Giới thiệu
- 8.2 Phân loại VPN
- 8.3 IPSec VPN
- 8.4 Cấu hình Site-to-site VPN
- 8.5 Cấu hình remote access VPN
- 8.6 Cấu hình SSL VPN

- 8.7 Tóm tắt chương
- 8.8 Trắc nghiệm ôn tập

CHƯƠNG 9. AN TOÀN TRONG VẬN HÀNH HỆ THỐNG MẠNG

- 9.1 Giới thiệu
- 9.2 Chu trình quản lý mạng
- 9.3 SecureX network
- 9.4 Thiết lập chính sách toàn diện về an toàn hệ thống mạng
- 9.5 Tóm tắt chương

7. HỌC LIỆU

<i>Tài liệu bắt buộc</i>		
1. Ciampa Mark, Comptia Security + Guide to Network Security Fundamentals	Cengage Learning	2011
<i>Tài liệu tham khảo</i>		
1. Vũ Đình Cường, Cách bảo vệ dữ liệu quan trọng và phương pháp phát hiện xâm nhập	NXB Lao động xã hội	2009
2. Phạm Huy Hoàng, Thiết kế mạng Intranet	NXB BK HN	2019

8. HÌNH THỨC TỔ CHỨC DẠY HỌC

8.1. Lịch trình chung

Nội dung	Hình thức tổ chức dạy học				
	LT	BT+ TL	TH	Tự học	KT ĐG
CHƯƠNG 1: CÁC NGUY CƠ VỀ AN TOÀN MẠNG HIỆN ĐẠI	2	2	0	9	
1.1. Giới thiệu	0.5				
1.2. Các nguyên tắc căn bản về an toàn mạng	0.5				
1.3. Virus, Worm và Trojan	0.5				
1.4. Các hình thức tấn công và phòng chống thông dụng	0.5				
1.5. Tóm tắt chương					

1.6. Trắc nghiệm ôn tập		2			
Chương 2: An toàn thiết bị mạng Cisco	2	2	0	9	
2.1. Giới thiệu	0.25				
2.2. Quản lý truy cập thiết bị mạng	0.25				
2.3. Cấu hình	0.5				
2.4. Theo dõi giám sát thiết bị	0.5				
2.5. Tính năng an toàn tự động	0.5				
2.6. Tóm tắt chương		0.25			
2.7. Trắc nghiệm ôn tập		1.75			
Chương 3: AAA	3	2	0	12	01 Bài kiểm tra (1 tiết)
3.1. Giới thiệu	0.25				
3.2. Mục đích và các hình thức AAA	0.5				
3.3. Cấu hình local AAA	1				
3.4. Cấu hình server AAA	1				
3.5. Tóm tắt chương	0.25				
3.6. Trắc nghiệm ôn tập		2			
Chương 4: Công nghệ firewall	3	2	4	18	
4.1. Giới thiệu	0.25				
4.2. Access Control List	0.25				
4.3. Các công nghệ về firewall	0.25				
4.4. Context-based Access Control	0.5				

4.5. Cấu hình CBAC	0.5				
4.6. Zone-based Policy	0.25				
4.7. Cấu hình ZPF	0.75				
4.8. Tóm tắt chương	0.25				
4.9. Trắc nghiệm ôn tập		2			
Chương 5: Hệ thống chống xâm nhập	3	2	4	18	01 Bài kiểm tra (1 tiết)
5.1. Giới thiệu	0.25				
5.2. Các công nghệ IPS	1.75				
5.3. Cấu hình	1				
5.4. Tóm tắt chương					
5.5. Trắc nghiệm ôn tập		2			
Chương 6: An toàn trên mạng LAN	3	2	0	18	
6.1. Giới thiệu	c				
6.2. An toàn trên thiết bị đầu cuối	0.25				
6.3. An toàn trên mạng LAN	0.25				
6.4. An toàn trên mạng không dây, VoIP và hệ thống SAN	0.25				
6.5. Cấu hình	1				
6.6. SPAN và RSPAN	1				
6.7. Tóm tắt chương					
6.8. Trắc nghiệm ôn tập		2.0			
Chương 7: Mật mã học	3	2	4	18	01 Bài kiểm

