Me and My Girlfriend（Writeup）

原创

Saber- 于 2020-01-30 22:12:44 发布 319 收藏

分类专栏： 渗透测试

本文链接：https://blog.csdn.net/qq_43691308/article/details/104108579

靶机下载

下载完成后使用VM导入

先要寻找到靶机IP地址，我用的Kali的fping

```
root@kali:~# fping -asg 192.168.1.0/24
192.168.1.1
192.168.1.5
192.168.1.2
192.168.1.3
192.168.1.8
192.168.1.12
192.168.1.7
^C
     254 targets
       7 alive
     247 unreachable
       0 unknown addresses

       0 timeouts (waiting for response)
      95 ICMP Echos sent
       7 ICMP Echo Replies received
       0 other ICMP received

 0.04 ms (min round trip time)
 42.0 ms (avg round trip time)
```

nmap挨个扫描ip地址，确定靶机为`192.168.1.12`看看有啥可以利用的

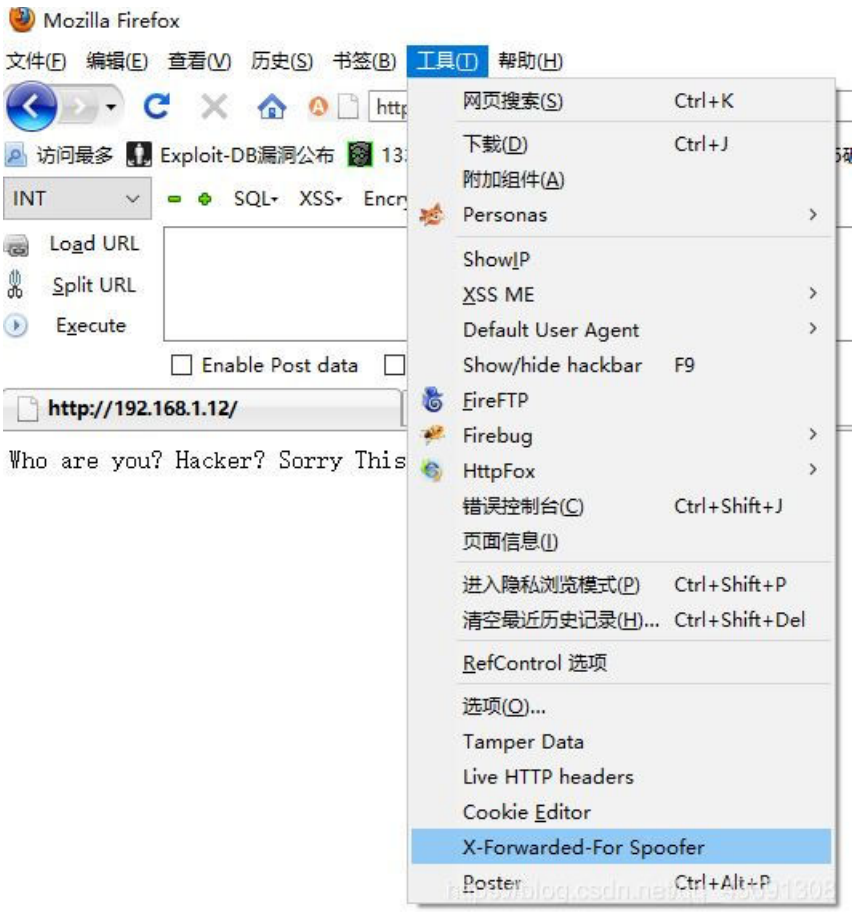
```
root@kali:~# nmap --script vulscan --script-args vulscandb=exploitdb.csv -sV 192.168.1.12
Starting Nmap 7.70 ( https://nmap.org ) at 2020-01-29 05:16 EST
Nmap scan report for 192.168.1.12
Host is up (0.000093s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13 (Ubuntu Linux; protocol 2.0)
| vulscan: exploitdb.csv:
| [3303] Portable OpenSSH <= 3.6.1p-PAM / 4.1-SUSE Timing Attack Exploit\x0D
| [21579] OpenSSH 3.x Challenge-Response Buffer Overflow Vulnerabilities (2)\x0D
| [21578] OpenSSH 3.x Challenge-Response Buffer Overflow Vulnerabilities (1)\x0D
| [21402] OpenSSH 2.x/3.x Kerberos 4 TGT/AFS Token Buffer Overflow Vulnerability\x0D
| [21314] OpenSSH 2.x/3.0.1/3.0.2 Channel Code Off-By-One Vulnerability\x0D
| [20253] OpenSSH 1.2 scp File Create/Overwrite Vulnerability\x0D
| [17462] OpenSSH 3.5p1 Remote Root Exploit for FreeBSD\x0D
| [14866] Novell Netware v6.5 OpenSSH Remote Stack Overflow\x0D
| [6094] Debian OpenSSH Remote SELinux Privilege Elevation Exploit (auth)\x0D
| [2444] OpenSSH <= 4.3 p1 (Duplicated Block) Remote Denial of Service Exploit\x0D
| [1572] Dropbear / OpenSSH Server (MAX_UNAUTH_CLIENTS) Denial of Service\x0D
| [258] glibc-2.2 and openssh-2.3.0p1 exploits glibc >= 2.1.9x\x0D
| [26] OpenSSH/PAM <= 3.6.1p1 Remote Users Ident (gossh.sh)\x0D
| [25] OpenSSH/PAM <= 3.6.1p1 Remote Users Discovery Tool\x0D
|
|_
80/tcp open  http    Apache httpd 2.4.7 ((Ubuntu))
|_http-server-header: Apache/2.4.7 (Ubuntu)
| vulscan: exploitdb.csv:
| [18329] Apache Struts2 <= 2.3.1 Multiple Vulnerabilities\x0D
|
|_
MAC Address: 00:0C:29:E9:72:AB (VMware)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 7.05 seconds
```

