	VIETTEL AI RACE	Public 253
	ĐỀ CƯƠNG CHI TIẾT HỌC PHẦN **Tên học phần: An toàn mạng (Network Security)**	Lần ban hành: 1

1. Thông tin chung về học phần

1) Mã học phần:	INT1482
2) Số tín chỉ:	3
3) Hoạt động học tập	
- Lý thuyết:	30 tiết
- Bài tập:	0 tiết
- Thảo luận:	6 tiết
- Thực hành/Thí nghiệm:	12 tiết
- Thực tế/Thực tập:	0 tiết
- Đề án/Bài tập lớn…:	18 tiết
- Tự học:	90 tiết
4) Điều kiện tham gia học phần:	
- Học phần tiên quyết:	Cơ sở An toàn thông tin
- Học phần học trước:	Mạng máy tính
5) Các giảng viên phụ trách học phần:	
- Giảng viên phụ trách chính:	TS. Nguyễn Ngọc Điệp

- Danh sách giảng viên cùng giảng dạy:	TS. Phạm Hoàng Duy, PGS.TS. Hoàng Xuân Dậu
- Khoa/ Bộ môn phụ trách giảng dạy:	Khoa An toàn thông tin/ Bộ môn An toàn mạng
6) Loại học phần:	☒ Bắt buộc ☐ Tự chọn tự do ☐ Tự chọn theo định hướng (bắt buộc)
7) Thuộc thành phần học tập	☐ Giáo dục đại cương (chung, khoa học cơ bản, kỹ năng) ☐ Cơ sở khối ngành (nhóm ngành/lĩnh vực) ☐ Cơ sở ngành ☐ Ngành ☒ Chuyên ngành ☐ Bổ trợ
	☐ Thực tập/ Đồ án tốt nghiệp/ Khóa luận tốt nghiệp
8) Ngôn ngữ giảng dạy	☒ Tiếng Việt ☐ Tiếng Anh
9) Phương thức giảng dạy	☒ Trực tiếp ☐ Trực tuyến ☐ Trực tiếp và trực tuyến

2. Mô tả tóm tắt học phần:

Học phần An toàn mạng là học phần bắt buộc trong khối kiến thức chuyên ngành của chương trình dạy học ngành An toàn thông tin được giảng dạy ở

học kỳ 7. Để có thể học tốt học phần này, người học cần nắm vững các kiến thức đã học trong học phần Mạng máy tính và Cơ sở An toàn thông tin. Học phần An toàn mạng sẽ trang bị cho người học các kiến thức cơ bản và chuyên sâu về các lỗ hổng, các dạng tấn công mạng và các giải pháp đảm bảo an toàn mạng. Nội dung chính của học phần tập trung vào các nguy cơ và lỗ hổng trong bảo mật mạng, các kỹ thuật tấn công của tin tặc và giải pháp phòng chống, các giải pháp phòng ngừa và đáp trả tấn công mạng. Bên cạnh đó, khi tham gia học phần này, người học được rèn luyện các kỹ năng cài đặt, triển khai, phân tích và đánh giá các giải pháp bảo mật, cũng như thực hành kỹ năng giao tiếp và làm việc nhóm trong khi thực hiện bài tập lớn.

3. Chuẩn đầu ra của học phần (CLOs)

3.1. Chuẩn đầu ra của học phần và mối liên hệ với các chỉ báo thuộc PLOs

Danh sách các PLO và bảng CM V0.5:
https://docs.google.com/spreadsheets/d/1jbfA5tnqT2ra7Vaoi7c5HhrXl8zbBslT/edit?gid=1389634614#gid=1389634614
PLO1: Áp dụng tri thức toán học, khoa học và công nghệ để xác định các giải pháp giải quyết các vấn đề phức hợp trong lĩnh vực an toàn thông tin.
PLO2: Thiết kế các giải pháp đáp ứng một tập hợp các yêu cầu cụ thể trong lĩnh vực an toàn thông tin.
PLO3: Áp dụng các kỹ thuật, công nghệ và công cụ bảo mật để giải quyết các vấn đề liên quan đến an toàn thông tin.

