An toàn mạng (INT1482) - Bài thực hành số 2

1. Mục đích:

- Tìm hiểu về các kỹ thuật rà quét cổng, mạng, lỗ hổng và khai thác
- Luyện thực hành các kỹ thuật rà quét cổng, mạng, lỗ hổng và khai thác sử dụng một số công cụ sẵn có

2. Các phần mềm, công cụ cần có

- Kali Linux và các công cụ rà quét cổng, mạng, lỗ hổng và khai thác có sẵn trong Kali Linux:
  - nmap, nmap scripts
  - metasploit
- Metasploitable2: máy ảo VMWare chứa lỗi, có thể tải tại: http://sourceforge.net/projects/metasploitable/files/Metasploitable2/

2. Tìm hiểu về các kỹ thuật rà quét cổng, mạng, lỗ hổng và khai thác

- Rà quét để tìm các host hoạt động
- Rà quét để tìm các cổng mở trên host
- Rà quét để tìm thông tin các dịch vụ đang chạy và hệ điều hành của host
- Rà quét để tìm các lỗ hổng trên 1 host hoặc 1 dịch vụ đang hoạt động
- Khai thác lỗ hổng tìm được.

3. Nội dung thực hành

3.1 Cài đặt các công cụ, nền tảng

- Cài đặt Kali Linux 2023 (nếu chưa cài đặt) trên 1 máy ảo (hoặc máy thực)
  - Bản ISO của Kali Linux có thể tải tại: https://www.kali.org/get-kali/#kali-bare-metal
  - Bản cài sẵn trên máy ảo của Kali Linux có thể tải tại: https://www.kali.org/get-kali/#kali-virtual-machines
  - Đổi tên máy Kali Linux thành dạng Mã SV-Tên-Kali. Ví dụ: Bạn Trần Đức Cường, mã sv B20DCAT018 → tên máy là B20AT018-Cuong-Kali.
  - Kiểm tra và chạy thử bộ công cụ khai thác MetaSploit trên Kali Linux
  - Mở terminal, chạy lệnh "ifconfig" để kiểm tra địa chỉ IP của máy Kali
  - Mở terminal, chạy lệnh "uname -a" để kiểm tra tên máy và phiên bản HĐH.
- Tải và cài đặt Metasploitable2 làm máy victim (nếu chưa có):
  - Tải Metasploitable2
  - Giải nén
  - Sử dụng VMWare Player hoặc VMWare để mở và khởi động máy ảo. Tài khoản đăng nhập vào hệ thống là msfadmin / msfadmin.
  - Đặt lại tên máy victim là Mã SV+Họ và tên. Ví dụ: Bạn Trần Đức Cường, mã sv B18DCAT018 → tên máy là B18AT018-Cuong-Meta. Khởi động lại máy victim để máy nhận tên mới.
  - Mở terminal, chạy lệnh "ifconfig" để kiểm tra địa chỉ IP của máy Meta
  - Mở terminal, chạy lệnh "uname -a" để kiểm tra tên máy và phiên bản HĐH.

3.2 Kiểm tra và cài đặt các NSE scripts cho nmap

- Kiểm tra các NSE scripts có sẵn cho nmap:

  cd /usr/share/nmap/scripts

  ls (chụp ảnh màn hình đầu tiên hiển thị các NSE scripts có sẵn lưu file kết quả)

- Cài đặt CSDL nmap-vulners (nếu chưa có):

  sudo git clone https://github.com/vulnersCom/nmap-vulners.git (chụp ảnh màn hình báo cài đặt thành công lưu file kết quả)

  ls nmap-vulners (chụp ảnh màn hình hiển thị các NSE scripts đã cài lưu file kết quả)

- Cài đặt CSDL vulscan (nếu chưa có):

  sudo git clone https://github.com/scipag/vulscan.git (chụp ảnh màn hình báo cài đặt thành công lưu file kết quả)

  ls vulscan (chụp ảnh màn hình hiển thị các NSE scripts đã cài lưu file kết quả)

3.3 Rà quét để tìm thông tin về host, cổng, dịch vụ và HĐH sử dụng nmap

- Tìm các host đang hoạt động (thực hiện với 3 dải địa chỉ IP hoạt động có tối thiểu 5 hosts)
  #nmap -sn 203.162.10.114-120
- Tìm các cổng đang hoạt động trên 1 host (thực hiện với máy Meta và 2 IP hoạt động)
  #nmap -sS <địa chỉ IP>
- Tìm thông tin các dịch vụ đang chạy và hệ điều hành của host (thực hiện với máy Meta và 2 địa chỉ IP hoạt động)
  #nmap -sV -A -p80 <địa chỉ IP>

3.4 Rà quét để tìm các lỗ hổng trên 1 host hoặc 1 dịch vụ đang hoạt động

- Tìm lỗ hổng trên các dịch vụ của máy Meta với script ngầm định:
  #nmap -sC <địa chỉ IP máy Meta>
- Tìm lỗ hổng trên các dịch vụ FTP của máy Meta với vulscan script:
  #nmap --scripts=vulscan/vulscan.nse -sV -p21 <địa chỉ IP máy Meta>
- Tìm lỗ hổng trên các dịch vụ HTTP của máy Meta với vulscan script:
  #nmap --scripts=vulscan/vulscan.nse -sV -p80 <địa chỉ IP máy Meta>
- Tìm lỗ hổng trên các dịch vụ FTP của máy Meta với vulscan script và chỉ với cơ sở dữ liệu cve.csv:
  #nmap --scripts=vulscan/vulscan.nse --script-args vulscandb=cve.csv -sV -p21 <địa chỉ IP máy Meta>
- Tìm lỗ hổng trên các dịch vụ HTTP của máy Meta với vulscan script và chỉ với cơ sở dữ liệu cve.csv:
  #nmap --scripts=vulscan/vulscan.nse --script-args vulscandb=cve.csv -sV -p80 <địa chỉ IP máy Meta>

3.5 Khai thác lỗ hổng

Lựa chọn 1 lỗ hổng (có mã CVE/ID của lỗ hổng) tìm được ở mục 3.4, tiến hành khai thác sử dụng MetaSploit.

4. Yêu cầu cần đạt

1. Máy Kali, Meta phải được đặt tên theo đúng qui định ở mục 3.1
2. Chụp ảnh màn hình kết quả lưu vào file (hoặc giữ nguyên cửa sổ màn hình thực hiện):
    a. Tất cả các màn hình chạy các lệnh (có thể gộp nhiều lệnh vào 1 màn hình)
    b. Có hiển thị ngày giờ thực hiện trong **từng** ảnh chụp màn hình
    c. Màn hình chụp phải gồm đầy đủ tên máy, tên người dùng (như sau)
    d. Với các kết quả dài có thể chụp nhiều trang màn hình và ghép lại.