然并卵
既然开了80端口，访问看看

Who are you? Hacker? Sorry This Site Can Only Be Accessed local!

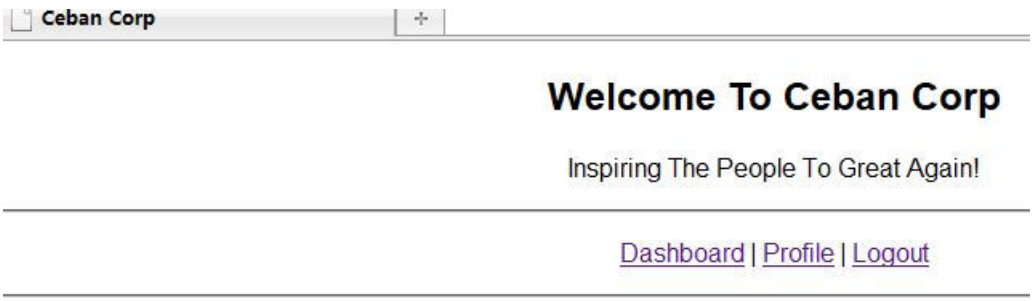
没啥东西看看源码

看样子是伪造X-FORWARDED-FOR来使服务器认为是本地访问
用burp来添加xff头，但是不知道咋每次访问时自动添加，用火狐吧



进来之后

瞎点点，随手一个admin root弱密码的碰碰运气。运气不行，扔burp字典爆破试试
失败
看来密码猜解走不通，看看有啥漏洞。
哪里有交互哪里就有可能有漏洞，一套手工+工具检测注入失败。看来没注入。
创建一个用户试试，就创建admin，万一运气爆棚，覆盖了岂不美哉。登陆



