KHAI THÁC LỖ HỔNG PHẦN MỀM

I. THÔNG TIN CHUNG

Tên học phần	**Khai thác lỗ hổng phần mềm**
Tên tiếng Anh	Exploit Software Vulnerabilities
Số tín chỉ	2
Số giờ học ở lớp	45 (15 LT, 30 TH)
Số giờ tự học ở nhà	60
Học phần học trước	Kiến trúc máy tính và hợp ngữ

II. MỤC TIÊU HỌC PHẦN

2.1. Mục tiêu chung

Học phần này cung cấp cho sinh viên kiến thức và kỹ năng để khai thác một số lỗ hổng phần mềm thường gặp.

2.2. Mục tiêu cụ thể

Mục tiêu	Mô tả	Chuẩn đầu ra CTĐT
M1	Nắm được cơ chế thực thi chương trình trong máy tính	R11B
M2	Có khả năng tạo shellcode để thực thi tác vụ mong muốn	R11B, R12B, R17A, R17B, R18B
M3	Hiểu được cơ chế xuất hiện các lỗ hổng phần mềm thường gặp	R10A, R11B, R11C, R12C, R18B
M4	Có khả năng phân tích phần mềm để xác định lỗ hổng và viết mã khai thác để khai thác lỗ hổng tương ứng	R12A, R11B, R12C, R17A, R17B, R18B, R18C

III. MÔ TẢ HỌC PHẦN

Phần đầu trình bày một số kiến thức cơ sở cho việc khai thác lỗ hổng phần mềm như kiến trúc bộ nhớ và kỹ thuật gọi hàm, các công cụ thường dùng. Phần thứ hai trình bày về shellcode. Các phần tiếp theo lần lượt trình bày về kỹ thuật khai thác lỗi buffer overflow, lỗi format string và lỗi race condition.

IV. ĐỀ CƯƠNG CHI TIẾT

Chương 1. Một số kiến thức nền tảng (3 LT + 3 TH)

1.1. Kiến trúc của bộ vi xử lý trung tâm

1.2. Bộ nhớ và địa chỉ tuyến tính

1.3. Mã máy và hợp ngữ

1.4. Stack và Heap

1.5. Cấu trúc của một hàm và các quy ước gọi hàm

1.6. Công cụ thường dùng

Chương 2. Shellcode (3 LT + 3 TH)

2.1. Khái niệm shellcode

2.2. Định địa chỉ trong shellcode

2.3. Xử lý các byte null trong shellcode

2.4. Tạo shellcode

2.4.1. Thực thi lời gọi hệ thống

2.4.2. Local Shellcode

2.4.3. Remote Shellcode

Chương 3. Khai thác lỗ hổng tràn bộ đệm (3 LT + 6 TH)

3.1. Lỗi tràn bộ đệm

3.2. Kỹ thuật khai thác lỗi tràn bộ đệm trên stack

3.2.1. Thay đổi giá trị biến cục bộ

3.2.2. Truyền dữ liệu vào chương trình

3.2.3. Ghi đè địa chỉ trả về

3.2.4. Quay về thư viện chuẩn

3.3. Lỗi tràn bộ đệm trên heap

Chương 4. Khai thác lỗ hổng tràn bộ đệm nâng cao (3 LT + 6 TH)

4.1. Thực thi shellcode bằng các lệnh nhảy

4.2. Thực thi shellcode với Egghunting

4.3. Khai thác qua SEH

4.4. Vượt qua cơ chế chống khai thác lỗi tràn bộ đệm

4.4.1. Cơ chế chống khai thác lỗi tràn bộ đệm

4.4.2. Vượt qua cơ chế Buffer Security Check

4.4.3. Vượt qua cơ chế DEP

4.4.4. Vượt qua cơ chế ASLR

Chương 5. Khai thác các lỗ hổng khác (3 LT + 6 TH)

5.1. Lỗi tràn 1 byte

5.2. Lỗi chuỗi định dạng

5.3. Lỗi tràn số nguyên

5.4. Lỗi race condition

V. KẾ HOẠCH GIẢNG DẠY

Giải thích ký hiệu: LT – lý thuyết; BT – bài tập/thảo luận; TH – Thực hành; ON – tự học ở nhà

TT	Nội dung và phương pháp dạy học	Mục tiêu	LT	BT	TH	ON
1	***Chương 1. Một số kiến thức nền tảng*** **Giảng dạy trên lớp** – Kiến trúc của bộ vi xử lý trung tâm – Bộ nhớ và địa chỉ tuyến tính – Mã máy và hợp ngữ – Stack và Heap – Cấu trúc của một hàm và các quy ước gọi hàm – Công cụ thường dùng **Phương pháp giảng dạy chính** – Trình chiếu Powerpoint – Thuyết giảng	M1, M2	3	0	0	6

