1. Mục đích:•Giúp sinh viên nắm được quy trình và thực hiện một tấn công khai thác lỗ  
hổng đã biết bằng cách sử dụng công cụ Metasploit.  
2. Yêu cầu đối với sinh viên:•Có kiến thức cơ bản về hệ điều hành Linux, Kali, công cụ metasploit, các lỗ  
hổng dịch vụ cơ bản: rlogin, ingreslock, distccd, IRC daemon, VSFtpd,  
Samba, HTTP, Postgres.  
3. Nội dung thực hành-Kiểm tra địa chỉ ip của máy victim  
- Kiểm tra địa chỉ ip của máy tấn công  
- Sử dụng câu lệnh “ping” để kiểm tra kết nối từ máy attacker đến máy  
Victim. Kết quả cần đạt được “ping” thực hiện thành công, có phản hồi từ  
máy Victim  
- Sử dụng công cụ “nmap” để quét các dịch vụ có thể tấn công. Kết quả cần  
đạt được tìm ra các cổng có thể tấn công vào máy Victim- Khai thác dịch vụ cấu hình rlogin (cổng 513): để truy nhập từ xa đến máy  
của Victim (với đặc quyền root). Kết quả cần đạt được truy cập thành công  
đến máy Victim với quyền root và mở được file trên máy Victim.  
+ cat /root/filetoview.txt- Khai thác dịch vụ ingreslock (cổng 1524). Sử dụng telnet để truy cập vào  
dịch vụ ingreslock và có được quyền root. Kết quả cần đạt được truy cập  
thành công đến máy Victim với quyền root và mở được file trên máy  
Victim.  
- Khai thác dịch vụ distccd (cổng 3632): Khởi chạy trình điều khiển  
Metasploit là “msfconsole”. Tìm và tấn công dịch vụ distccd.  
- sử dụng công cụ khai thác “exploit”  
- xem cấu hình liên quan đến “exploit”  
- Đặt RHOST và thực hiện tấn công  
- Khai thác lỗ hổng IRC daemon (cổng 6667) Khởi chạy trình điều khiển  
Metasploit là “msfconsole”. Tìm và tấn công lỗ hổng unreal\_ircd.  
- sử dụng công cụ khai thác “exploit” use  
exploit/unix/irc/unreal\_ircd\_3281\_backdoor  
- SetRHOST và tiến hành tấn công 🡪tấn công thành công  
- Khai thác dịch vụ VSFtpd (cổng 21). Khởi chạy trình điều khiển  
Metasploit là “msfconsole”. Tìm và tấn công lỗ hổng vsftpd\_234  
- sử dụng công cụ khai thác “exploit” use  
exploit/unix/ftp/vsftpd\_234\_backdoor  
- SETRHOST và thực hiện tấn công 🡪Tấn công thành công  
- Khai thác dịch vụ Samba service (cổng 139): Khởi chạy trình điều khiển  
Metasploit là “msfconsole”. Tìm và tấn công lỗ hổng samba usermap\_script.  
- sử dụng công cụ khai thác “exploit” use exploit/multi/samba/usermap\_script  
- SETRHOST và thực hiện tấn công 🡪Tấn công thành công  
- Khai thác dịch vụ HTTP (cổng 80): Khởi chạy trình điều khiển Metasploit  
là “msfconsole”. Tìm và tấn công lỗ hổng php\_cgi.  
- sử dụng công cụ khai thác “exploit” use  
exploit/multi/http/php\_cgi\_arg\_injection  
- SETRHOST và thực hiện tấn công 🡪Tấn công thành công  
- Khai thác dịch vụ Postgres (cổng 5432). Khởi chạy trình điều khiển  
Metasploit là “msfconsole”. Tìm và tấn công lỗ hổng postgres\_payload:  
search postgres\_payload- sử dụng công cụ khai thác “exploit” use  
exploit/linux/postgres/postgres\_payload