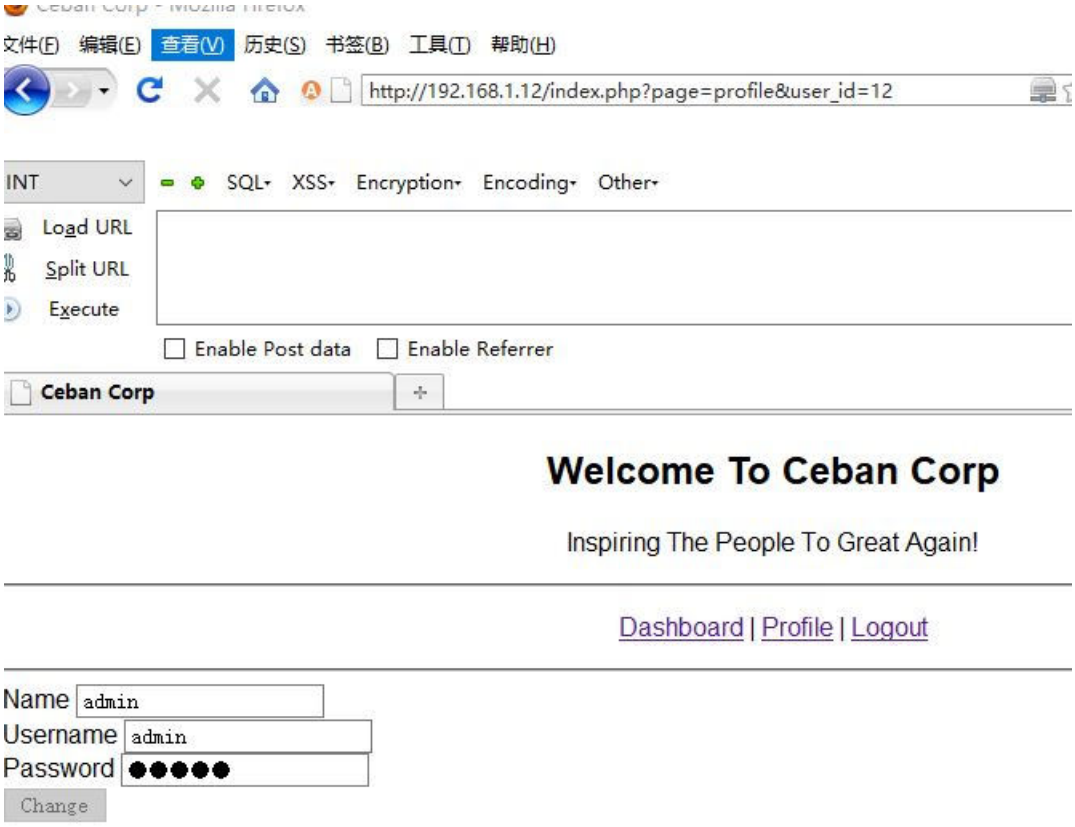
Wellcome Back!

Are you ready for Inspiring The People? Let's Do It!

没啥东西

-。-

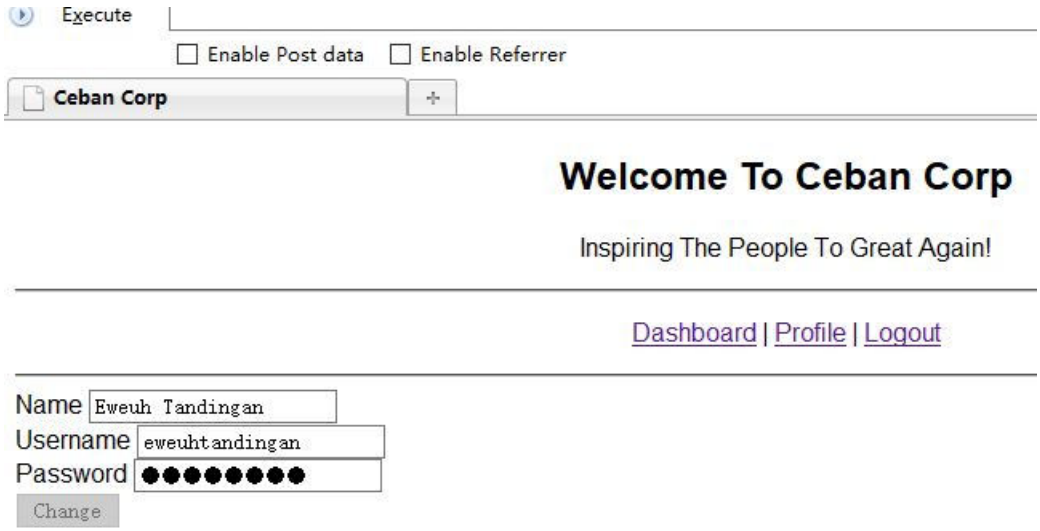
Profile点进去貌似可以修改密码，但是change点不了，要点的话需要F12修改html的disabled属性，登陆处的注入试过，试试点



