

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

## 1. Thông tin chung về học phần

<b>1) Mã học phần:</b>	INT1482
<b>2) Số tín chỉ:</b>	3
<b>3) Hoạt động học tập</b>	
- 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
<b>4) Điều kiện tham gia học phần:</b>	
- Học phần tiên quyết:	Cơ sở An toàn thông tin
- Học phần học trước:	Mạng máy tính
<b>5) Các giảng viên phụ trách học phần:</b>	
- Giảng viên phụ trách chính:	TS. Nguyễn Ngọc Điện
- 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

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

<b>6) Loại học phần:</b>	<input checked="" type="checkbox"/> Bắt buộc <input type="checkbox"/> Tự chọn tự do <input type="checkbox"/> Tự chọn theo định hướng (bắt buộc)
<b>7) Thuộc thành phần học tập</b>	<input type="checkbox"/> Giáo dục đại cương (chung, khoa học cơ bản, kỹ năng) <input type="checkbox"/> Cơ sở khối ngành (nhóm ngành/lĩnh vực) <input type="checkbox"/> Cơ sở ngành <input type="checkbox"/> Ngành <input checked="" type="checkbox"/> Chuyên ngành <input type="checkbox"/> Bổ trợ
<b>8) Ngôn ngữ giảng dạy</b>	<input checked="" type="checkbox"/> Tiếng Việt <input type="checkbox"/> Tiếng Anh
<b>9) Phương thức giảng dạy</b>	<input checked="" type="checkbox"/> Trực tiếp <input type="checkbox"/> Trực tuyến <input type="checkbox"/> 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

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

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	<b>Chuẩn đầu ra học phần (CLOs)</b>	Kiến thức Cognitive	Kỹ năng Psychomotor	Thái độ Affective	<b>PLO</b>
-----	-------------------------------------	---------------------	---------------------	-------------------	------------

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

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

CLO s	Hình thức kiểm tra theo chuẩn đầu ra					Hình thức dạy học theo chuẩn đầu ra			
	Trắc nghiệm	Báo cáo	Bài tập thực hành	Thu yết trình	Đem o/ Trình diễn	Bài giảng	Làm việc nhóm	Thảo luận nhóm	Hướng dẫn thực hành
CLO 1	x					x			x

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

CLO 2		x	x	x	x	x	x	x	x	x
CLO 3		x	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)	CDR 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

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

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	<b>Chương 1: Giới thiệu về an toàn mạng</b>					<b>Chuẩn bị (Pre-class):</b> người học chuẩn bị trước nội dung của bài học thông qua tài liệu được cung cấp.		CLO1, CLO2, CLO3
	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	2				<b>Trên lớp (In-class)</b>  - 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		

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

	1.2.3. Các mô hình phòng thủ				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 1.3.2. Quản lý hoạt động an toàn 1.3.3. Đào tạo nhận thức an toàn mạng				<b>Chuẩn bị (Pre-class):</b> người học chuẩn bị trước nội dung của bài học thông qua tài liệu được cung cấp.	CLO1, CLO2, CLO3
		2			<b>Trên lớp (In-class)</b> <ul style="list-style-type: none"> <li>- Hoạt động Dạy trên lớp: Giảng viên giới thiệu, giải thích các nội dung của Tổ chức và quản lý an toàn.</li> <li>- Hoạt động Học trên lớp: người học lắng nghe và hiểu được các nội dung của bài học.</li> </ul>	
3	<b>Chương 2: Các nguy cơ và lỗ hổng</b>				Sau giờ học (Post-Class): người học tìm hiểu thông tin về các khái niệm trong chương 1.	

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

<b>trong bảo mật mạng</b>  2.1. Các nguy cơ và lỗ hổng trong bảo mật giao thức 2.1.1. Các giao thức phổ biến tầng ứng dụng	2	học thông qua tài liệu được cung cấp.			CLO1, CLO2, CLO3
		<b>Trên lớp (In-class)</b> <ul style="list-style-type: none"> <li>- 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.</li> <li>- Hoạt động Học trên lớp: người học lắng nghe và hiểu được các nội dung của bài học.</li> </ul>			
		<b>Sau giờ học (Post-Class):</b> 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				<b>Chuẩn bị (Pre-class):</b> người học chuẩn bị trước nội dung của bài học thông qua tài liệu được cung cấp.	CLO1, CLO2, CLO3