					tra (1 tiết)
7.1. Giới thiệu	0.25				
7.2. Các dịch vụ về mật mã học	0.25				
7.3. Hash, chữ lý điện tử và chứng thực	0.25				
7.4. Mã hóa đối xứng và bất đối xứng	0.25				
7.5. Chứng chỉ số	1				
7.6. Hạ tầng PKI	1				
7.7. Tóm tắt chương					
7.8. Trắc nghiệm ôn tập		2.0			
Chương 8: Triển khai mạng VPN	3	2	4	18	01 Bài kiểm tra (1 tiết)
8.1. Giới thiệu	0.25				
8.2. Phân loại VPN	0.25				
8.3. IPSec VPN	0.25				
8.4. Cấu hình Site-to-site VPN	0.25				
8.5. Cấu hình remote access VPN	1				
8.6. Cấu hình SSL VPN	1				
8.7. Tóm tắt chương					
8.8. Trắc nghiệm ôn tập		2.0			
Chương 9. An toàn trong vận hành hệ thống mạng	3	2	4	18	
9.1. Giới thiệu	0.25				

9.2. Chu trình quản lý mạng	0.75				
9.3. SecureX network	1.5				
9.4. Thiết lập chính sách toàn diện về an toàn hệ thống mạng	0.5				
9.5. Tóm tắt chương		2.0			
Tổng	25	20	20	135	

8.2. Lịch trình cụ thể cho từng nội dung

Nội dung tuần 1 (3LT + 2TL)

Hình thức	Thời gian, địa điểm	Nội dung chính	Mục tiêu cụ thể	Yêu cầu người học chuẩn bị	CDR học phần
Lý thuyết	3 tiết, tại phòng học	<p>Chương 1: Các nguy cơ về an toàn mạng hiện đại</p> <p>1.1. Giới thiệu</p> <p>1.2. Các nguyên tắc căn bản về an toàn mạng</p> <p>1.3. Virus, Worm và Trojan</p> <p>1.4. Các hình thức tấn công và phòng chống thông dụng</p> <p>1.5. Tóm tắt chương</p>	<ul style="list-style-type: none"> - Hiểu được về nguồn gốc các rủi ro xuất hiện trên mạng máy tính - Nắm được nguyên lý hoạt động của Virus, Worm và Trojan - Nắm được các hình thức tấn công và phương pháp phòng chống thông dụng 	<ul style="list-style-type: none"> - Đọc tài liệu [1] - Nghiên cứu tài liệu tham khảo [1] - Sử dụng Internet để tham khảo thêm 	A
Thảo luận	2 tiết, tại phòng học	<p>Thảo luận về:</p> <ul style="list-style-type: none"> - Các nguyên tắc căn bản về an toàn mạng - Nguyên lý hoạt động của các phần mềm độc hại - Các hình thức tấn công và phương án phòng thủ 	<ul style="list-style-type: none"> - Hiểu được về nguồn gốc các rủi ro xuất hiện trên mạng máy tính - Nắm được nguyên lý hoạt động của Virus, Worm và Trojan 	<ul style="list-style-type: none"> - Chuẩn bị câu hỏi cần thảo luận về các vấn đề nêu trên 	A

			- Nắm được các hình thức tấn công và phương pháp phòng chống thông dụng		
Tự học	9 tiết, ở nhà hoặc thư viện	Nghiên cứu thêm về các thành phần liên quan đến an toàn và các chuẩn an toàn thông tin mạng máy tính	Củng cố thêm kiến thức và rèn luyện khả năng tự học	- Đọc kỹ các tài liệu tham khảo để nắm vững các khái niệm về an toàn và các nguyên tắc cơ bản của an toàn thông tin mạng	

Nội dung tuần 2 (2TL + 3LT)

Hình thức	Thời gian, địa điểm	Nội dung chính	Mục tiêu cụ thể	Yêu cầu người học chuẩn bị	CDR học phần
Thảo luận	2 tiết, tại phòng học	Thảo luận về: - Các nguyên tắc căn bản về an toàn mạng - Nguyên lý hoạt động của các phần mềm độc hại - Các hình thức tấn công và phương án phòng thủ	- Hiểu được về nguồn gốc các rủi ro xuất hiện trên mạng máy tính - Nắm được nguyên lý hoạt động của Virus, Worm và Trojan - Nắm được các hình thức tấn công và phương pháp phòng chống thông dụng	- Chuẩn bị câu hỏi cần thảo luận về các vấn đề nêu trên	A

