GamingServer_THM

Enumuration

Web source code reveales 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

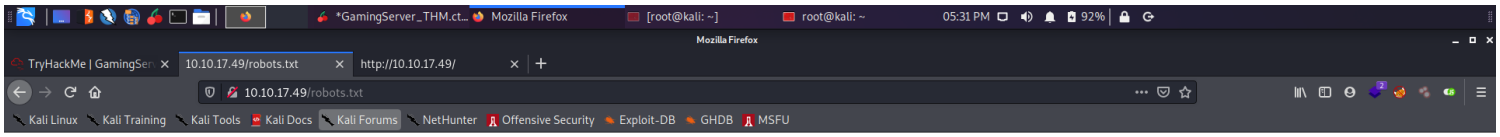
```
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 34:0e:fe:06:12:67:3e:a4:eb:ab:7a:c4:81:6d:fe:a9 (RSA)
|   256 49:61:1e:f4:52:6e:7b:29:98:db:30:2d:16:ed:f4:8b (ECDSA)
|_  256 b8:60:c4:5b:b7:b2:d0:23:a0:c7:56:59:5c:63:1e:c4 (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

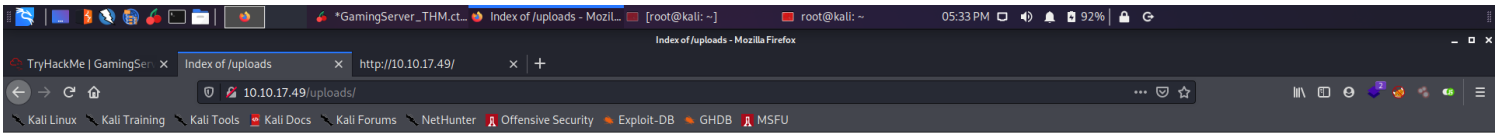
```
#  /uploads
```



#

/uploads

interesting files



Index of /uploads

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 10.10.17.49 Port 80

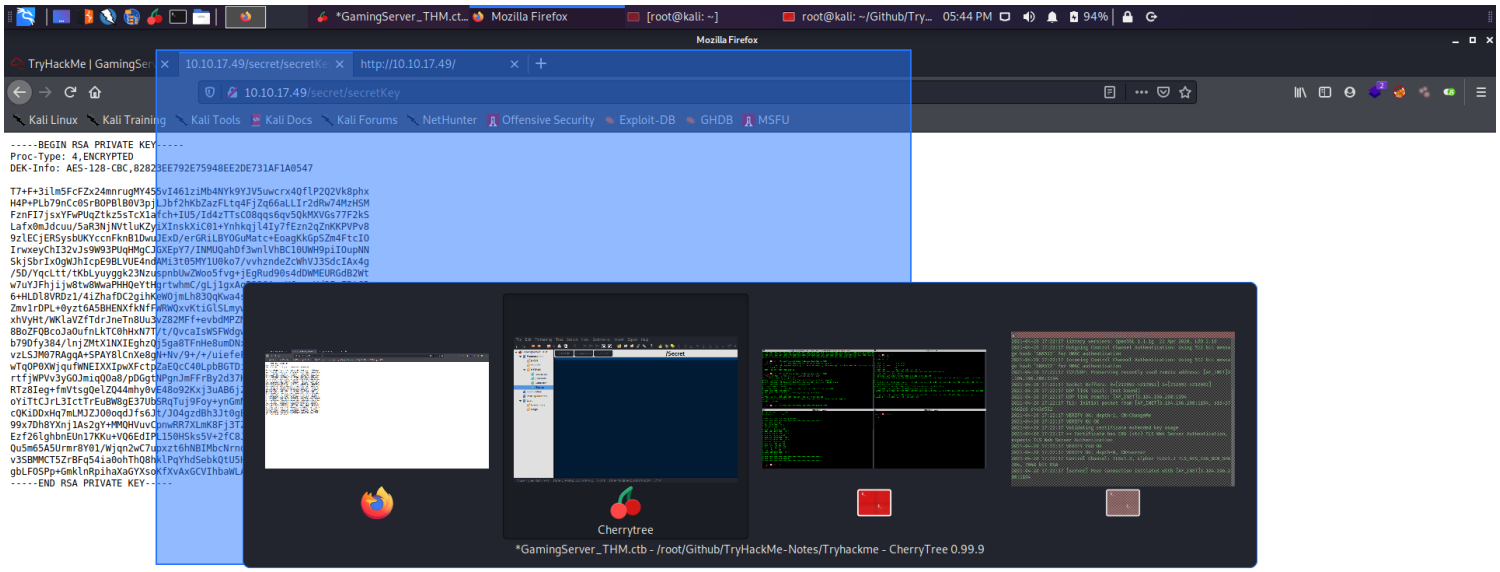
#

Gobuster

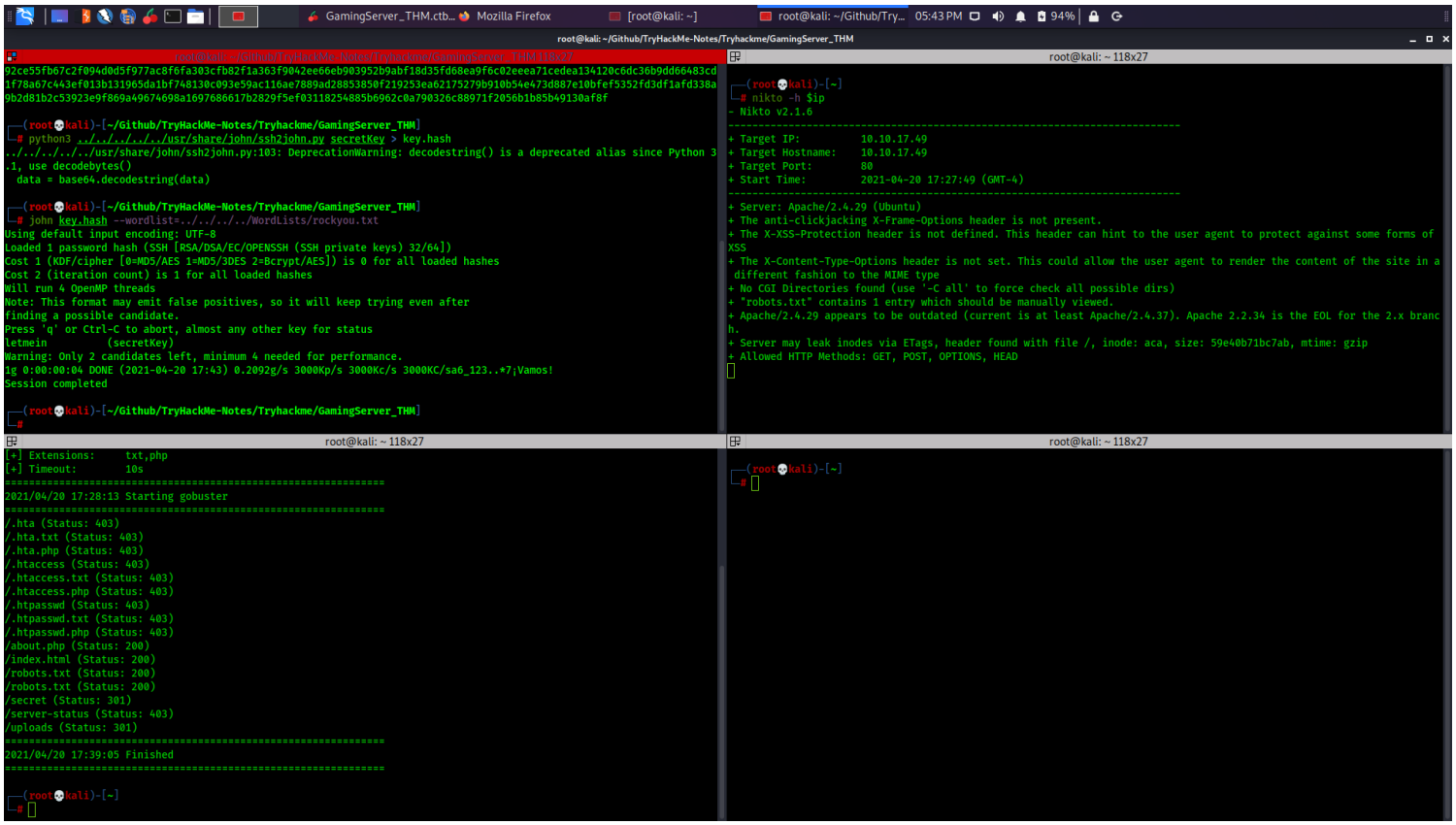
hta.txt (Status: 403)
/.hta.php (Status: 403)
