Môn học Thực tập cơ sở

Bài 11: Tìm kiếm và khai thác lỗ hổng

1. Mục đích

- Hiểu được các mối đe dọa và lỗ hổng.
- Hiểu được cách thức hoạt động của một số công cụ rà quét và tìm kiếm đe dọa và lỗ lổng như: nmap/zenmap, nessus, Metasploit framework.
- Biết cách sử dụng công cụ để tìm kiếm và khai thác các mối đe dọa, lỗ hổng bao gồm: nmap/zenmap, nessus, Metasploit framework.

2. Nội dung thực hành

2.1. Tìm hiểu lý thuyết

Sinh viên đọc trước các nội dung liên quan đến các nội dung thực hành tại một số tài liệu như.

- Chương 2, Giáo trình Cơ sở an toàn thông tin, Học viện Công Nghệ Bưu Chính Viễn Thông, 2020 của tác giả Hoàng Xuân Dậu.
- Tài liệu CEH, https://www.eccouncil.org/programs/certified-ethical-hacker-ceh/
- Lab 14 của CSSIA CompTIA Security+® Supported Labs

2.2. Chuẩn bị môi trường

- Phần mềm VMWare Workstation hoặc Virtual Box hoặc các phần mềm ảo hóa khác.
- Các công cụ nmap/zenmap, nessus, Metasploit framework

2.3. Các bước thực hiện

2.3.1. Chuẩn bị môi trường

- Cài đặt công cụ ảo hóa.
- Cài đặt các công cụ: nmap/zenmap, nessus, Metasploit framework.

2.3.2. Nội dung thử nghiệm

Lựa chọn máy nạn nhân là máy chứa các lỗ hổng bảo mật của các hệ điều hành windows. Máy của người tấn công là máy tính cài đặt các công cụ nmap/zenmap; nmap/zenmap; Metasploit framework.

- Sử dụng nmap/zenmap để quét các cổng dịch vụ (ít nhất 2 cổng).
- Sử dụng nessus để quét các lỗ hổng (ít nhất 2 lỗ hổng).
- Sử dụng Metasploit framework khai thác lỗ hổng (ít nhất khai thác thành công 1 lỗ hổng trên máy nạn nhân).

3. Kết quả cần đạt được

3.1. Yêu cầu về hình thức trình bày

- Bài nộp ở dạng file pdf, tên file ví dụ như:

Bài thực hành 11_Họ tên_Mã sinh viên.pdf

- Trang bìa (ghi rõ môn học, bài thực hành, mã sv và họ và tên)

3.2. Yêu cầu đối với nội dung

3.2.1. Đối với nội dung lý thuyết

- Mô tả ngắn gọn lý thuyết về các công cụ nmap/zenmap; nessus; Metasploit framework.
- Mô tả ngắn gọn lý thuyết về một số lỗ hổng, một số cổng dịch vụ quét được.
- Mô tả ngắn gọn lý thuyết về lỗ hổng mà Metasploit framework khai thác được.

3.2.2. Đối với nội dung thực hành

- Mô tả quá trình cài đặt các công cụ kèm theo ảnh minh chứng.
- Mô tả quá trình thực nghiệm và ảnh chụp kết quả minh chứng của quá trình rà quét cổng dịch vụ, rà quét lỗ hổng bảo mật, thực hiện tấn công và khai thác lỗ hổng bảo mật...

- Lưu ý: Sinh viên cần chứng minh các kết quả thực nghiệm là do chính mình tiến hành cài đặt và thực hiện trong báo cáo. Minh chứng có thể thực hiện theo các cách sau:
    - Đặt tên máy/tên người dùng là họ tên SV và Mã SV.
    - Mở cmd gõ “date” để hiển thị ngày tháng năm; gõ “echo” + “họ tên và Mã SV” để hiển thị thông tin của SV. Chụp ảnh phần này với nội dung đang thực hiện hoặc kết quả của bài.