Metasploit dùng để kiểm thử xâm nhập, kiểm thử bảo mật

Multi/handler: chạy các payload bên ngoài Metasploit và sẵn sàng nhận kết nối

MSFvenom dùng để tạo các payload lưu trên máy tấn công; tải payload đó từ máy tấn công về máy nạn nhân để thực hiện 1 phiên kết nối

Tạo 1 MSI payload trong 1 file ISO; MSI file sẽ thỉnh thoảng đc cho phép chạy kể cả khi bị disable. Tải file iso về máy nạn nhân

Chạy sliver-server để tạo 1 file mã độc DLL (php, đa dạng

# Mục tiêu:

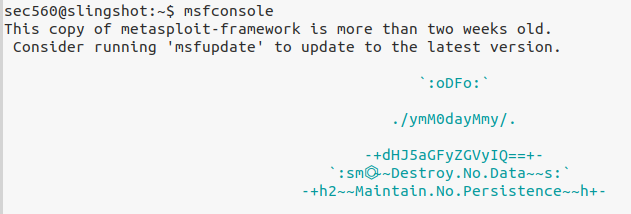
Hiểu và nắm rõ các tùy chọn payload có sẵn trong Metasploit và công cụ MSFVenom.

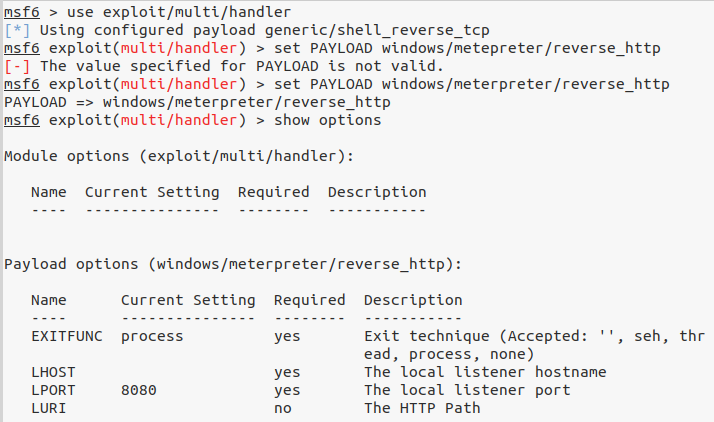
Cấu hình handler (bộ xử lý) trong metasploit để nhận nhiều kết nối từ các payload khác nhau.

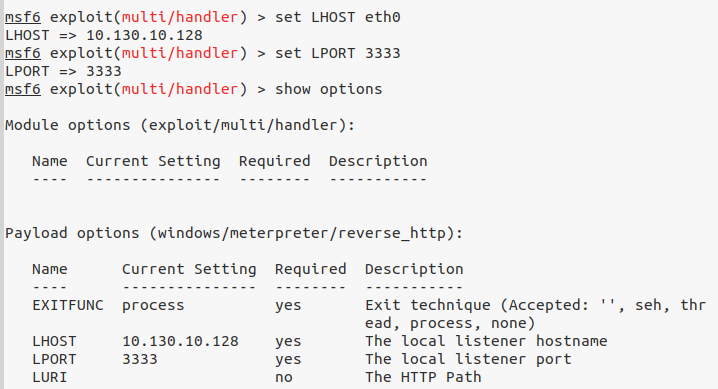
Tạo payload khác nhau bằng cách sử dụng Metasploit hay công cụ msfvenom.

Sử dụng sliver để tạo ra payload và thực thi trên các kết nối từ xa.

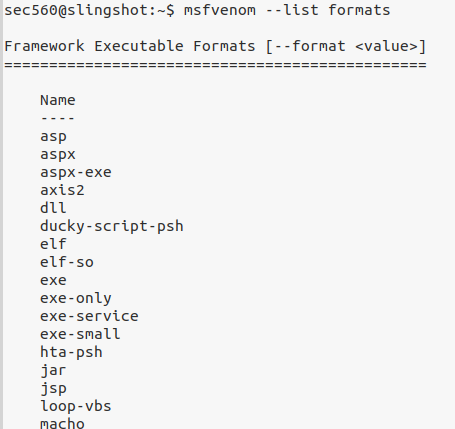
# 1. Setup Metasploit to receive a connection