/.htaccess (Status: 403)
/.htaccess.txt (Status: 403)
/.htaccess.php (Status: 403)
/.htpasswd (Status: 403)
/.htpasswd.txt (Status: 403)
/.htpasswd.php (Status: 403)
/about.php (Status: 200)
/index.html (Status: 200)
/robots.txt (Status: 200)
/robots.txt (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

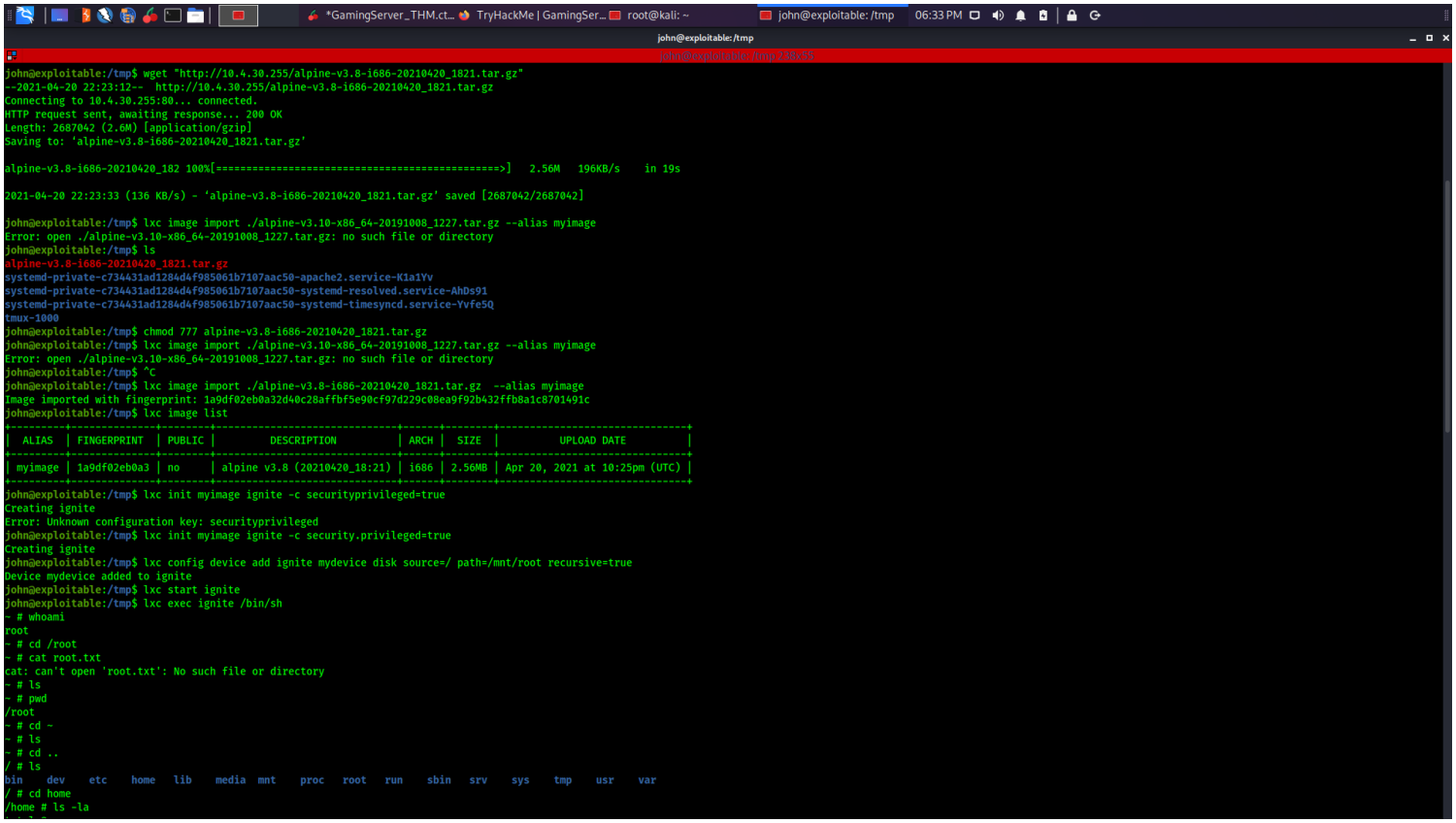
PostExploitation