Lý thuyết	3 tiết, tại phòng học	Chương 2: An toàn thiết bị mạng Cisco 2.1. Giới thiệu 2.2. Quản lý truy cập thiết bị mạng 2.3. Cấu hình 2.4. Theo dõi giám sát thiết bị 2.5. Tính năng an toàn tự động 2.6. Tóm tắt chương	- Hiểu được các bước được thực thi trong quá trình quản lý truy cập thiết bị - Cấu hình được thiết bị - Nắm được các thao tác cơ bản trong quá trình theo dõi và giám sát thiết bị	- Đọc tài liệu [1] - Nghiên cứu tài liệu tham khảo [1], [2] - Sử dụng Internet để tham khảo thêm	B
Tự học	9 tiết, ở nhà hoặc thư viện	Nghiên cứu thêm các kiến thức đã học	-Củng cố thêm kiến thức và rèn luyện khả năng tự học; - Chuẩn bị kiến thức để làm bài kiểm tra số 1.	-Báo cáo kết quả tự học, trình kết quả tự học khi có yêu cầu.	

Nội dung tuần 3 (3LT + 1TL + 1KT)

Hình thức	Thời gian, địa điểm	Nội dung chính	Mục tiêu cụ thể	Yêu cầu người học chuẩn bị	CDR học phần
Lý thuyết	3 tiết, tại phòng học	Chương 3: AAA 3.1. Giới thiệu 3.2. Mục đích và các hình thức AAA 3.3. Cấu hình local AAA 3.4. Cấu hình server AAA 3.5. Tóm tắt chương	- Nắm được mục đích và các hình thức của cơ chế đảm bảo an toàn thông tin AAA - Cấu hình được hệ thống AAA cục bộ - Cấu hình được hệ thống AAA chủ	- Đọc tài liệu [1] - Nghiên cứu tài liệu tham khảo [1], [2] - Sử dụng Internet để tham khảo thêm	C
Thảo	1 tiết, tại	Thảo luận:	- Có thể xây	- Đọc tài liệu	C

luận	phòng học	- Các phương pháp xây dựng hệ thống đảm bảo an toàn thông tin theo mô hình AAA	dựng được một AAA đơn giản đảm bảo an toàn thông tin	[1], [2] - Nghiên cứu tài liệu tham khảo [1], [2] - Sử dụng Internet để tham khảo thêm	
KT-ĐG	1 tiết tại phòng học	Kiểm tra kiến thức chương 1, 2, 3		Nghiên cứu kỹ các bài giảng đã học	
Tự học	9 tiết, ở nhà hoặc thư viện	Nghiên cứu các câu hỏi ôn tập	Củng cố kiến thức và rèn luyện khả năng tự học	Làm đầy đủ các bài tập theo yêu cầu;	

Nội dung tuần 4 (3LT + 2TL)

Hình thức	Thời gian, địa điểm	Nội dung chính	Mục tiêu cụ thể	Yêu cầu người học chuẩn bị	CDR học phần
Lý thuyết	3 tiết, tại phòng học	Chương 4: Công nghệ Firewall 4.1. Giới thiệu 4.2. Access Control List 4.3. Các công nghệ về firewall 4.4. Context-based Access Control 4.5. Cấu hình CBAC 4.6. Zone-based Policy 4.7. Cấu hình ZPF 4.8. Tóm tắt chương 4.9. Trắc nghiệm ôn tập	<ul style="list-style-type: none"> - Hiểu được nguyên lý hoạt động của phương pháp sử dụng Access Control List - Nắm được các công nghệ về tường lửa - Hiểu được phương pháp kiểm soát truy cập theo ngữ cảnh - Cấu hình được một hệ thống dựa vào chính 	<ul style="list-style-type: none"> - Đọc tài liệu [1] - Nghiên cứu tài liệu tham khảo [1], [2] - Sử dụng Internet để tham khảo thêm 	C

			sách		
Thảo luận	2 tiết, tại phòng học	Thảo luận về: - Các công nghệ tường lửa - Các phương pháp truy cập	- Hiểu được các công nghệ về tường lửa - Hiểu được phương pháp kiểm soát truy cập theo ngữ cảnh - Cấu hình được một hệ thống dựa vào chính sách	- Đọc tài liệu [1] - Nghiên cứu tài liệu tham khảo [1], [2] - Sử dụng Internet để tham khảo thêm	C
Tự học	9 tiết, ở nhà hoặc thư viện	Tìm hiểu thêm thông tin về về các loại tường lửa	- Cùng cố kiến thức và rèn luyện khả năng tự học	Làm đầy đủ các bài tập theo yêu cầu.	