PLO4: Giao tiếp và hoạt động hiệu quả trong các nhóm đa ngành liên quan đến lĩnh vực an toàn thông tin.
PLO5: Nhận thức được vấn đề đạo đức và trách nhiệm nghề nghiệp trong lĩnh vực an toàn thông tin.

Sau khi kết thúc học phần, người học có khả năng:

STT	Chuẩn đầu ra học phần (CLOs)	Kiến thức Cognitive	Kỹ năng Psychomotor	Thái độ Affective	PLO

CLO1	Diễn giải được các nguy cơ và mối đe dọa trong bảo mật mạng, các kỹ thuật tấn công mạng và các giải pháp phòng ngừa	C2			X R PLO3
CLO2	Đánh giá được mức độ rủi ro bảo mật của hệ thống mạng	C5	P3		X R PLO2
CLO3	Triển khai được các giải pháp an toàn mạng cơ bản	C3	P3		X E PLO3
CLO4	Tham gia tích cực hoạt động nhóm, giao tiếp và hợp tác hiệu quả để thực hiện bài tập lớn học phần		P3	A2	X R PLO4

3.2. Hoạt động kiểm tra và hoạt động dạy học theo chuẩn đầu ra

CLOs	**Hình thức kiểm tra theo chuẩn đầu ra**					**Hình thức dạy học theo chuẩn đầu ra**			
	Trắc nghiệm	Báo cáo	Bài tập thực hành	Thuyết trình	Demo/ Trình diễn	Bài giảng	Làm việc nhóm	Thảo luận nhóm	Hướng dẫn thực hành
CLO1	x					x			x
CLO2		x	x	x	x	x	x	x	x
CLO3		x	x	x	x	x	x	x	x

CLO 4		x	x	x	x		x	x	

4. Kế hoạch kiểm tra theo chuẩn đầu ra

- Thang điểm đánh giá: Thang điểm 10

Thành phần kiểm tra	Hoạt động Kiểm tra	Hình thức kiểm tra	Trọng số (%)	Thời điểm kiểm tra (tuần)	CĐR HP (CLOs)
Kiểm tra quá trình (%) (formative assessment)	Kiểm tra (%)	Vấn đáp	10%	Trong các buổi học	
	Thực hành (%)	Báo cáo		Tuần 4-14	
	Kiểm tra giữa kỳ (%)	Trắc nghiệm	10%	Tuần 8-10	
Kiểm tra tổng kết (%) (summative assessment)	Thi cuối kỳ 1 (%)	Trắc nghiệm	30 %	Theo kế hoạch của trường	CLO1
	Thi cuối kỳ 2 (%)	Báo cáo, thuyết trình, demo bài tập lớn	50%	Theo kế hoạch của trường	CLO2, CLO3, CLO4

5. Kế hoạch dạy và học

TT	Nội dung chi tiết	Thời lượng (giờ định mức)				Hình thức và phương thức tổ chức dạy học	Kiểm tra (nếu có)	Đóng góp vào CLO
		Lý thuyết	Bài tập lớn	Thảo luận	Thực hành			