profile后页面url的注入

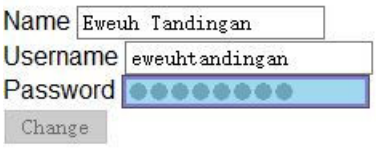
参数可控，存在数据交互。放sqlmap跑，没注入。

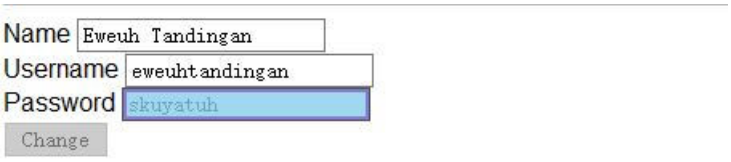
这个参数是user_id，表示用户的一个id，难道是越权？我注册了一个用户，最大可能该是1，但却是12，也就是还可能有其他用



户。

12去个2直接就是其他用户的账号密码了，账号密码收集起来。密码在html中类型为password，会隐藏，改为text





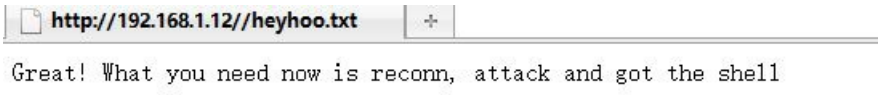
貌似都不用改了。。。他的值已经有了

遍历，收集下来。

貌似这些没地方用啊，再翻翻其他的，看看有啥敏感目录

御剑

挨个看



第一个看robots.txt的内容找到

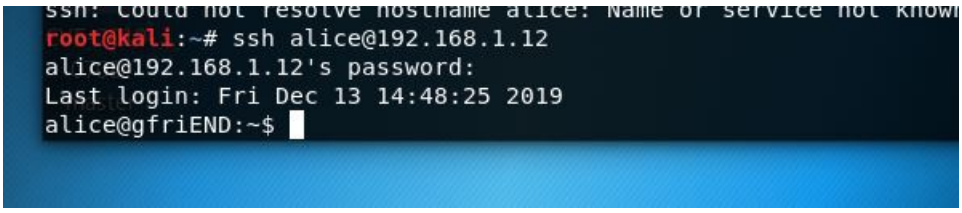
审查元素啥也没有

中间两个打开有两个php文件，但是被解析，也啥也没有。

打打游戏整理思路ing

```
开放了80，22
有几个账号密码
知道了网站有config目录和一个misc目录，但是被解析看不到下面的php文件
```

试试用账号密码能连接ssh不



轮流试，成功一个

这里有两个选择，第一个直接提权，第二个是通过其他途径提权

先不急直接提权，先看看能得到root不

```
alice@gfriEND:~$ w
 00:52:25 up  3:07,  1 user,  load average: 0.00, 0.00, 0.00
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
alice    pts/0    192.168.1.5      00:43    1.00s  0.26s  0.00s w
alice@gfriEND:~$ cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
libuuid:x:100:101::/var/lib/libuuid:
syslog:x:101:104::/home/syslog:/bin/false
messagebus:x:102:106::/var/run/dbus:/bin/false
landscape:x:103:109::/var/lib/landscape:/bin/false
alice:x:1000:1001:Alice Geulis,1337,+62,+62:/home/alice:/bin/bash
eweuhtandingan:x:1001:1002:,,,:/home/eweuhtandingan:/bin/bash
aingmaung:x:1002:1003:,,,:/home/aingmaung:/bin/bash
sundatea:x:1003:1004:,,,:/home/sundatea:/bin/bash
sshd:x:104:65534::/var/run/sshd:/usr/sbin/nologin
mysql:x:105:113:MySQL Server,,,:/var/lib/mysql:/bin/false
alice@gfriEND:~$
```