Nội dung tuần 5 (3LT + 2TL)

Hình thức	Thời gian, địa điểm	Nội dung chính	Mục tiêu cụ thể	Yêu cầu người học chuẩn bị	CDR học phần
Lý thuyết	3 tiết, tại phòng học	Chương 5: Hệ thống chống xâm nhập 5.1. Giới thiệu 5.2. Các công nghệ IPS 5.3. Cấu hình 5.4. Tóm tắt chương	- Hiểu được nguyên lý hoạt động của các hệ thống chống xâm nhập - Hiểu được các công nghệ chống xâm nhập - Cấu hình được một hệ thống chống xâm nhập cơ bản	- Đọc trước tài liệu [1] và tài liệu tham khảo [1], [2] - Nghiên cứu thêm thông tin trên Internet về cách xây dựng các hệ thống chống xâm nhập	D
Thảo luận	2 tiết, tại phòng học	Thảo luận: - Các công nghệ chống xâm nhập	- Hiểu được các công nghệ chống xâm nhập - Cấu hình được	- Đọc trước tài liệu [1] và tài liệu tham khảo [1]	D

			một hệ thống chống xâm nhập cơ bản	- Nghiên cứu thêm thông tin trên Internet về cách thức xây dựng các hệ thống chống xâm nhập	
KT-ĐG		Kiểm tra bài viết 1 tiết	- Đánh giá mức độ tiếp thu của sinh viên các kỹ thuật lập trình đa luồng	Ôn tập các nội dung các phần đã học	
Tự học	9 tiết, ở nhà hoặc thư viện	Đọc thêm về kỹ thuật lập trình trong phần tài liệu tham khảo [1]	- củng cố kiến thức về xâm nhập và chống xâm nhập trên mạng và rèn luyện khả năng tự học.	Thực hiện các yêu cầu tự học.	

Nội dung tuần 6 (2TL + 3LT)

Hình thức	Thời gian, địa điểm	Nội dung chính	Mục tiêu cụ thể	Yêu cầu người học chuẩn bị	CĐR học phần
Thảo luận	2 tiết, tại phòng học	Thảo luận: - Các công nghệ chống xâm nhập	- Hiểu được các công nghệ chống xâm nhập - Cấu hình được một hệ thống chống xâm nhập cơ bản	- Đọc trước tài liệu [1] và tài liệu tham khảo [1], [2] - Nghiên cứu thêm thông tin trên Internet về cách thức xây dựng các hệ thống chống xâm nhập	D

Lý thuyết	3 tiết, tại phòng học	<p>Chương 6: An toàn trên mạng LAN</p> <p>6.1. Giới thiệu</p> <p>6.2. An toàn trên thiết bị đầu cuối</p> <p>6.3. An toàn trên mạng LAN</p> <p>6.4. An toàn trên mạng không dây, VoIP và hệ thống SAN</p> <p>6.5. Cấu hình</p> <p>6.6. SPAN và RSPAN</p> <p>6.7. Tóm tắt chương</p>	<ul style="list-style-type: none"> - Nắm được yêu cầu về an toàn trên thiết bị đầu cuối - Hiểu được phương pháp đảm bảo an toàn trên mạng LAN - Cấu hình được một mạng LAN nhằm đảm bảo an toàn hệ thống 	<ul style="list-style-type: none"> - Đọc trước tài liệu [1] và tài liệu tham khảo [1], [2] về các phương thức đảm bảo an toàn trên mạng cục bộ và các mạng truyền thông đa phương tiện khác 	D
KT-ĐG		Kiểm tra giữa kỳ	<ul style="list-style-type: none"> - Đánh giá mức độ tiếp thu của sinh viên về các kiến thức tổng hợp từ các chương đã học. 	Ôn tập nội dung chương 1,2,3,4,5 để làm bài kiểm tra.	
Tự học	9 tiết, ở nhà hoặc thư viện	Tham khảo thêm tài liệu [1] về các phương pháp an toàn trong mạng cục bộ.	Rèn luyện khả năng tự học.	<ul style="list-style-type: none"> - Thực hiện các yêu cầu tự học. - Làm đầy đủ các bài tập theo yêu cầu; 	