1	**Chương 1: Giới thiệu về an toàn mạng** 1.1. Các yêu cầu và phương pháp đảm bảo an toàn mạng 1.1.1. Các yêu cầu về đảm bảo an toàn mạng 1.1.2. Phương pháp đảm bảo an toàn mạng 1.2. Phân tích rủi ro và các mô hình phòng thủ 1.2.1. Xác định nguy cơ 1.2.2. Phân tích rủi ro 1.2.3. Các mô hình phòng thủ					**Chuẩn bị (Pre-class):** người học chuẩn bị trước nội dung của bài học thông qua tài liệu được cung cấp.		CLO1, CLO2, CLO3
		2				**Trên lớp (In-class)** - Hoạt động Dạy trên lớp: + Giảng viên giới thiệu đề cương và chuẩn đầu ra của môn học + Giảng viên giới thiệu các vấn đề về an toàn mạng, các phương pháp đảm bảo an toàn mạng và đưa ra yêu cầu về bài tập lớn theo nhóm + Giảng viên giới thiệu về phân tích rủi ro và các mô hình phòng thủ - Hoạt động Học trên lớp: người học lắng nghe và hiểu được các nội dung của bài học và yêu cầu bài tập lớn theo nhóm		
						Sau giờ học (Post-Class): Người học tìm hiểu thêm về các chủ đề bài tập lớn theo nhóm		
2	1.3. Tổ chức, quản lý an toàn 1.3.1. Vai trò và trách nhiệm					**Chuẩn bị (Pre-class):** người học chuẩn bị trước nội dung của bài học thông qua tài liệu được cung cấp.		CLO1, CLO2, CLO3

	1.3.2. Quản lý hoạt động an toàn 1.3.3. Đào tạo nhận thức an toàn mạng	2				**Trên lớp (In-class)** - Hoạt động Dạy trên lớp: Giảng viên giới thiệu, giải thích các nội dung của Tổ chức và quản lý an toàn. - Hoạt động Học trên lớp: người học lắng nghe và hiểu được các nội dung của bài học.		
						Sau giờ học (Post-Class): người học tìm hiểu thông tin về các khái niệm trong chương 1.		
3	**Chương 2: Các nguy cơ và lỗ hổng trong bảo mật mạng** 2.1. Các nguy cơ và lỗ hổng trong bảo mật giao thức 2.1.1. Các giao thức phổ biến tầng ứng dụng					**Chuẩn bị (Pre-class):** người học chuẩn bị trước nội dung của bài học thông qua tài liệu được cung cấp.		CLO1, CLO2, CLO3
		2				**Trên lớp (In-class)** - Hoạt động Dạy trên lớp: Giảng viên giới thiệu, giải thích các nội dung về Các nguy cơ và lỗ hổng trong bảo mật giao thức phổ biến tầng ứng dụng. - Hoạt động Học trên lớp: người học lắng nghe và hiểu được các nội dung của bài học.		

						Sau giờ học (Post-Class): người học thực hiện các bài tập về nhà được giao trên lớp.		
4	2.1.2. Giao thức DNS 2.1.3. Giao thức TCP/UDP					**Chuẩn bị (Pre-class):** người học chuẩn bị trước nội dung của bài học thông qua tài liệu được cung cấp.		CLO1, CLO2, CLO3
		2				**Trên lớp (In-class)** Hoạt động Dạy trên lớp: iảng viên giới thiệu, giải ích các nội dung về Các guy cơ và lỗ hổng trong ao thức DNS và CP/UDP. - Hoạt động Học trên lớp: người học lắng nghe và hiểu được các nội dung của bài học.		
			6			**Trên lớp (In-class)** - Hoạt động báo cáo tiến độ về bài tập lớn của các nhóm.		
						Sau giờ học (Post-Class): người học thực hiện các bài tập về nhà được giao trên lớp.		

5	2.1.4. Các giao thức định tuyến 2.1.5. Một số giao thức khác					**Chuẩn bị (Pre-class):** người học chuẩn bị trước nội dung của bài học thông qua tài liệu được cung cấp.		CLO1, CLO2, CLO3
		2				**Trên lớp (In-class)** - Hoạt động Dạy trên lớp: Giảng viên giới thiệu, giải thích các nội dung về Các nguy cơ và lỗ hổng trong giao thức định tuyến và một số giao thức khác. - Hoạt động Học trên lớp: người học lắng nghe và hiểu được các nội dung của bài học.		
						Sau giờ học (Post-Class): người học thực hiện các bài tập về nhà được giao trên lớp.		
6	2.2. Phân tích và thiết kế giao thức an toàn					**Chuẩn bị (Pre-class):** người học chuẩn bị trước nội dung của bài học thông qua tài liệu được cung cấp.		CLO1, CLO2, CLO3, CLO4