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

		2			<p><b>Trên lớp (In-class)</b></p> <p>Hoạt động Dạy trên lớp: giảng viên giới thiệu, giải thích các nội dung về Các guy cơ và lỗ hổng trong giao thức DNS và TCP/UDP.</p> <p>- Hoạt động Học trên lớp: người học lắng nghe và hiểu được các nội dung của bài học.</p>	
		6			<p><b>Trên lớp (In-class)</b></p> <p>- Hoạt động báo cáo tiến độ về bài tập lớn của các nhóm.</p>	
					<p><b>Sau giờ học (Post-Class):</b> người học thực hiện các bài tập về nhà được giao trên lớp.</p>	
5	2.1.4. Các giao thức định tuyến 2.1.5. Một số giao thức khác				<p><b>Chuẩn bị (Pre-class):</b> người học chuẩn bị trước nội dung của bài học thông qua tài liệu được cung cấp.</p>	CLO1, CLO2, CLO3

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

		2			<p><b>Trên lớp (In-class)</b></p> <ul style="list-style-type: none"> <li>- 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.</li> <li>- Hoạt động Học trên lớp: người học lắng nghe và hiểu được các nội dung của bài học.</li> </ul> <p><b>Sau giờ học (Post-Class):</b> người học thực hiện các bài tập về nhà được giao trên lớp.</p>	
6	2.2. Phân tích và thiết kế giao thức an toàn				<p><b>Chuẩn bị (Pre-class):</b> người học chuẩn bị trước nội dung của bài học thông qua tài liệu được cung cấp.</p>	CLO1, CLO2, CLO3, CLO4

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

		2			<b>Trên lớp (In-class)</b>  - 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		<b>Trên lớp (In-class)</b>  - Hoạt động thực hành: người học thực hành trên lớp về phân tích giao thức dựa trên bắt gói tin trên mạng	
					<b>Sau giờ học (Post-Class):</b> 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				<b>Chuẩn bị (Pre-class):</b> người học chuẩn bị trước nội dung của bài học thông qua tài liệu được cung cấp.	CLO1, CLO2, CLO3

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

				<b>Trên lớp (In-class)</b>	
				<ul style="list-style-type: none"> <li>- 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.</li> <li>- Hoạt động Học trên lớp: người học lắng nghe và hiểu được các nội dung của bài học.</li> </ul>	
				<b>Sau giờ học (Post-Class):</b> người học thực hiện các bài tập về nhà được giao trên lớp.	
8	<b>Chương 3:</b> <b>Các kỹ thuật tấn công mạng</b>  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			<b>Chuẩn bị (Pre-class):</b> người học chuẩn bị trước nội dung của bài học thông qua tài liệu được cung cấp.	CLO1, CLO2, CLO3
		2		<b>Trên lớp (In-class)</b> <ul style="list-style-type: none"> <li>- Hoạt động Dạy trên lớp: Giảng viên giới thiệu, giải thích các nội dung về Các kỹ thuật do thám.</li> <li>- Hoạt động Học trên lớp: người học lắng nghe</li> </ul>	

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

	miền và thông tin địa chỉ IP 3.1.4. Do thám sử dụng các máy tìm kiếm				và hiểu được các nội dung của bài học.		CLO2, CLO3, CLO4
		6			<b>Trên lớp (In-class)</b>  - Hoạt động báo cáo tiến độ bài tập lớn		
					<b>Sau giờ học (Post-Class):</b> 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				<b>Chuẩn bị (Pre-class):</b> người học chuẩn bị trước nội dung của bài học thông qua tài liệu được cung cấp.		CLO1, CLO2, CLO3, CLO4

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

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	2			<b>Trên lớp (In-class)</b>  - 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	<b>Trên lớp (In-class)</b>  - Hoạt động thực hành: người học thực hiện thực hành các công cụ phần mềm để rà quét mạng.	
				<b>Sau giờ học (Post-Class):</b> 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	Chuẩn bị (Pre-class):		Chuẩn bị (Pre-class): người học chuẩn bị trước nội dung của bài học thông qua tài liệu được cung cấp.	CLO1, CLO2, CLO3

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

	3.3.2. Kỹ thuật vượt qua tường lửa và tránh bị phát hiện	2		<b>Trên lớp (In-class)</b> <ul style="list-style-type: none"> <li>- Hoạt động Dạy trên lớp: Giảng viên giới thiệu, giải thích các nội dung về Các kỹ thuật xâm nhập.</li> <li>- Hoạt động Học trên lớp: người học lắng nghe và hiểu được các nội dung của bài học.</li> </ul>	
				<b>Sau giờ học (Post-Class):</b> 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 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		<b>Chuẩn bị (Pre-class):</b> người học chuẩn bị trước nội dung của bài học thông qua tài liệu được cung cấp.	CLO1, CLO2, CLO3, CLO4