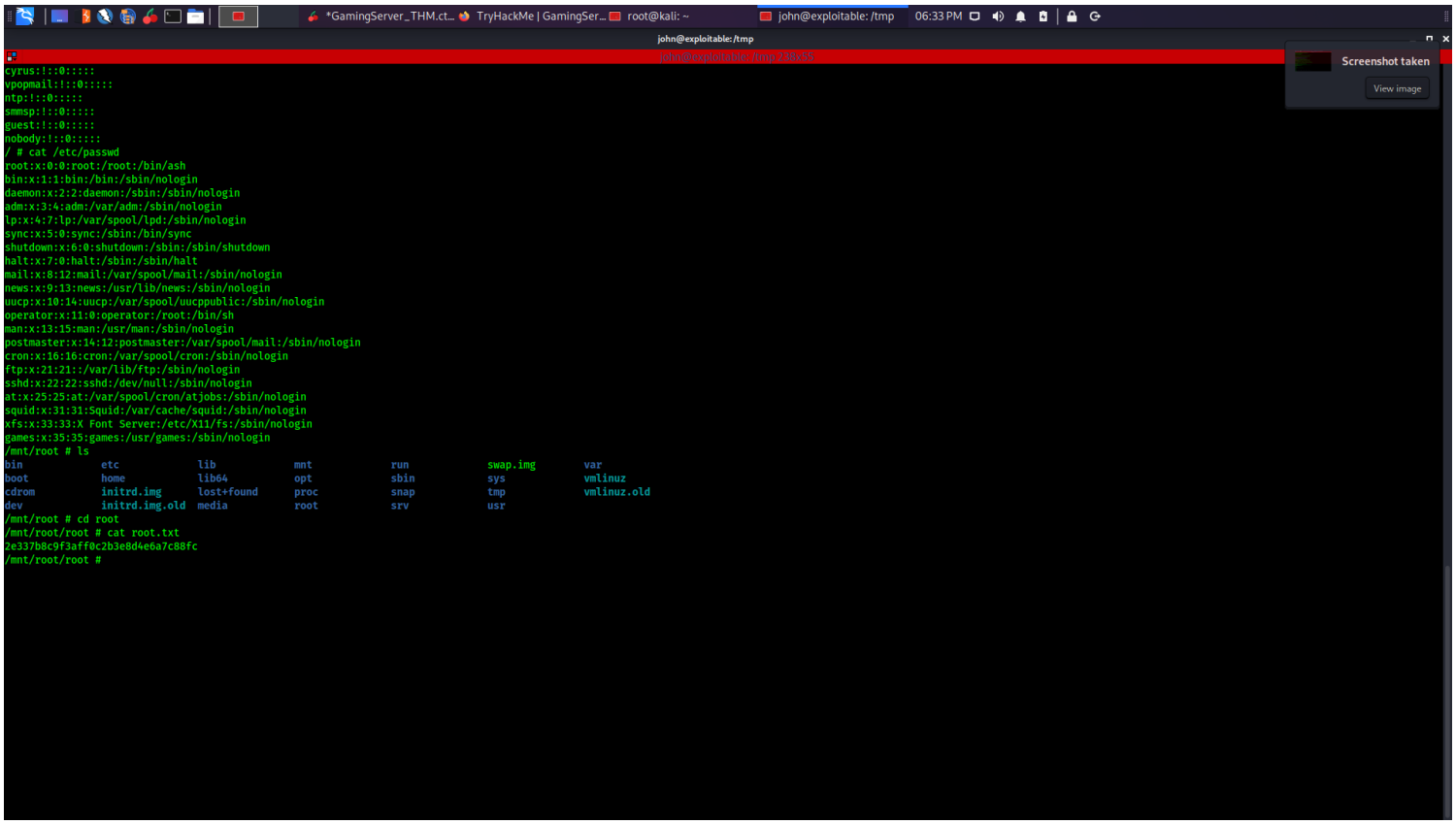
AFter getting access we see that sudo password is required for john which we dont have

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 oveer to that container and have root access





#

Loot

Credentials

We got a dictionary from /uploads directory

Flags

User Flag

a5c2ff8b9c2e3d4fe9d4ff2f1a5a6e7e

Root Flag

2e337b8c9f3aff0c2b3e8d4e6a7c88fc