		2				**Trên lớp (In-class)** - Hoạt động Dạy trên lớp: Giảng viên giới thiệu, giải thích các nội dung về phân tích hoạt động của giao thức và phương pháp thiết kế giao thức an toàn. - Hoạt động Học trên lớp: người học lắng nghe và hiểu được các nội dung của bài học.		
					4	**Trên lớp (In-class)** - Hoạt động thực hành: người học thực hành trên lớp về phân tích giao thức dựa trên bắt gói tin trên mạng		
						Sau giờ học (Post-Class): người học làm báo cáo thực hành và thực hiện các bài tập về nhà.		
7	2.3. Các nguy cơ và lỗ hổng trong bảo mật thiết bị mạng 2.3.1. Thiết bị chuyển mạch					**Chuẩn bị (Pre-class):** người học chuẩn bị trước nội dung của bài học thông qua tài liệu được cung cấp.		CLO1, CLO2, CLO3

	2.3.2. Thiết bị định tuyến 2.3.3. Một số thiết bị khác	2				**Trên lớp (In-class)** - Hoạt động Dạy trên lớp: Giảng viên giới thiệu, giải thích các nội dung về các nguy cơ và lỗ hổng trong bảo mật thiết bị mạng. - Hoạt động Học trên lớp: người học lắng nghe và hiểu được các nội dung của bài học.		
						Sau giờ học (Post-Class): người học thực hiện các bài tập về nhà được giao trên lớp.		
8	**Chương 3: Các kỹ thuật tấn công mạng** 3.1. Kỹ thuật do thám 3.1.1. Giới thiệu về kỹ thuật do thám 3.1.2. Do thám DNS 3.1.3. Thu thập và kiểm tra các tên miền và thông tin địa chỉ IP 3.1.4. Do thám sử dụng					**Chuẩn bị (Pre-class):** người học chuẩn bị trước nội dung của bài học thông qua tài liệu được cung cấp.		CLO1, CLO2, CLO3
		2				**Trên lớp (In-class)** - Hoạt động Dạy trên lớp: Giảng viên giới thiệu, giải thích các nội dung về Các kỹ thuật do thám. - Hoạt động Học trên lớp: người học lắng nghe và hiểu được các nội dung của bài học.		CLO2,

	các máy tìm kiếm		6			**Trên lớp (In-class)** - Hoạt động báo cáo tiến độ bài tập lớn		CLO3, CLO4
						Sau giờ học (Post-Class): người học thực hiện các bài tập về nhà được giao trên lớp.		
9	3.2. Kỹ thuật rà quét 3.2.1. Giới thiệu về kỹ thuật rà quét 3.2.2. Xác định các host hoạt động 3.2.3. Xác định các cổng và dịch vụ hoạt động 3.2.4. Xác định hệ điều hành 3.2.5. Rà quét các lỗ hổng					**Chuẩn bị (Pre-class):** người học chuẩn bị trước nội dung của bài học thông qua tài liệu được cung cấp.		CLO1, CLO2, CLO3, CLO4
		2				**Trên lớp (In-class)** - Hoạt động Dạy trên lớp: Giảng viên giới thiệu, giải thích các nội dung về Các kỹ thuật rà quét trong mạng. - Hoạt động Học trên lớp: người học lắng nghe và hiểu được các nội dung của bài học.		
					4	**Trên lớp (In-class)** - Hoạt động thực hành: người học thực hiện thực hành các công cụ phần mềm để rà quét mạng.		