Nội dung tuần 7 (4TL + 1KT)

Hình thức	Thời gian, địa điểm	Nội dung chính	Mục tiêu cụ thể	Yêu cầu người học chuẩn bị	CDR học phần
Thảo luận	4 tiết, tại phòng học	Thảo luận về: <ul style="list-style-type: none"> - Các phương pháp đảm bảo an toàn trên mạng cục bộ - Cách thức cấu hình mạng cục bộ 	<ul style="list-style-type: none"> - Nắm được yêu cầu về an toàn trên thiết bị đầu cuối - Hiểu được phương pháp đảm bảo an toàn trên mạng LAN - Cấu hình được một mạng LAN nhằm đảm bảo an toàn hệ thống 	<ul style="list-style-type: none"> - Đọc trước tài liệu [1] và tài liệu tham khảo [1], [2] về các phương thức đảm bảo an toàn trên mạng cục bộ và các mạng truyền thông đa phương tiện khác 	D
KT-ĐG	1 tiết, tại phòng học	Kiểm tra 01 tiết về các phương pháp đảm bảo an toàn thông tin cho mạng cục bộ			
Tự học	9 tiết, ở nhà hoặc thư viện	- Tự tìm hiểu và học cách xây dựng và phát triển các giải pháp mạng cục bộ	Củng cố kiến thức và rèn luyện khả năng tự học	Thực hiện các yêu cầu ở phần nội dung	

Nội dung tuần 8 (3LT + 2TL)

Hình thức	Thời gian,	Nội dung chính	Mục tiêu cụ thể	Yêu cầu người học chuẩn bị	CDR học
-----------	------------	----------------	-----------------	----------------------------	---------

	địa điểm				phần
Lý thuyết	3 tiết, tại phòng học	<p>Chương 7: Mật mã học</p> <p>7.1. Giới thiệu</p> <p>7.2. Các dịch vụ về mật mã học</p> <p>7.3. Hash, chữ ký điện tử và chứng thực</p> <p>7.4. Mã hóa đối xứng và bất đối xứng</p> <p>7.5. Chứng chỉ số</p> <p>7.6. Hạ tầng PKI</p> <p>7.7. Tóm tắt chương</p>	<ul style="list-style-type: none"> - Hiểu được vai trò của mật mã học trong đảm bảo an toàn thông tin - Nắm được các dịch vụ về mật mã - Hiểu được nguyên lý xây dựng chữ kí điện tử - Biết được khái niệm và phương thức hoạt động của chứng chỉ số - Biết được hạ tầng quản lý khóa công khai 	<ul style="list-style-type: none"> - Đọc trước tài liệu [1] và tài liệu tham khảo [1], [2] - Nghiên cứu thêm thông tin trên Internet 	D
Thảo luận	2 tiết, tại phòng học	<p>Thảo luận</p> <ul style="list-style-type: none"> - Các dịch vụ về mật mã - Chữ ký điện tử và chứng thực - Các phương pháp mã hóa - Chứng chỉ số 	<ul style="list-style-type: none"> - Nắm được các dịch vụ về mật mã - Hiểu được nguyên lý xây dựng chữ kí điện tử - Biết được khái niệm và phương thức hoạt động của chứng chỉ số - Biết được hạ tầng quản lý khóa công khai 	<ul style="list-style-type: none"> - Nghiên cứu tài liệu [2] - Đọc thêm thông tin trên mạng về các phương pháp quản lý người dùng 	D
KT-ĐG	1 tiết tại phòng học	Kiểm tra các thuật toán liên quan đến mã hoá		Nghiên cứu các thuật toán liên quan đến mã hoá	

Tự học	9 tiết, ở nhà hoặc thư viện	Nghiên cứu về các thuật toán mã hóa			
--------	--------------------------------------	--	--	--	--

Nội dung tuần 9 (3LT + 2TL)

