BAN CƠ YẾU CHÍNH PHỦ
HỌC VIỆN KỸ THUẬT MẬT MÃ

LẠI MINH TUẤN, CAO MINH TUẤN, ĐỒNG THỊ THÙY LINH

NGÂN HÀNG CÂU HỎI THI TRẮC NGHIỆM

KIỂM THỬ & ĐÁNH GIÁ ATHTTT

Hà Nội, 2021

PHẦN I. TỔNG HỢP CÁC PHẦN NỘI DUNG MÔN HỌC

Môn học: Kiểm thử & Đánh giá ATHTTT

Khoa: An toàn thông tin

Các chương trình đào tạo có sử dụng môn học:

P1: ĐH Chính quy An toàn thông tin

Các phần nội dung môn học trong các chương trình đào tạo:

TT	Phần nội dung	P1
1	Tổng quan về kiểm thử & đánh giá ATHTTT	☑
2	Thu thập thông tin và xác định lỗ hổng	☑
3	Kiểm thử hệ thống	☑
4	Kiểm thử máy chủ và ứng dụng Web	☑
5	Kiểm thử mạng không dây	☑
6	Lập báo cáo	☑

PHẦN II. TRÍCH LƯỢC ĐỀ CƯƠNG CHI TIẾT MÔN HỌC

1. Thông tin chung

Tên học phần	Kiểm thử và đánh giá an toàn hệ thống thông tin
Tên tiếng Anh	Penetration Testing and Information Security Assessment
Số tín chỉ	3
Học phần học trước	Mạng máy tính, cơ sở an toàn thông tin

2. Mục tiêu học phần

2.1.Mục tiêu chung

Học phần này cung cấp kiến thức cơ bản về kiểm thử và đánh giá an toàn thông tin, các phương pháp và quy trình khi thực hiện kiểm thử. Đồng thời học phần này cũng cung cấp cho sinh viên các kỹ năng để sinh viên có thể thực hiện các kiểm thử cho một hệ thống mạng, hệ thống ứng dụng web phục vụ định hướng nghề nghiệp cho sinh viên sau này.

2.2.Mục tiêu cụ thể

Mục tiêu	Mô tả
M1	Nắm được khái niệm, kiến thức căn bản về kiểm thử, đánh giá và kiểm định an toàn hệ thống thông tin. Phân biệt một cách rõ ràng các thuật ngữ cũng như nhiệm vụ của từng phương pháp.
M2	Hiểu được phương pháp luận và các kỹ thuật trong kiểm thử, đánh giá an toàn hệ thống thông tin
M3	Biết được cách thức thu thập thông tin, dò quét và xác định lỗ hổng khi thực hiện kiểm thử
M4	Nắm được các công việc cần thực hiện khi kiểm thử an toàn cho hệ thống
M5	Nắm được các công việc cần thực hiện khi kiểm thử an toàn cho máy chủ và ứng dụng web
M6	Nắm được các công việc cần thực hiện khi kiểm thử an toàn cho mạng không dây
M7	Có kỹ năng thực hiện kiểm thử cho một hệ thống hoặc website
M8	Hiểu về cách thức lập báo cáo kiểm thử
M9	Có kỹ năng nghiên cứu tài liệu, đọc dịch các tài liệu bằng ngôn ngữ tiếng Anh
M10	Có khả năng làm việc độc lập hoặc làm việc nhóm

3. Mô tả học phần

Học phần bao gồm 6 chương. Chương 1 giới thiệu các khái niệm cơ bản về kiểm thử, đánh giá, kiểm định an toàn thông tin và giới thiệu về các phương pháp luận, kỹ thuật cũng như một số lưu ý khi kiểm thử và đánh giá an toàn hệ thống thông tin. Chương 2 giới thiệu về kỹ thuật thu thập thông tin và xác định lỗ hổng khi thực hiện kiểm thử. Chương 3 giới thiệu kỹ thuật và các nhiệm vụ cần thực hiện khi thực hiện kiểm thử hệ thống. Chương 4 giới thiệu quy trình và các vấn đề cần lưu ý khi kiểm thử máy chủ web, ứng dụng web. Chương 5 giới thiệu các nhiệm vụ cần

thực hiện khi kiểm thử mạng không dây. Chương 6 giới thiệu về cách thức tổng hợp và lập báo cáo kiểm thử.