						Sau giờ học (Post-Class): người học làm báo cáo thực hành và thực hiện các bài tập về nhà.		
10	3.3. Kỹ thuật xâm nhập 3.3.1. Xâm nhập hệ thống máy khách 3.3.2. Kỹ thuật vượt qua tường lửa và tránh bị phát hiện					**Chuẩn bị (Pre-class):** người học chuẩn bị trước nội dung của bài học thông qua tài liệu được cung cấp.		CLO1, CLO2, CLO3
		2				**Trên lớp (In-class)** - Hoạt động Dạy trên lớp: Giảng viên giới thiệu, giải thích các nội dung về Các kỹ thuật xâm nhập. - Hoạt động Học trên lớp: người học lắng nghe và hiểu được các nội dung của bài học.		
						Sau giờ học (Post-Class): người học thực hiện các bài tập về nhà được giao trên lớp.		
11	3.4. Tấn công từ chối dịch vụ 3.4.1. Tấn công từ chối					**Chuẩn bị (Pre-class):** người học chuẩn bị trước nội dung của bài học thông qua tài liệu được cung cấp.		CLO1, CLO2, CLO3, CLO4

	dịch vụ tại tầng liên kết 3.4.2. Tấn công từ chối dịch vụ tại tầng giao vận 3.4.3. Tấn công từ chối dịch vụ tại tầng ứng dụng	2				**Trên lớp (In-class)** - Hoạt động Dạy trên lớp: Giảng viên giới thiệu, giải thích các nội dung về kỹ thuật tấn công từ chối dịch vụ. - Hoạt động Học trên lớp: người học lắng nghe và hiểu được các nội dung của bài học.		
					4	**Trên lớp (In-class)** - Hoạt động thực hành: thử nghiệm tấn công từ chối dịch vụ và cách phòng chống.		
						Sau giờ học (Post-Class): người học làm báo cáo thực hành và thực hiện các bài tập về nhà.		
12	**Chương 4: Các giải pháp phòng ngừa và đáp trả tấn công**					**Chuẩn bị (Pre-class):** người học chuẩn bị trước nội dung của bài học thông qua tài liệu được cung cấp.		CLO1, CLO2, CLO3, CLO4

	4.1. Các giải pháp phòng ngừa, ngăn chặn tấn công 4.1.1 Đảm bảo an toàn môi trường vật lý 4.1.2 Cập nhật bản vá 4.1.3 Đảm bảo an toàn cho người dùng 4.1.4 Đảm bảo an toàn cho hệ thống tập tin 4.1.5 Xây dựng kế hoạch phòng ngừa **Kiểm tra giữa kỳ**	2				**Trên lớp (In-class)** - Hoạt động Dạy trên lớp: Giảng viên giới thiệu, giải thích các nội dung về Các giải pháp phòng ngừa, ngăn chặn tấn công. - Hoạt động Học trên lớp: người học lắng nghe và hiểu được các nội dung của bài học.		
			6			**Trên lớp (In-class)** **- Hoạt động kiểm tra giữa kỳ**: báo cáo giữa kỳ bài tập lớn theo nhóm	X	
						Sau giờ học (Post-Class): người học thực hiện các bài tập về nhà được giao trên lớp.	X	
13	4.2. Các phương pháp đáp trả tấn công					**Chuẩn bị (Pre-class):** người học chuẩn bị trước nội dung của bài học thông qua tài liệu được cung cấp.		CLO1, CLO2, CLO3

	4.2.1 Lập kế hoạch đáp trả tấn công 4.2.2 Điều tra 4.2.3 Công cụ pháp luật	2				**Trên lớp (In-class)** - Hoạt động Dạy trên lớp: Giảng viên giới thiệu, giải thích các nội dung về Các phương pháp đáp trả tấn công. - Hoạt động Học trên lớp: người học lắng nghe và hiểu được các nội dung của bài học.		
				4		**Trên lớp (In-class)** - Hoạt động thảo luận: sinh viên thảo luận theo nhóm về các cách thức hiệu quả để đáp trả tấn công trong thực tế.		
						Sau giờ học (Post-Class): người học thực hiện các bài tập về nhà được giao trên lớp.		
14	4.3. Khôi phục sau sự cố và tiếp tục hoạt động					**Chuẩn bị (Pre-class):** người học chuẩn bị trước nội dung của bài học thông qua tài liệu được cung cấp.		CLO1, CLO2, CLO3

