

ĐỀ CƯƠNG CHI TIẾT HỌC PHẦN**1. Thông tin chung về học phần**

- **Tên học phần** : **Kiểm Thử (Penetration Testing)**
- **Mã số học phần** : 1250254
- **Số tín chỉ học phần:** 4 (3+1) tín chỉ
- Thuộc chương trình đào tạo của bậc, ngành: Bậc Đại học, ngành Công nghệ thông tin
- **Số tiết học phần:**
 - Nghe giảng lý thuyết : 45 tiết
 - Làm bài tập trên lớp : 0 tiết
 - Thảo luận : 0 tiết
 - Thực hành, thực tập (ở phòng thực hành, phòng Lab,...): 30 tiết
 - Hoạt động theo nhóm : 0 tiết
 - Thực tế: : 0 tiết
 - Tự học : 120 giờ
- **Đơn vị phụ trách học phần:** Bộ môn Bộ môn Mạng máy tính / Khoa Công nghệ thông tin

2. Học phần trước: An ninh mạng**3. Mục tiêu của học phần:**

- Sinh viên nắm vững được quy trình kiểm thử
- Sinh viên nắm vững kỹ thuật kiểm thử cho các loại hình.
- Sinh viên có khả năng đưa ra các ý kiến bổ sung cho bảo mật.

4. Chuẩn đầu ra:

	Nội dung	Đáp ứng CDR CTĐT
Kiến thức	4.1.1. Trang bị cho sinh viên những kiến thức cơ bản về kỹ thuật kiểm thử	K1
	4.1.2. Sinh viên có kỹ thuật kiểm thử trên các đối tượng kiểm thử	K2, K3
Kỹ năng	4.2.1. Sinh viên có khả năng phân tích tấn công	S2
	4.2.2. Sinh viên có kỹ năng tấn công kiểm thử	S1, S3
Thái độ	4.3.1. Đi học đúng giờ và đọc bài trước ở nhà.	A2
	4.3.2. Nhìn nhận đúng vai trò môn học cho công	A3

	việc tương lai. Tham gia tích cực trong nghiên cứu học tập kiến thức.	
--	---	--

5. Mô tả tóm tắt nội dung học phần:

Học phần này nhằm cung cấp cho các sinh viên các kiến thức liên quan đến Kỹ Thuật Penetration Testing:

- Các kiến thức cơ bản về Penetration testing.
- Quy trình kiểm thử
- Kiến thức kiểm thử trên hệ điều hành
- Kiến thức kiểm thử trên web, web server
- Kiến thức kiểm thử trên mạng nội bộ
- Kiến thức kiểm thử trên thiết bị di động
- Kiến thức kiểm thử trên mã nguồn ứng dụng
- Công cụ và môi trường kiểm thử.

6. Nội dung và lịch trình giảng dạy:

- Các học phần lý thuyết:

Buổi/ Tiết	Nội dung	Hoạt động của giảng viên	Hoạt động của sinh viên	Giáo trình chính	Tài liệu tham khảo	Ghi chú
1	Tổng quan về Penetration testing	<ul style="list-style-type: none">- Thuyết giảng- Cho bài tập	<ul style="list-style-type: none">- Nghe giảng, ghi chú- Trả lời câu hỏi- Làm bài tập	Chương 1 cuốn [1]	Chương 1 cuốn [2]	Giải quyết 4.1.1, 4.3
2	Môi trường thực hiện Penetration testing	<ul style="list-style-type: none">- Thuyết giảng- Hướng dẫn làm việc nhóm- Cho bài tập	<ul style="list-style-type: none">- Nghe giảng, ghi chú- Trả lời câu hỏi- Thảo luận nhóm theo chủ đề- Làm bài tập	Chương 2 cuốn [1]	Chương 2 cuốn [3]	Giải quyết 4.1.1, 4.3
3	Kỹ thuật kiểm thử trong LAN (các vấn đề lỗ hổng hệ điều hành)	<ul style="list-style-type: none">- Thuyết giảng- Hướng dẫn làm việc nhóm- Cho bài tập	<ul style="list-style-type: none">- Nghe giảng, ghi chú- Trả lời câu hỏi- Thảo luận nhóm theo chủ đề- Làm bài tập	Chương 5,6,8 cuốn [1]	Chương 4 cuốn [2] Chương 5,6 cuốn [3]	Giải quyết 4.1, 4.3
4	Kỹ thuật kiểm thử trong LAN (Password và chính sách chứng thực)	<ul style="list-style-type: none">- Thuyết giảng- Hướng dẫn làm việc nhóm- Cho bài tập	<ul style="list-style-type: none">- Nghe giảng, ghi chú- Trả lời câu hỏi- Thảo luận nhóm theo chủ đề- Làm bài tập	Chương 7,9 cuốn [1]	Chương 8 cuốn [3]	Giải quyết 4.1, 4.3
5	Social Engineering	<ul style="list-style-type: none">- Thuyết giảng- Hướng dẫn làm việc nhóm- Cho bài tập	<ul style="list-style-type: none">- Nghe giảng, ghi chú- Trả lời câu hỏi- Thảo luận nhóm theo chủ đề- Làm bài tập	Chương 11 cuốn [1]	Chương 5 cuốn [2] Chương 8 cuốn [4]	Giải quyết 4.1.2, 4.3
6	Bypassing chương trình chống virus	<ul style="list-style-type: none">- Thuyết giảng- Hướng dẫn làm việc	<ul style="list-style-type: none">- Nghe giảng, ghi chú- Trả lời câu hỏi	Chương 12 cuốn [1]		Giải quyết 4.1.2, 4.3