4. Nội dung học phần

Chương 1. Tổng quan về kiểm thử và đánh giá an toàn hệ thống thông tin (6 LT)

1.1. Các khái niệm cơ bản

1.1.1. Mối đe dọa an toàn thông tin

1.1.2. Lỗ hổng an toàn thông tin

1.1.3. Điểm yếu an toàn thông tin

1.1.4. Kiểm thử an toàn thông tin

1.1.5. Đánh giá an toàn thông tin

1.1.6. Kiểm định an toàn thông tin

1.2. Phương pháp luận kiểm thử và đánh giá an toàn hệ thống thông tin

1.2.1. NIST 800-115

1.2.2. ISSAF

1.2.3. OSSTMM

1.3. Kỹ thuật kiểm thử và đánh giá an toàn hệ thống thông tin

1.3.1. Hộp đen

1.3.2. Hộp trắng

1.3.3. Hộp xám

1.4. Một số lưu ý khi thực hiện kiểm thử và đánh giá an toàn hệ thống thông tin

1.4.1. Giai đoạn lập kế hoạch

1.4.2. Giai đoạn thực hiện kiểm thử và đánh giá

1.4.3. Giai đoạn sau kiểm thử và đánh giá

1.5. Một số công cụ hỗ trợ trong kiểm thử an toàn hệ thống thông tin

1.5.1. Kali Linux

1.5.2. Metasploit

1.5.3. BurpSuite

Tổng kết chương 1

Chương 2. Thu thập thông tin và xác định lỗ hổng (6 LT + 9 TH)

2.1. Thu thập thông tin

2.1.1. Thu thập thông tin trên các website

2.1.2. Thu thập thông tin dựa trên vị trí

2.1.3. Thu thập thông tin dựa trên việc làm

2.1.4. Thu thập thông tin thông qua email

2.1.5. Thu thập thông tin sử dụng công cụ

2.2. Khám phá mạng

2.3. Xác định cổng và dịch vụ

2.3.1. Quét đầy đủ

2.3.2. Quét một nửa

2.3.3. Quét XMAS

2.3.4. Quét FIN

2.3.5. Quét NULL

2.3.6. Quét IDLE

2.4. Xác định hệ điều hành

2.4.1. Xác định hệ điều hành theo kiểu chủ động

2.4.2. Xác định hệ điều hành theo kiểu bị động

2.5. Dò quét lỗ hổng bảo mật

2.5.1. Giới hạn của việc quét lỗ hổng

2.5.2. Quy trình quét lỗ hổng

2.5.3. Các phương pháp quét lỗ hổng

2.6. Một số phương pháp thu thập thông tin nâng cao

2.6.1. Tránh hệ thống phát hiện xâm nhập

2.6.2. Vượt tường lửa

Tổng kết chương 2

Chương 3. Kiểm thử hệ thống (6 LT + 6 TH)

3.1. Kiểm thử mật khẩu

3.2. Kiểm thử khả năng khai thác lỗ hổng

3.3. Kiểm thử leo thang đặc quyền

3.4. Kiểm thử duy trì truy cập

3.5. Kiểm thử chính sách hệ thống

Tổng kết chương 3

Chương 4. Kiểm thử máy chủ và ứng dụng Web (6 LT + 9 TH)

4.1. Giới thiệu quy trình kiểm thử OWASP

4.2. Một số lỗ hổng điển hình trong ứng dụng Web

4.3. Kiểm thử quản lý cấu hình

4.4. Kiểm thử quản lý định danh

4.5. Kiểm thử xác thực

4.6. Kiểm thử phân quyền

4.7. Kiểm thử quản lý phiên

4.8. Kiểm thử giá trị nhập

4.9. Kiểm thử vấn đề xử lý lỗi

4.10. Kiểm thử điểm yếu khi sử dụng mật mã

4.11. Kiểm thử Logic

4.12. Kiểm thử phía Client

Tổng kết chương 4

Chương 5. Kiểm thử mạng không dây (3 LT + 3 TH)

5.1. Chặn bắt gói tin không dây

5.2. Phân tích điểm truy cập không dây

5.3. Kiểm thử xác thực mạng không dây

5.4. Kiểm thử chức năng WPS

Tổng kết chương 5

Chương 6. Lập báo cáo (3 LT)

6.1. Tổng hợp thông tin

6.2. Đánh dấu các thông tin quan trọng

6.3. Thêm tài liệu hỗ trợ

6.4. Đảm bảo chất lượng báo cáo

Tổng kết chương 6

PHẦN III. PHÂN RÃ CHUẨN ĐẦU RA HỌC PHẦN

1. Các chuẩn đầu ra được đánh giá

TT	Ký hiệu	Chuẩn đầu ra	P1
1	CLO1	Trình bày được các khái niệm, phương pháp, quy trình thực hiện kiểm thử & đánh giá ATHTTT.	☑
2	CLO2	Trình bày được các phương pháp luận, các kỹ thuật thực hiện kiểm thử & đánh giá ATHTTT.	☑
3	CLO3	Vận dụng được các công cụ trong việc thực hiện kiểm thử & đánh giá ATHTTT	☑

PHẦN IV. MA TRẬN ĐỀ THI

6.5. Chương trình ĐH Chính quy An toàn thông tin (P1)

Tổng số câu hỏi: 60 câu. Thời gian làm bài: 60 phút.