	4.3.1 Khôi phục sau sự cố 4.3.2 Kế hoạch đảm bảo tiếp tục hoạt động	2				**Trên lớp (In-class)** - Hoạt động Dạy trên lớp: Giảng viên giới thiệu, giải thích các nội dung về Khôi phục sau sự cố và tiếp tục hoạt động. - Hoạt động Học trên lớp: người học lắng nghe và hiểu được các nội dung của bài học.		
						Sau giờ học (Post-Class): người học thực hiện các bài tập về nhà được giao trên lớp.		
15	Ôn tập và trả lời câu hỏi					**Chuẩn bị (Pre-class):** người học chuẩn bị trước nội dung của bài học thông qua tài liệu được cung cấp.		CLO1, CLO2, CLO3
		2				**Trên lớp (In-class)** - Hoạt động Dạy trên lớp: Giảng viên đưa ra các câu hỏi ôn tập và trả lời câu hỏi của người học. - Hoạt động Học trên lớp: Người học nghiên cứu các câu hỏi ôn tập, trao đổi và hỏi giảng viên.		

				2		**Trên lớp (In-class)** - Hoạt động tự học: sinh viên trao đổi thêm về các câu hỏi ôn tập		
						Sau giờ học (Post-Class): người học tìm hiểu và trả lời các câu hỏi ôn tập.		
	Tổng số giờ	**30**	**18**	**6**	**12**			

6. Nhiệm vụ của người học:

Người học phải thực hiện các nhiệm vụ sau đây:

- Tham gia nghe giảng và tương tác theo quy định của lớp học phần;
- Tham gia các hoạt động làm việc nhóm theo quy định của lớp học phần;
- Tự tìm hiểu các vấn đề do giảng viên giao để thực hiện ngoài giờ học trên lớp;
- Hoàn thành tất cả bài đánh giá của học phần.
- Người học phải tôn trọng giảng viên và người học khác, phải thực hiện quy định liêm chính học thuật của Nhà trường, phải chấp hành các quy định, nội quy của Nhà trường.

7. Tài liệu học tập

7.1. Tài liệu chính

1. Roberta Bragg, Mark Rhodes-Ousley and Keith Strassberg, Network Security: The Complete Reference, McGraw-Hill Osborne Media, 2013.

7.2. Tài liệu tham khảo

1. John Chirillo, Hack attacks revealed: A complete reference with custom security hacking toolkit, John Wiley & Sons, 2001.
2. Jie Wang, Computer Network Security: Theory and Practice, Springer, 2009.
3. Michael T. Simpson, Kent Backman, Hands-On Ethical Hacking and Network Defense, Delmar Cengage Learning, 2010.
4. Stuart McClure, Joel Scambray and George Kurtz, Hacking Exposed 7: Network Security Secrets & Solutions, McGraw-Hill Osborne Media, 2012.
5. William Stallings, Cryptography and Network Security Principles And Practice, 7th edition, Pearson Education Limited, 2017.