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

					và hiểu được các nội dung của bài học.	
				4	<p><b>Trên lớp (In-class)</b></p> <ul style="list-style-type: none"> <li>- Hoạt động thực hành: thử nghiệm tấn công từ chối dịch vụ và cách phòng chống.</li> </ul>	
					<p><b>Sau giờ học (Post-Class):</b> người học làm báo cáo thực hành và thực hiện các bài tập về nhà.</p>	
12	<b>Chương 4:</b> <b>Các giải pháp phòng ngừa và đáp trả tấn công</b>				<p><b>Chuẩn bị (Pre-class):</b> người học chuẩn bị trước nội dung của bài học thông qua tài liệu được cung cấp.</p>	CLO1, CLO2, CLO3, CLO4

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

<p>4.1. Các giải pháp phòng ngừa, ngăn chặn tấn công</p> <p>    4.1.1 Đảm bảo an toàn môi trường vật lý</p> <p>    4.1.2 Cập nhật bản vá</p> <p>    4.1.3 Đảm bảo an toàn cho người dùng</p> <p>    4.1.4 Đảm bảo an toàn cho hệ thống tập tin</p> <p>    4.1.5 Xây dựng kế hoạch phòng ngừa</p> <p><b>Kiểm tra giữa kỳ</b></p>	<p>2</p>	<p></p>	<p></p>	<p><b>Trên lớp (In-class)</b></p> <ul style="list-style-type: none"> <li>- Hoạt động Dạy trên lớp: Giảng viên giới thiệu, giải thích các nội dung về Các giải pháp phòng ngừa, ngăn chặn tấn công.</li> <li>- Hoạt động Học trên lớp: người học lắng nghe và hiểu được các nội dung của bài học.</li> </ul>	
	<p>6</p>	<p></p>	<p><b>Trên lớp (In-class)</b></p> <ul style="list-style-type: none"> <li>- <b>Hoạt động kiểm tra giữa kỳ:</b> báo cáo giữa kỳ bài tập lớn theo nhóm</li> </ul>	<p>X</p>	
	<p></p>	<p></p>	<p><b>Sau giờ học (Post-Class):</b> người học thực hiện các bài tập về nhà được giao trên lớp.</p>	<p>X</p>	
<p>13</p>	<p>4.2. Các phương pháp đáp trả tấn công</p>	<p></p>	<p><b>Chuẩn bị (Pre-class):</b> người học chuẩn bị trước nội dung của bài học thông qua tài liệu được cung cấp.</p>	<p>CLO1, CLO2, CLO3</p>	

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

4.2.1 Lập kế hoạch đáp trả tấn công 4.2.2 Điều tra 4.2.3 Công cụ pháp luật	2			<b>Trên lớp (In-class)</b>  - 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	<b>Trên lớp (In-class)</b>  - Hoạt động thảo luận: sinh viên thảo luận theo nhóm về các cách thức hiệu quả để đáp trả tấn công trong thực tế.	
				<b>Sau giờ học (Post-Class):</b> 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)		<b>Chuẩn bị (Pre-class):</b> người học chuẩn bị trước nội dung của bài học thông qua tài liệu được cung cấp.	CLO1, CLO2, CLO3

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

	4.3.1 Khôi phục sau sự cố 4.3.2 Kế hoạch đảm bảo tiếp tục hoạt động	2	<p><b>Trên lớp (In-class)</b></p> <ul style="list-style-type: none"> <li>- 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.</li> <li>- Hoạt động Học trên lớp: người học lắng nghe và hiểu được các nội dung của bài học.</li> </ul>			
			<p><b>Sau giờ học (Post-Class):</b> người học thực hiện các bài tập về nhà được giao trên lớp.</p>			
15	Ôn tập và trả lời câu hỏi		<p><b>Chuẩn bị (Pre-class):</b> người học chuẩn bị trước nội dung của bài học thông qua tài liệu được cung cấp.</p>			CLO1, CLO2, CLO3
			<p><b>Trên lớp (In-class)</b></p> <ul style="list-style-type: none"> <li>- Hoạt động Dạy trên lớp: Giảng viên đưa ra các câu hỏi ôn tập và trả lời câu hỏi của người học.</li> <li>- Hoạt động Học trên lớp: Người học nghiên cứu các câu hỏi ôn tập,</li> </ul>			

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

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

## 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.

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

- 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.