		nhóm - Cho bài tập	- Thảo luận nhóm theo chủ đề - Làm bài tập			
7	Kỹ thuật kiểm thử website	- Thuyết giảng - Hướng dẫn làm việc nhóm - Cho bài tập	- Nghe giảng, ghi chú - Trả lời câu hỏi - Thảo luận nhóm theo chủ đề - Làm bài tập	Chương 14 cuốn [1]	Chương 6 cuốn [2]	Giải quyết 4.1, 4.2, 4.3
8	Kỹ thuật kiểm thử website (tt)	- Thuyết giảng - Hướng dẫn làm việc nhóm - Cho bài tập	- Nghe giảng, ghi chú - Trả lời câu hỏi - Thảo luận nhóm theo chủ đề - Làm bài tập	Chương 14 cuốn [1]	Chương 6 cuốn [2]	Giải quyết 4.1, 4.3
9	Kỹ thuật kiểm thử webserver	- Thuyết giảng - Hướng dẫn làm việc nhóm - Cho bài tập	- Nghe giảng, ghi chú - Trả lời câu hỏi - Thảo luận nhóm theo chủ đề - Làm bài tập	Chương 14 cuốn [1]	Chương 6 cuốn [2]	Giải quyết 4.1.2, 4.2.1, 4.3
10	Kỹ thuật kiểm thử Wireless	- Thuyết giảng - Hướng dẫn làm việc nhóm - Cho bài tập	- Nghe giảng, ghi chú - Trả lời câu hỏi - Thảo luận nhóm theo chủ đề - Làm bài tập	Chương 15 cuốn [1]		Giải quyết 4.1.2, 4.2.1, 4.3
11	Kỹ thuật kiểm thử trên windows	- Thuyết giảng - Hướng dẫn làm việc nhóm - Cho bài tập	- Nghe giảng, ghi chú - Trả lời câu hỏi - Thảo luận nhóm theo chủ đề - Làm bài tập	Chương 17 cuốn [1]	Chương 2 cuốn [4] Chương 4 cuốn [3]	Giải quyết 4.1.2, 4.3
12	Kỹ thuật kiểm thử trên linux	- Thuyết giảng - Hướng dẫn làm việc nhóm	- Nghe giảng, ghi chú - Trả lời câu hỏi - Thảo luận nhóm theo	Chương 16 cuốn [1]	Chương 2 cuốn [4] Chương 4 cuốn [3]	Giải quyết 4.1, 4.2, 4.3

		- Cho bài tập	chủ đề - Làm bài tập			
13	Kỹ thuật kiểm thử trên mobile	- Thuyết giảng - Hướng dẫn làm việc nhóm - Cho bài tập	- Nghe giảng, ghi chú - Trả lời câu hỏi - Thảo luận nhóm theo chủ đề - Làm bài tập	Chương 20 cuốn [1]	Chương 9 cuốn [4]	Giải quyết 4.1, 4.2, 4.3
14	Report	- Thuyết giảng - Hướng dẫn làm việc nhóm - Cho bài tập	- Nghe giảng, ghi chú - Trả lời câu hỏi - Thảo luận nhóm theo chủ đề - Làm bài tập		Chương 8 cuốn [2]	Giải quyết 4.1, 4.2, 4.3
15	Ôn tập	- Thuyết giảng - Cho bài tập	- Nghe giảng, ghi chú - Trả lời câu hỏi			

- Các học phần thực hành:

Buổi/ Tiết	Nội dung	Hoạt động của giảng viên	Hoạt động của sinh viên	Giáo trình chính	Tài liệu tham khảo	Ghi chú
1	Cài đặt môi trường thực hiện Penetration testing	<ul style="list-style-type: none"> - Thuyết giảng - Hướng dẫn làm việc nhóm 	<ul style="list-style-type: none"> - Nghe giảng, ghi chú - Trả lời câu hỏi - Thảo luận nhóm theo chủ đề 	Chương 2 cuốn [1]	Chương 2 cuốn [3]	Giải quyết 4.1.1, 4.3
2	Kỹ thuật kiểm thử trong LAN	<ul style="list-style-type: none"> - Thuyết giảng - Hướng dẫn làm việc nhóm - Cho bài tập 	<ul style="list-style-type: none"> - Nghe giảng, ghi chú - Trả lời câu hỏi - Thảo luận nhóm theo chủ đề - Làm bài tập 	Chương 5,6,8 cuốn [1]	Chương 4 cuốn [2] Chương 5,6 cuốn [3]	Giải quyết 4.1, 4.3
3	Bypassing chương trình chống virus	<ul style="list-style-type: none"> - Thuyết giảng - Hướng dẫn làm việc nhóm - Cho bài tập 	<ul style="list-style-type: none"> - Nghe giảng, ghi chú - Trả lời câu hỏi - Thảo luận nhóm theo chủ đề - Làm bài tập 	Chương 12 cuốn [1]		Giải quyết 4.1.2, 4.3
4	Kỹ thuật kiểm thử website	<ul style="list-style-type: none"> - Thuyết giảng - Hướng dẫn làm việc nhóm - Cho bài tập 	<ul style="list-style-type: none"> - Nghe giảng, ghi chú - Trả lời câu hỏi - Thảo luận nhóm theo chủ đề - Làm bài tập 	Chương 14 cuốn [1]	Chương 6 cuốn [2]	Giải quyết 4.1, 4.2, 4.3
5	Kỹ thuật kiểm thử website (tt)	<ul style="list-style-type: none"> - Thuyết giảng - Hướng dẫn làm việc nhóm - Cho bài tập 	<ul style="list-style-type: none"> - Nghe giảng, ghi chú - Trả lời câu hỏi - Thảo luận nhóm theo chủ đề - Làm bài tập 	Chương 14 cuốn [1]	Chương 6 cuốn [2]	Giải quyết 4.1, 4.3
6	Kỹ thuật kiểm thử webserver	<ul style="list-style-type: none"> - Thuyết giảng - Hướng dẫn làm việc nhóm 	<ul style="list-style-type: none"> - Nghe giảng, ghi chú - Trả lời câu hỏi - Thảo luận nhóm theo 	Chương 14 cuốn [1]	Chương 6 cuốn [2]	Giải quyết 4.1.2, 4.2.1, 4.3

		- Cho bài tập	chủ đề - Làm bài tập			
7	Kỹ thuật kiểm thử Wireless	- Thuyết giảng - Hướng dẫn làm việc nhóm - Cho bài tập	- Nghe giảng, ghi chú - Trả lời câu hỏi - Thảo luận nhóm theo chủ đề - Làm bài tập	Chương 15 cuốn [1]		Giải quyết 4.1.2, 4.2.1, 4.3
8	Kỹ thuật kiểm thử trên windows	- Thuyết giảng - Hướng dẫn làm việc nhóm - Cho bài tập	- Nghe giảng, ghi chú - Trả lời câu hỏi - Thảo luận nhóm theo chủ đề - Làm bài tập	Chương 17 cuốn [1]	Chương 2 cuốn [4] Chương 4 cuốn [3]	Giải quyết 4.1.2, 4.3
9	Kỹ thuật kiểm thử trên linux	- Thuyết giảng - Hướng dẫn làm việc nhóm - Cho bài tập	- Nghe giảng, ghi chú - Trả lời câu hỏi - Thảo luận nhóm theo chủ đề - Làm bài tập	Chương 16 cuốn [1]	Chương 2 cuốn [4] Chương 4 cuốn [3]	Giải quyết 4.1, 4.2, 4.3
10	Kỹ thuật kiểm thử trên mobile	- Thuyết giảng - Hướng dẫn làm việc nhóm - Cho bài tập	- Nghe giảng, ghi chú - Trả lời câu hỏi - Thảo luận nhóm theo chủ đề - Làm bài tập	Chương 20 cuốn [1]	Chương 9 cuốn [4]	Giải quyết 4.1, 4.2, 4.3

7. Nhiệm vụ của sinh viên:

Sinh viên phải thực hiện các nhiệm vụ như sau:

- Tham dự tối thiểu 80% số tiết học lý thuyết.
- Tham gia đầy đủ 100% giờ thực hành và có báo cáo kết quả.
- Thực hiện đầy đủ các bài tập nhóm/ bài tập và được đánh giá kết quả thực hiện.
- Tham dự thi kết thúc học phần.
- Chủ động tổ chức thực hiện giờ tự học.