Phụ lục 01 - ĐCCT

BẢNG MA TRẬN VÀ THANG ĐO

Bảng 1 - Quan hệ giữa chuẩn đầu ra học phần và chuẩn đầu ra chương trình đào tạo

	PLOs				
	PLO1	PLO2	PLO3	PLO4	PLO5
CLO 1			X R		
CLO 2		X R			
CLO 3			X E		
CLO 4				X R	

Bảng 2 - Thang đánh giá chuẩn đầu ra (CLO)

CLO1: Diễn giải được các nguy cơ và mối đe dọa trong bảo mật mạng, các kỹ thuật tấn công mạng và các giải pháp phòng ngừa (C2)

Thang đánh giá	Fail - Below Expectation < 40%	Beginning - Needs mprovement 40%-54%	Developing - Marginally Adequate 55%-69%	Sufficient - Meet Expectation 70%-84%	Exemplary- Exceeds Expectation 85% - 100%
Tiêu chí					
1.1. Giải thích được các nguy cơ, lỗ hổng trong bảo mật mạng và các kỹ thuật tấn công của tin tặc	Trả lời đúng <40% số câu hỏi (đã phân bổ đều theo nội dung)	Trả lời đúng từ 40% đến <55% số câu hỏi (đã phân bổ đều theo nội dung)	Trả lời đúng từ 55% đến <70% số câu hỏi (đã phân bổ đều theo nội dung)	Trả lời đúng từ 70% đến <85% số câu hỏi (đã phân bổ đều theo nội dung)	Trả lời đúng từ 85% số câu hỏi (đã phân bổ đều theo nội dung) trở lên
1.2. Giải thích được các giải pháp phòng chống, các giải pháp phòng ngừa và đáp trả tấn công mạng	Trả lời đúng <40% số câu hỏi (đã phân bổ đều theo nội dung)	Trả lời đúng từ 40% đến <55% số câu hỏi (đã phân bổ đều theo nội dung)	Trả lời đúng từ 55% đến <70% số câu hỏi (đã phân bổ đều theo nội dung)	Trả lời đúng từ 70% đến <85% số câu hỏi (đã phân bổ đều theo nội dung)	Trả lời đúng từ 85% số câu hỏi (đã phân bổ đều theo nội dung) trở lên

CLO2: Đánh giá được mức độ rủi ro bảo mật của hệ thống mạng (C5-P3; PLO2-XR)

Thang đánh giá	Fail - Below Expectation < 40%	Beginning - Needs Improvement 40%-54%	Developing - Marginally Adequate 55%-69%	Sufficient - Meet Expectation 70%-84%	Exemplary- Exceeds Expectation 85% - 100%
Tiêu chí					
2.1. Xác định các rủi ro bảo mật đối với một hệ thống mạng cụ thể	Không thể xác định được các rủi ro bảo mật	Chỉ xác định được một số rủi ro bảo mật, còn thiếu nhiều rủi ro bảo mật	Xác định đa số rủi ro bảo mật, nhưng còn thiếu một số rủi ro bảo mật	Xác định đầy đủ các rủi ro bảo mật	Xác định đầy đủ và chi tiết các rủi ro bảo mật

2.2. Phân ích, đánh giá mức độ rủi ro bảo mật đối với hệ thống mạng	Không thể phân tích và đánh giá được mức độ rủi ro bảo mật	Chỉ phân tích và đánh giá được mức độ rủi ro một cách sơ sài	Phân tích và đánh giá tương đối đầy đủ mức độ rủi ro bảo mật, nhưng còn thiếu một số rủi ro bảo mật	Phân tích và đánh giá đầy đủ mức độ rủi ro bảo mật	Phân tích và đánh giá đầy đủ và chi tiết mức độ rủi ro bảo mật

CLO3: Triển khai được các giải pháp an toàn mạng cơ bản (C3-P3)