Tài liệu được phép sử dụng: Không

Cấu trúc đề thi:

TT	Ký hiệu	Nhóm câu hỏi	SL	Điểm	NB	TH	VD	VDC
1	***1***	***TỔNG QUAN***	***6***		***6***			
2	1.1	Khái niệm cơ bản	2		2			
3	1.2	Phương pháp luận kiểm thử	2		2			
4	1.3	Quy trình kiểm thử	2		2			
5	2	***THU THẬP THÔNG TIN & XÁC ĐỊNH LỖ HỔNG***	***5***		***9***	***2***	***4***	
6	2.1	Kỹ thuật thu thập thông tin & xác định lỗ hổng	***4***		***4***			
7	2.2	Vận dụng công cụ thu thập thông tin & xác định lỗ hổng	***11***		***5***	***2***	***4***	
8	2.2.1	Thu thập thông tin & xác định lỗ hổng sử dụng nmap	7		1	2	4	
9	2.2.2	Thu thập thông tin & xác định lỗ hổng sử dụng Google	1		1			
10	2.2.3	Thu thập thông tin & xác định lỗ hổng sử dụng Shodan	1		1			
11	2.2.4	Thu thập thông tin & xác định lỗ hổng sử dụng các công cụ khác	2		2			
12	3	***KIỂM THỬ HỆ THỐNG***	***15***		***7***	***2***	***6***	
13	3.1	Kỹ thuật kiểm thử hệ thống	***3***		***3***			
14	3.1.1	Bẻ khóa mật khẩu	3		3			
15	3.2	Vận dụng công cụ kiểm thử hệ thống	***12***		***4***	***2***	***6***	
16	3.2.1	Vận dụng công cụ bẻ khóa mật khẩu	3		1		2	
17	3.2.2	Vận dụng công cụ kiểm thử truy cập & leo thang đặc quyền	6		2		4	
18	3.2.3	Vận dụng công cụ kiểm thử các tác vụ khác	3		1	2		
19	4	***KIỂM THỬ MÁY CHỦ & ỨNG DỤNG WEB***	***15***		***7***	***4***	***4***	
20	4.1	Kỹ thuật kiểm thử máy chủ & ứng dụng Web	***8***		***4***	***4***		

TT	Ký hiệu	Nhóm câu hỏi	SL	Điểm	NB	TH	VD	VDC
21	4.1.1	Kỹ thuật thu thập thông tin máy chủ & ứng dụng Web			1			
22	4.1.2	Kỹ thuật kiểm thử lỗ hổng máy chủ & ứng dụng Web						
23	4.1.2.1	Kỹ thuật kiểm thử lỗ hổng XSS			1			
24	4.1.2.2	Kỹ thuật kiểm thử lỗ hổng SQL injection			1	1		
25	4.1.2.3	Kỹ thuật kiểm thử 1 số lỗ hổng ứng dụng web khác			1	3		
26	4.2	Vận dụng công cụ kiểm thử máy chủ & ứng dụng Web	***7***		***3***		***4***	
27	4.2.1	*Kiểm thử máy chủ & ứng dụng Web sử dụng Burp Suite*			*1*			
28	4.2.2	*Kiểm thử máy chủ & ứng dụng Web sử dụng các công cụ khác*			*2*		*4*	
29	5	***KIỂM THỬ MẠNG KHÔNG DÂY***	***9***		***5***	***2***	***2***	
30	5.1	Kỹ thuật kiểm thử mạng không dây	***3***		***3***			
31	5.1.1	*Tổng quan*			*1*			
32	5.1.2	*Cơ chế hoạt động*			*1*			
33	5.1.3	*Tấn công trong mạng không dây*			*1*			
34	5.2	Vận dụng công cụ kiểm thử mạng không dây	***6***		***2***	***2***	***2***	
35	5.2.1	*Kiểm thử mạng không dây sử dụng aircrack-ng*			*1*	*2*	*2*	
36	5.2.2	*Kiểm thử mạng không dây sử dụng công cụ khác*			*1*			
37	**Tổng**		60		34	10	16	