TT	Nội dung và phương pháp dạy học	Mục tiêu	LT	BT	TH	ON
	– Minh họa bằng những đoạn mã cụ thể **Tài liệu tham khảo** [1: Chương 2] [7] **Tự học ở nhà** – Nghiên cứu tài liệu tham khảo – Ôn tập lại kiến thức, kỹ năng lập trình hợp ngữ – Tải về và tập sử dụng các công cụ được giới thiệu					
2	***Thực hành chương 1*** **Giảng dạy trên lớp** – Thực hành sử dụng các công cụ thường dùng trong quá trình khai thác lỗ hổng phần mềm **Phương pháp giảng dạy chính** – Làm mẫu – Cho sinh viên thực hành theo tài liệu hướng dẫn – Giao tiếp, hỏi đáp với sinh viên **Tự học ở nhà** – Củng cố kiến thức lý thuyết – Củng cố kỹ năng sử dụng các công cụ	M1, M2	0	0	3	6
3	***Chương 2. Shellcode*** **Giảng dạy trên lớp** – Khái niệm shellcode – Định địa chỉ trong shellcode – Xử lý các byte null trong shellcode – Tạo shellcode **Phương pháp giảng dạy chính** – Trình chiếu Powerpoint – Thuyết giảng – Minh họa quá trình tạo một shellcode **Tài liệu tham khảo** [2: Chapter 2] [3: Chapter 3] [4: Chapter 5] **Tự học ở nhà** – Nghiên cứu tài liệu tham khảo – Thực hành sử dụng các công cụ để tạo shellcode	M2	3	0	0	6
4	***Thực hành chương 2*** **Giảng dạy trên lớp**	M2	0	0	3	6

TT	Nội dung và phương pháp dạy học	Mục tiêu	LT	BT	TH	ON
	– Thực hành tạo shellcode **Phương pháp giảng dạy chính** – Làm mẫu – Cho sinh viên thực hành theo tài liệu hướng dẫn – Giao tiếp, hỏi đáp với sinh viên **Tự học ở nhà** – Củng cố kiến thức lý thuyết – Củng cố kỹ năng tạo shellcode					
5	***Chương 3. Khai thác lỗ hổng tràn bộ đệm*** **Giảng dạy trên lớp** – Lỗi tràn bộ đệm – Kỹ thuật khai thác lỗi tràn bộ đệm trên stack – Lỗi tràn bộ đệm trên heap **Phương pháp giảng dạy chính** – Trình chiếu Powerpoint – Thuyết giảng – Minh họa quá trình khai thác lỗ hổng **Tài liệu tham khảo** [1: Chương 3] [2: Chapters 3, 4] [3: Chapters 2, 5] **Tự học ở nhà** – Nghiên cứu tài liệu tham khảo – Thực hành các ví dụ trong [7] – Đọc thêm [8]	M3, M4	3	0	0	6
6	***Thực hành chương 3*** **Giảng dạy trên lớp** – Thực hành các kỹ thuật khai thác lỗi tràn bộ đệm **Phương pháp giảng dạy chính** – Làm mẫu – Cho sinh viên thực hành theo tài liệu hướng dẫn – Giao tiếp, hỏi đáp với sinh viên **Tự học ở nhà** – Củng cố kiến thức lý thuyết – Làm thêm các bài tập để củng cố kỹ năng khai thác	M3, M4	0	0	6	6
7	***Thi giữa kỳ*** Hình thức thi: Thực hành		0	0	6	0
8	***Chương 4. Khai thác lỗ hổng tràn bộ đệm nâng cao***	M3, M4	3	0	0	6