hang ánh giá	Fail - Below Expectation < 40%	Beginning - Needs Improvement 40%-54%	Developing - Marginally Adequate 55%-69%	fficient - Meet Expectation 70%-84%	Exemplary- Exceeds Expectation 85% - 100%
u chí					
.1. Lựa họn giải háp	hông thể ra chọn giải háp an toàn ạng phù ợp cho tình uống cụ thể.	ựa chọn giải háp chưa phù ợp với yêu cầu ảo mật hoặc hả năng triển hai thực tế.	ựa chọn được iải pháp an àn mạng phù ợp cho tình uống cụ thể, hưng chưa tối u.	ựa chọn được iải pháp an àn mạng phù ợp và tối ưu ho tình huống ụ thể.	ựa chọn được giải háp an toàn mạng hù hợp và tối ưu, ồng thời đưa ra ược lý do lựa họn trên cơ sở so ánh với các giải háp khác.
.2. riển hai giải háp	hông thể iển khai giải háp an toàn ạng đã họn.	riển khai giải háp gặp nhiều ỗi, chưa hoàn hiện, hoặc hông đúng quy ình.	riển khai được iải pháp an àn mạng đã họn, nhưng òn một số lỗi hỏ.	riển khai giải háp an toàn ạng đã chọn ột cách chính ác và hiệu quả.	riển khai giải pháp n toàn mạng đã họn một cách hính xác, hiệu quả, à tối ưu hóa hiệu ăng hoạt động.

CLO4: Tham gia tích cực hoạt động nhóm, giao tiếp và hợp tác hiệu quả để thực hiện bài tập lớn học phần (P3-A2)

Thang đánh giá	Fail - Below pectation < 40%	Beginning - Needs nprovement 40%-54%	eveloping - Marginally Adequate 55%-69%	Sufficient - Meet Expectation 70%-84%	Exemplary- Exceeds xpectation 5% - 100%
Tiêu chí					

. Mức độ tham gia và ng góp vào hoạt động óm	hông tham các hoạt ng nhóm; ông hoàn nh đúng n, hoặc chất ợng hầu hết ần việc ợc giao ông đạt	am gia một hoạt động óm, nhưng thụ động; àn thành và m bảo chất ợng một số ần việc được ao, nhưng iều việc chưa t chất lượng, ặc chưa đúng n	am gia đa số ạt động óm, nhưng h thụ động; àn thành và m bảo chất ợng đa số ần việc được ao, nhưng ột số việc ưa đạt chất ợng, hoặc ưa đúng hạn	n sàng tham đầy đủ các ạt động óm; hoàn nh đúng hạn đảm bảo ất lượng các ần việc được ao	ủ động, sẵn ng tham gia c hoạt động óm; hoàn nh đúng hạn đạt chất ợng xuất sắc c phần việc ợc giao
. Khả năng giao tiếp và p tác	ỉ có khả ng giao tiếp hợp tác ở ức rất yếu	ao tiếp cơ n, hỗ trợ các ành viên khác hoàn thành ng việc ung hạn chế	ao tiếp cơ n, hỗ trợ các ành viên khác hoàn thành ng việc ung, nhưng ưa chủ động	ao tiếp hiệu ả, sẵn sàng trợ các thành ên khác để àn thành ng việc ung	ao tiếp chủ ng, tích cực trợ các ành viên khác hoàn thành ng việc ung
. Yêu cầu với báo cáo, uyết trình và demo	Báo cáo ưa đúng nh dạng, i dung ếu mục Thuyết trình u: không nh bày rõ i dung Demo (nếu) không ạt động, ặc rất nhiều	Báo cáo cơ n đúng định ng, bố cục ưa hợp lý, i dung cơ n đủ các mục ính Thuyết trình: ỉ trình bày ợc một số Demo (nếu): một số các h năng hoạt ng, còn nhiều	Báo cáo cơ n đúng định ng, bố cục ợng đối hợp nội dung đủ c mục chính Thuyết trình: nh bày được c ý chính Demo (nếu): đa số các h năng hoạt ng, còn một lỗi	Báo cáo đúng nh dạng, bố c hợp lý, nội ng đủ các ục Thuyết trình ạch lạc, trình y được các ý ính Demo (nếu): đủ các tính ng hoạt động	Báo cáo đúng nh dạng, bố c hợp lý, nội ng đủ các ục Thuyết trình ất sắc, trình y đầy đủ nội ng Demo (nếu): đầy đủ các h năng, đúng u cầu hoạt ng