8. Đánh giá kết quả học tập của sinh viên:

8.1. Cách đánh giá

Sinh viên được đánh giá tích lũy học phần như sau:

TT	Điểm thành phần	Quy định	Trọng số	Mục tiêu	
1	Lý Thuyết	Điểm thi kết thúc học phần	- Thi vấn đáp - Tham dự đủ 80% tiết lý thuyết - Bắt buộc dự thi	50%	4.1, 4.2.1, 4.3
2		Tìm hiểu chuyên đề mới	- Làm theo nhóm. - Một nhóm tối đa hai sv		
3	Thực hành	Đồ án cuối khóa	- Những nhóm tìm hiểu tốt được chọn trình bày seminar. - Nhóm gồm tối đa 4 SV.	20%	4.1, 4.2, 4.3
4		Điểm thực hành	- Tham gia 100% số giờ - Nộp theo cột mốc quy định trong học kỳ	10%	

8.2. Cách tính điểm

- Điểm đánh giá thành phần và điểm thi kết thúc học phần được chấm theo thang điểm 10 (từ 0 đến 10), làm tròn đến 0.5.
- Điểm học phần là tổng điểm của tất cả các điểm đánh giá thành phần của học phần nhân với trọng số tương ứng. Điểm học phần theo thang điểm 10 làm tròn đến một chữ số thập phân.

9. Tài liệu học tập:

9.1. Giáo trình chính:

[1]. Hacking Exposed 7: Network Security Secrets and Solutions, Stuart McClure, Joel Scambray, George Kurtz, McGraw-Hill Education, 2012.

9.2. Tài liệu tham khảo:

[2]. Web Hacking: Attacks and Defense, Stuart McClure, Saamil Shah, Shreeraj Shah, Addison-Wesley Professional, 2003

[3] Coding for Penetration Testers, 2nd Edition, Jason Andress, Ryan Linn, Syngress, 2017

10. Hướng dẫn sinh viên tự học:

Tuần/ Buổi	Nội dung	Lý thuyết (tiết)	Thực hành (tiết)	Nhiệm vụ của sinh viên
1	Tổng quan về Penetration testing	3	0	Tìm hiểu trước chương 1 trong [1]
2	Môi trường thực hiện Penetration testing	3	3	Tìm hiểu trước chương 2 trong [1]
3	Kỹ thuật kiểm thử trong LAN (các vấn đề lỗ hổng hệ điều hành)	3	3	Tìm hiểu trước chương 5,6,8 trong [1]
4	Kỹ thuật kiểm thử trong LAN (Password và chính sách chứng thực)	3	0	Tìm hiểu trước chương 7,9 trong [1]
5	Social Engineering	3	0	Tìm hiểu trước chương 11 trong [1]
6	Bypassing chương trình chống virus	3	3	Tìm hiểu trước chương 12 trong [1]
7	Kỹ thuật kiểm thử website	3	3	Tìm hiểu trước chương 8 trong [1]
8	Kỹ thuật kiểm thử website (tt)	3	3	Tìm hiểu trước chương 14 trong [1]
9	Kỹ thuật kiểm thử webservers	3	3	Tìm hiểu trước chương 14 trong [1]
10	Kỹ thuật kiểm thử Wireless	3	3	Tìm hiểu trước chương 15 trong [2]
11	Kỹ thuật kiểm thử trên windows	3	3	Tìm hiểu trước chương 17 trong [1]
12	Kỹ thuật kiểm thử trên linux	3	3	Tìm hiểu trước chương 16 trong [1]
13	Kỹ thuật kiểm thử trên mobile	3	3	Tìm hiểu trước chương 20 trong [1]

14	Report	3	0	Tìm hiểu trước chương 8 trong [2] Tìm hiểu trước chương 16 trong [3]
15	Ôn tập	3	0	

Ngày... tháng.... Năm 2017
Trưởng khoa
(Ký và ghi rõ họ tên)

Ngày... tháng.... Năm 2017
Trưởng Bộ môn
(Ký và ghi rõ họ tên)

Ngày... tháng.... Năm 2017
Người biên soạn
(Ký và ghi rõ họ tên)

Phạm Đình Thắng

Phạm Đình Thắng

Ngày... tháng.... Năm 2017
Ban giám hiệu