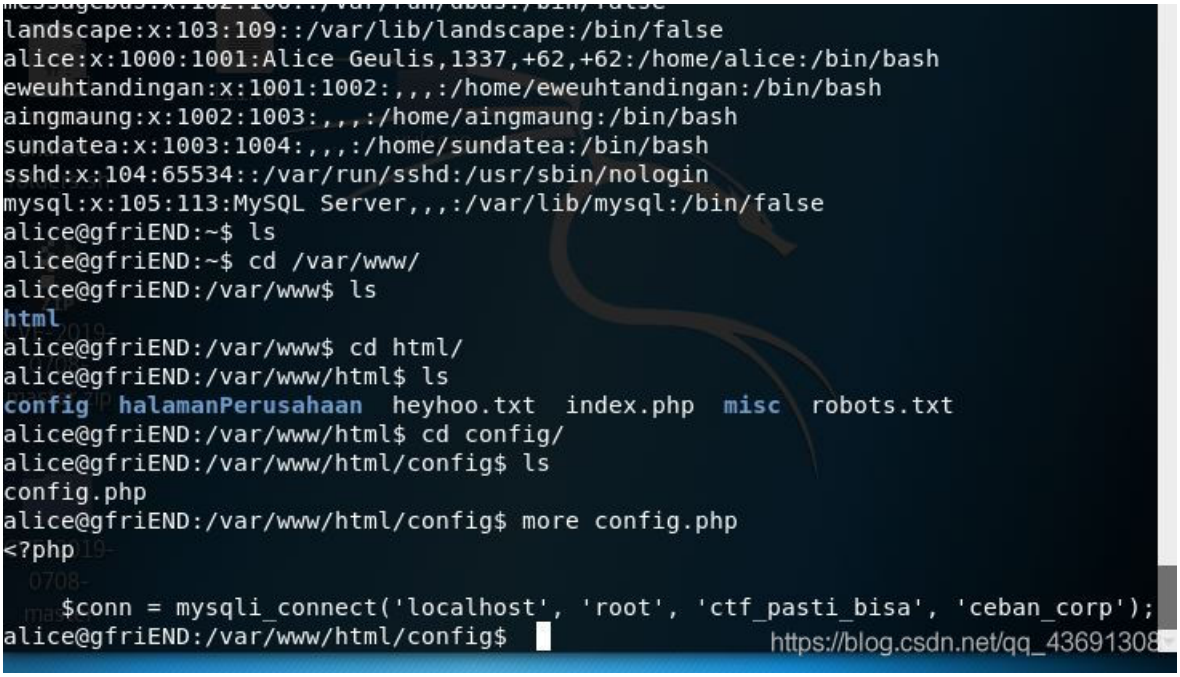
这里看到

`alice:x:1000:1001:Alice Geulis,1337,+62,+62:/home/alice:/bin/bash`

`eweuhtandingan:x:1001:1002:,,,:/home/eweuhtandingan:/bin/bash`

eweuhtandingan这个账户也可以登录但是密码不对

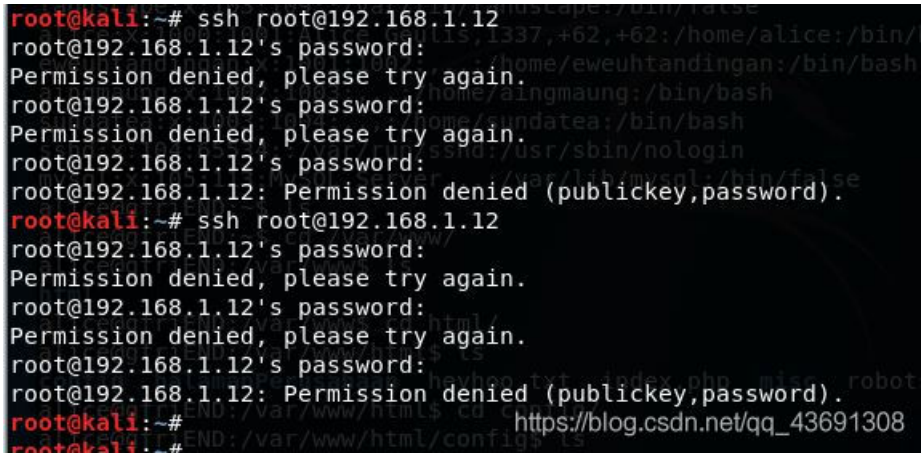
直捣黄龙，去看看配置目录和misc目录下的是个啥玩意



带有config的文件果然

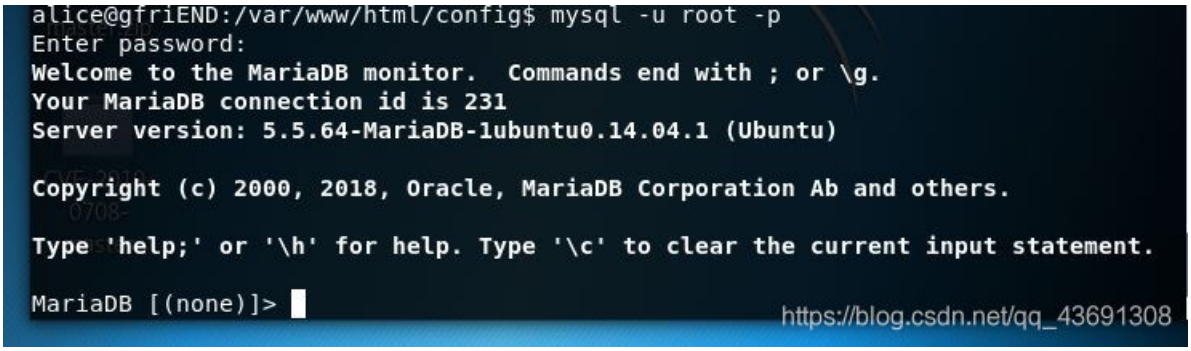
都是好东西！

连接直接用的root。。。试试这个账号密码能不能ssh连接



拒绝访问！

连接mysql看看



```
MariaDB [ceban_corp]> show databases;
+--------------------+
| Database           |
+--------------------+
| information_schema |
| ceban_corp         |
| mysql              |
| performance_schema |
+--------------------+
4 rows in set (0.00 sec)

MariaDB [ceban_corp]> show tables;
+----------------------+
| Tables_in_ceban_corp |
+----------------------+
| tbl_users            |
+----------------------+
1 row in set (0.00 sec)

MariaDB [ceban_corp]> select * from tbl_users;
+----+-----------------+---------------+-------------+------------------------------+
| id | name            | username      | password    | email                        |
+----+-----------------+---------------+-------------+------------------------------+
|  1 | Eweuh Tandingan | eweuhtandingan | skuyatuh    | eweuhtandingan@cebancorp.com |
|  2 | Aing Maung      | aingmaung     | qwerty!!!   | aingmaung@cebancorp.com      |
|  3 | Sunda Tea       | sundatea      | indONEsia   | sundatea@cebancorp.com       |
|  4 | Sedih Aing Mah  | sedihaingmah  | cedihhihihi | sedihaingmah@cebancorp.com   |
|  5 | Alice Geulis    | alice         | 4lic3       | alice@cebancorp.com          |
|  9 | Abdi Kasep      | abdikasepak   | dorrrrr     | abdikasep@cebancorp.com      |
| 12 | admin           | admin         | admin       | test@qq.com                  |
| 13 |                 | 111           | 111         |                              |
| 14 |                 | 111           | 111         |                              |
| 15 |                 | 111           | 111         |                              |
| 16 |                 | hhh           | hhh         |                              |
+----+-----------------+---------------+-------------+------------------------------+
11 rows in set (0.00 sec)

MariaDB [ceban_corp]>
```