Hình thức	Thời gian, địa điểm	Nội dung chính	Mục tiêu cụ thể	Yêu cầu người học chuẩn bị	CĐR học phần
Lý thuyết	3 tiết, tại phòng học	Chương 8: Triển khai mạng VPN 8.1. Giới thiệu 8.2. Phân loại VPN 8.3. IPSec VPN 8.4. Cấu hình Site-to-site VPN 8.5. Cấu hình remote access VPN 8.6. Cấu hình SSL VPN 8.7. Tóm tắt chương	- Hiểu được vai trò của mạng riêng ảo - Hiểu được công nghệ mạng riêng ảo - Cấu hình được các mạng riêng ảo	- Đọc trước tài liệu [1] và tài liệu tham khảo [1], [2] - Nghiên cứu thêm thông tin trên Internet	D
Thảo luận	2 tiết, tại phòng học	Thảo luận - Các phương pháp xây dựng mạng riêng ảo - Các phần mềm hỗ trợ xây dựng các mạng riêng ảo - Các phương pháp quản lý người dùng mạng riêng ảo	- Hiểu được công nghệ mạng riêng ảo - Cấu hình được các mạng riêng ảo	- Nghiên cứu tài liệu [1] - Đọc thêm thông tin trên mạng về các phương pháp quản lý người dùng	D
Tự học	9 tiết, ở nhà hoặc thư viện	- Nghiên cứu các ví dụ về các chương trình hỗ trợ xây dựng các mạng riêng ảo và phương pháp quản lý người dùng		- Đọc các tài liệu và tham khảo thông tin trên mạng Internet	

Nội dung tuần 10 (3LT + 2TL)

Hình thức	Thời gian, địa điểm	Nội dung chính	Mục tiêu cụ thể	Yêu cầu người học chuẩn bị	CDR học phần
Lý thuyết	3 tiết, tại phòng học	<p>Chương 9. An toàn trong vận hành hệ thống mạng</p> <p>9.1. Giới thiệu</p> <p>9.2. Chu trình quản lý mạng</p> <p>9.3. SecureX network</p> <p>9.4. Thiết lập chính sách toàn diện về an toàn hệ thống mạng</p>	<ul style="list-style-type: none"> - Hiểu được vai trò của mạng riêng ảo - Hiểu được công nghệ mạng riêng ảo - Cấu hình được các mạng riêng ảo 	<ul style="list-style-type: none"> - Đọc trước tài liệu [1] và tài liệu tham khảo [1], [2] - Nghiên cứu thêm thông tin trên Internet 	D
Thảo luận	2 tiết, tại phòng học	<p>Thảo luận</p> <ul style="list-style-type: none"> - Chu trình quản lý mạng - Cách thức thiết lập chính sách an toàn hệ thống 	<ul style="list-style-type: none"> - Hiểu được công nghệ mạng riêng ảo - Cấu hình được các mạng riêng ảo 	<ul style="list-style-type: none"> - Nghiên cứu tài liệu [1] - Đọc thêm thông tin trên mạng về các phương pháp quản lý mạng 	D
Tự học	9 tiết, ở nhà hoặc thư viện	<ul style="list-style-type: none"> - Nghiên cứu các ví dụ về các chương trình hỗ trợ xây dựng các mạng riêng ảo và phương pháp quản lý người dùng 		<ul style="list-style-type: none"> - Đọc các tài liệu và tham khảo thông tin trên mạng Internet 	

Nội dung tuần 11(10TH)

Hình thức	Thời gian, địa điểm	Nội dung chính	Mục tiêu cụ thể	Yêu cầu người học chuẩn bị	CDR học phần
Thực	5 tiết,	Thực hành chương 4:			D, E

hành	phòng máy	- Cài đặt và cấu hình hệ điều hành LINUX trên máy cá nhân - Sử dụng các lệnh cơ bản trong LINUX - Cấu hình tường lửa			
Thực hành	5 tiết, phòng máy	Thực hành chương 5: - Xây dựng hệ thống chống xâm nhập - Thử nghiệm hệ thống với các xâm nhập			D, E
Tự học	10 tiết, ở nhà hoặc thư viện	Thực hiện các thao tác đã học tại lớp			

Nội dung tuần 12 (10TH)