TT	Nội dung và phương pháp dạy học	Mục tiêu	LT	BT	TH	ON
	Giảng dạy trên lớp – Thực thi shellcode bằng các lệnh nhảy – Thực thi shellcode với Egghunting – Khai thác qua SEH – Vượt qua cơ chế chống khai thác lỗi tràn bộ đệm **Phương pháp giảng dạy chính** – Trình chiếu Powerpoint – Thuyết giảng – Minh họa quá trình khai thác lỗ hổng **Tài liệu tham khảo** [7], [8] **Tự học ở nhà** – Nghiên cứu tài liệu tham khảo – Thực hành các ví dụ trong [7] và [8] – Tìm kiếm và nghiên cứu các bài viết về kỹ thuật vượt qua cơ chế phòng chống tấn công tràn bộ đệm					
9	***Thực hành chương 4*** **Giảng dạy trên lớp** – Thực hành các kỹ thuật khai thác lỗi tràn bộ đệm nâng cao **Phương pháp giảng dạy chính** – Làm mẫu – Cho sinh viên thực hành theo tài liệu hướng dẫn – Giao tiếp, hỏi đáp với sinh viên **Tự học ở nhà** – Củng cố kiến thức lý thuyết – Làm thêm các bài tập để củng cố kỹ năng khai thác	M3, M4	0	0	6	6
10	***Chương 5. Khai thác các lỗ hổng khác*** **Giảng dạy trên lớp** – Lỗi tràn 1 byte – Lỗi chuỗi định dạng – Lỗi tràn số nguyên – Lỗi race condition **Phương pháp giảng dạy chính** – Trình chiếu Powerpoint – Thuyết giảng – Minh họa quá trình khai thác lỗ hổng **Tài liệu tham khảo** [1: Chương 4, 5] [2: Chapters 3, 5]	M3, M4	3	0	0	6

TT	Nội dung và phương pháp dạy học	Mục tiêu	LT	BT	TH	ON
	Tự học ở nhà – Nghiên cứu tài liệu tham khảo – Thực hành các ví dụ trong [7] và [8]					
11	***Thực hành chương 5*** **Giảng dạy trên lớp** – Thực hành khai thác các lỗi phần mềm: Off By One, Format String, Integer Overflow, Race Condition **Phương pháp giảng dạy chính** – Làm mẫu – Cho sinh viên thực hành theo tài liệu hướng dẫn – Giao tiếp, hỏi đáp với sinh viên **Tự học ở nhà** – Củng cố kiến thức lý thuyết – Làm thêm các bài tập để củng cố kỹ năng khai thác	M3, M4	0	0	6	6
	Tổng		**15**	**0**	**30**	**60**

VI. GIÁO TRÌNH VÀ TÀI LIỆU THAM KHẢO

6.1. Tài liệu tham khảo chính

[1] Nguyễn Thành Nam, Nghệ thuật tận dụng lỗi phần mềm, NXB Khoa học & Kỹ thuật, 2009

[2] James C. Foster, Vincent Liu, Writing Security Tools and Exploits, Syngress, 2006

[3] Jack Koziol et al., The Shellcoder's Handbook: Discovering and Exploiting Security Holes, Wiley and Sons, 2004

6.2. Tài liệu tham khảo bổ sung

[4] Jon Erickson, Hacking: The Art of Exploitation, No Starch, 2008

[5] James C. Foster et al., Buffer Overflow Attacks: Detect, Exploit, Prevent, Syngress, 2005

[6] James C. Foster, Socket, Shellcode, Porting and Coding, Syngress, 2005

[7] Massimiliano Tomassoli, No-merci, Modern Windows Exploit Development, Online: http://docs.alexomar.com/biblioteca/Modern%20Windows%20Exploit%20Development.pdf

[8] Mike Czumak, Series of posts on Windows Exploit Development, Online: https://www.securitysift.com/windows-exploit-development-part-1-basics/

VII. TRANG THIẾT BỊ DẠY HỌC

7.1. Giảng đường cho các buổi học lý thuyết

- Máy chiếu
- Bảng viết

7.2. Phòng máy cho các buổi học thực hành

- Máy chiếu
- Máy tính chạy hệ điều hành Windows
- Máy ảo: Kali Linux, Windows

– Công cụ: IDA Pro with Hex-Rays, Immunity Debugger

VIII. ĐÁNH GIÁ KẾT QUẢ HỌC TẬP

8.1. Chấm điểm

Điểm đánh giá	Căn cứ đánh giá	Công thức tính
Điểm chuyên cần	Đi học đầy đủ, tham gia xây dựng bài; Kết quả các bài thực hành	(1)
Điểm thi giữa kỳ	Bài thi giữa kỳ	(2)
Điểm quá trình	(1), (2)	(3) = 0,3×(1) + 0,7×(2)
Điểm thi kết thúc học phần	Bài thi kết thúc học phần	(4)
Điểm học phần	(3), (4)	(5) = 0,3×(3) + 0,7×(4)

8.2. Điều kiện để được thi kết thúc học phần

– Dự lớp tối thiểu 75% số giờ học

– Điểm quá trình đạt tối thiểu 4,0 (thang điểm 10)

8.3. Hình thức thi kết thúc học phần

Thực hành (có thể kết hợp vấn đáp)

IX. THÔNG TIN VỀ GIẢNG VIÊN

TT	Giảng viên	Điện thoại	Email
1	TS. Nguyễn Tuấn Anh	0977199902	tuananh1982act@gmail.com
2			