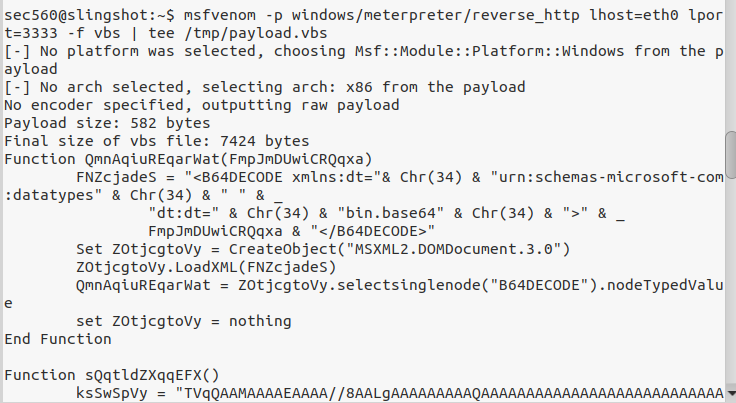






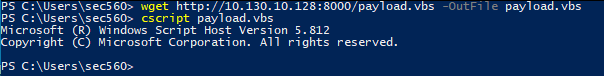
# 2. Metasploit PAYLOADs with MSFVenom

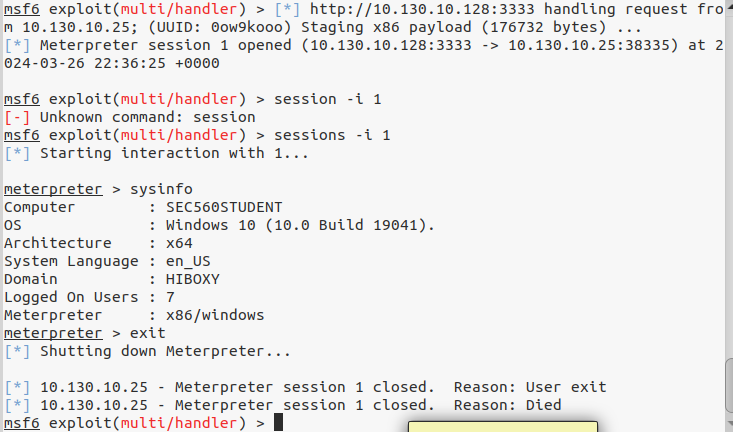




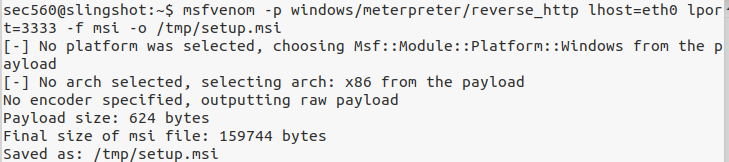
# 3. Copying the VBS payload to Windows and execute it

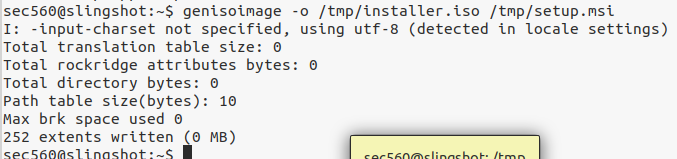




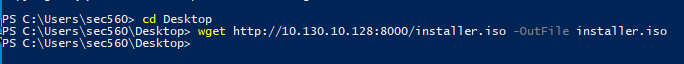


# 4. Creating an MSI payload in an ISO file

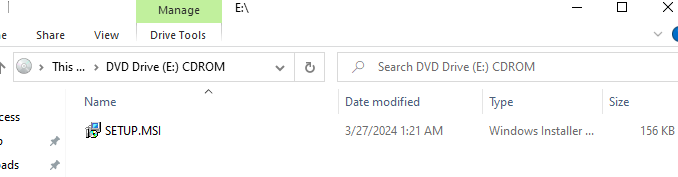


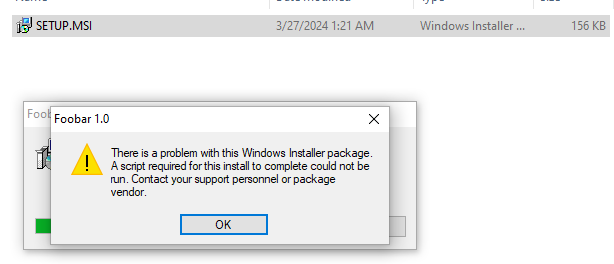


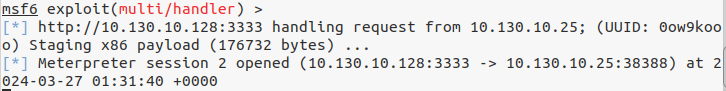
# 5. Download and open ISO and MSI files

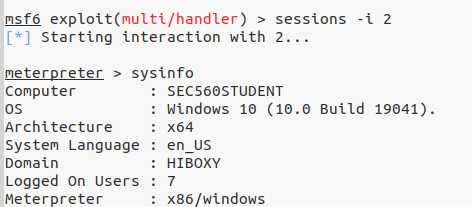


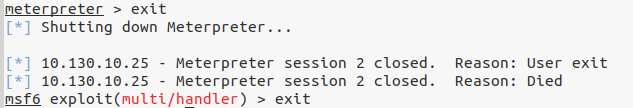






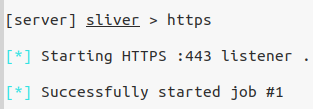


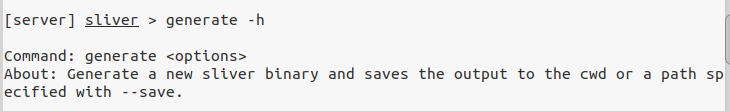


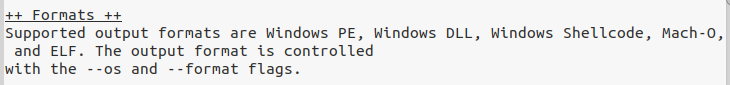


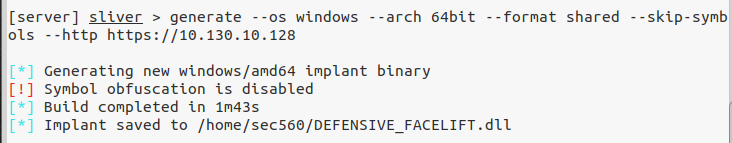
# 6. Sliver and Payloads











# 7. Copying and executing the DLL