貌似没啥，翻翻其他数据库里也没啥东西。继续去系统里找找有没有东西。
找不到，可能被隐藏了
find大法

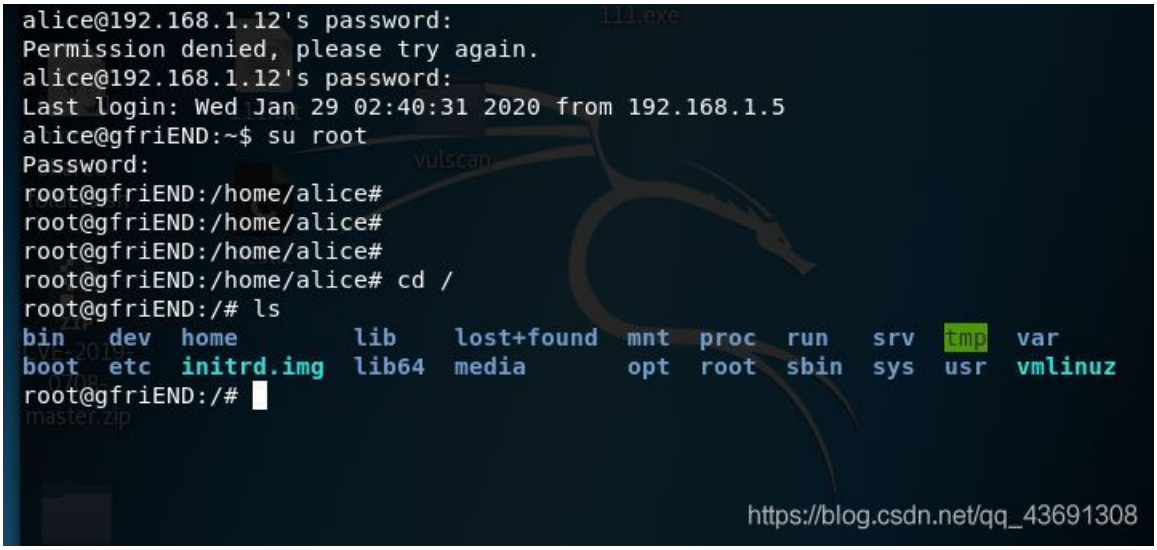
```
alice@gfriEND:~$ find / .*(flag)* | grep flag
```

找到了很多，最后发现了flag

```
/sys/devices/platform/serial8250/tty/ttyS30/flags
/sys/devices/platform/serial8250/tty/ttyS31/flags
find: `/sys/kernel/debug': Permission denied
/sys/module/scsi_mod/parameters/default_dev_flags
find: `/lost+found': Permission denied
./.my_secret/flag1.txt
../alice/.my_secret/flag1.txt
.my_secret/flag1.txt
```

```
alice@gfriEND:~$ ls -a
.   .bash_history  .bashrc  .my_secret      .profile
..  .bash_logout   .cache   .mysql_history
alice@gfriEND:~$ cd .my_secret/
alice@gfriEND:~/.my_secret$ ls
flag1.txt  my_notes.txt
alice@gfriEND:~/.my_secret$ cat flag1.txt
Greattttt my brother! You saw the Alice's note! Now you save the record information to give to bob! I know if it
's given to him then Bob will be hurt but this is better than Bob cheated!

Now your last job is get access to the root and read the flag ^_^

Flag 1 : gfriEND{2f5f21b2af1b8c3e227bcf35544f8f09}
alice@gfriEND:~/.my_secret$
```

找到flag了，说可以开始尝试获取root。
刚才root账户不能ssh连接，试试能不能本地su切换，Ubuntu root账户默认都是不能直接ssh连接。



root登陆成功。