Hình thức	Thời gian, địa điểm	Nội dung chính	Mục tiêu cụ thể	Yêu cầu người học chuẩn bị	CDR học phần
Thực hành	5 tiết, phòng máy	Thực hành chương 6,7 - Xây dựng các phương pháp đảm bảo an toàn mạng LAN - Thử nghiệm các hệ mã			D, E
Thực hành	5 tiết, phòng máy	Thực hành chương 8,9: - Triển khai mạng riêng ảo và cấu hình mạng riêng ảo cho mục đích cá nhân - Thực hiện quản lý tài khoản mạng riêng ảo - Xây dựng các chính sách đảm bảo an toàn hệ thống			D, E
Tự học	10 tiết, ở nhà hoặc thư	- Thực hành các thao tác đã học tại phòng máy		Làm đầy đủ các bài tập theo	

	viện			yêu cầu;	
--	------	--	--	----------	--

9. CHÍNH SÁCH ĐỐI VỚI MÔN HỌC

* Yêu cầu của môn học đối với sinh viên.

Sinh viên phải có đủ các điều kiện sau mới được dự thi cuối kì và được đánh giá kết quả môn học.

- *Mức độ chuyên cần*: Sinh viên phải tham gia học tối thiểu là 80% số tiết học trên lớp.
- *Thái độ học tập*: Sinh viên phải tích cực tự học, tự nghiên cứu, làm các bài tập đầy đủ và nộp đúng hạn theo yêu cầu của giáo viên; tích cực tham gia thảo luận nhóm, tích cực tham gia ý kiến xây dựng bài trên lớp.
- *Điểm quá trình*: Phải có tối thiểu 3 con điểm thường xuyên; 1 con điểm kiểm tra giữa kì.
- *Điểm thi kết thúc học phần*: Bắt buộc sinh viên phải tham gia dự thi khi đã có đủ điều kiện dự thi.

* Ngoài ra:

- Người học tối thiểu phải có các học liệu [1], để tự nghiên cứu và chuẩn bị bài trước khi đến lớp.
- Người học phải có tài liệu hướng dẫn thực hành và chuẩn bị bài thực hành theo quy định trước khi thực hành trên phòng máy.

10. PHƯƠNG PHÁP, HÌNH THỨC KIỂM TRA – ĐÁNH GIÁ KẾT QUẢ HỌC TẬP HỌC PHẦN

10.1. Tiêu chí, đánh giá :

- Đối với hình thức vấn đáp: có thể kiểm tra thông qua các bài tập tại lớp. Yêu cầu người học phải nắm vững lý thuyết cơ bản, kỹ năng áp dụng vào các bài tập một cách thành thạo.
- Đối với các bài kiểm tra viết: Học sinh phải đạt được các yêu cầu của đề bài, biết vận dụng kiến thức được học để giải quyết các bài tập liên quan.

10.2. Kiểm tra- đánh giá thường xuyên:

- Đánh giá quá trình học và tự học của người học trong các giờ học.
- Kiểm tra viết theo lịch, thời gian: từ 40 đến 50 phút/bài.
- Điểm trung bình của các bài kiểm tra có trọng số 0,3.

10.3. Kiểm tra – đánh giá giữa kỳ

- Kiểm tra - đánh giá giữa kì: 1 bài kiểm tra viết vào tuần 6 ; thời gian: 50 phút.
- Điểm: từ 0 đến 10.

- Điểm của bài kiểm tra giữa kỳ có trọng số 0,2.

10.4. Kiểm tra – đánh giá cuối kì:

- Hình thức: Thi viết; Thời gian: 120 phút.
- Điểm: từ 0 đến 10, làm tròn đến một chữ số thập phân.
- Địa điểm: Phòng thi do phòng Đào tạo xếp ; Trọng số: 0,5.

11. CÁC YÊU CẦU KHÁC

- Bố trí lịch học, thời gian học theo đúng lịch trình cụ thể (mục 8.2)
- Giờ lý thuyết được bố trí học tại phòng học có máy chiếu, nếu phòng học lớn cần có thêm micro, loa.
- Giờ thực hành được bố trí ở các phòng máy có đầy đủ các trang thiết bị.

Ngày 20 tháng 8 năm 2019

Thanh Hóa, ngày 6 tháng 8 năm 2019

KHOA CNTT&TT

TRƯỞNG BỘ MÔN

GIẢNG VIÊN SOẠN

Phạm Thế Anh

Nguyễn Thế Cường

Hoàng Văn Quý