ANONFORCE -- WriteUp

MACHINE DETAILS:

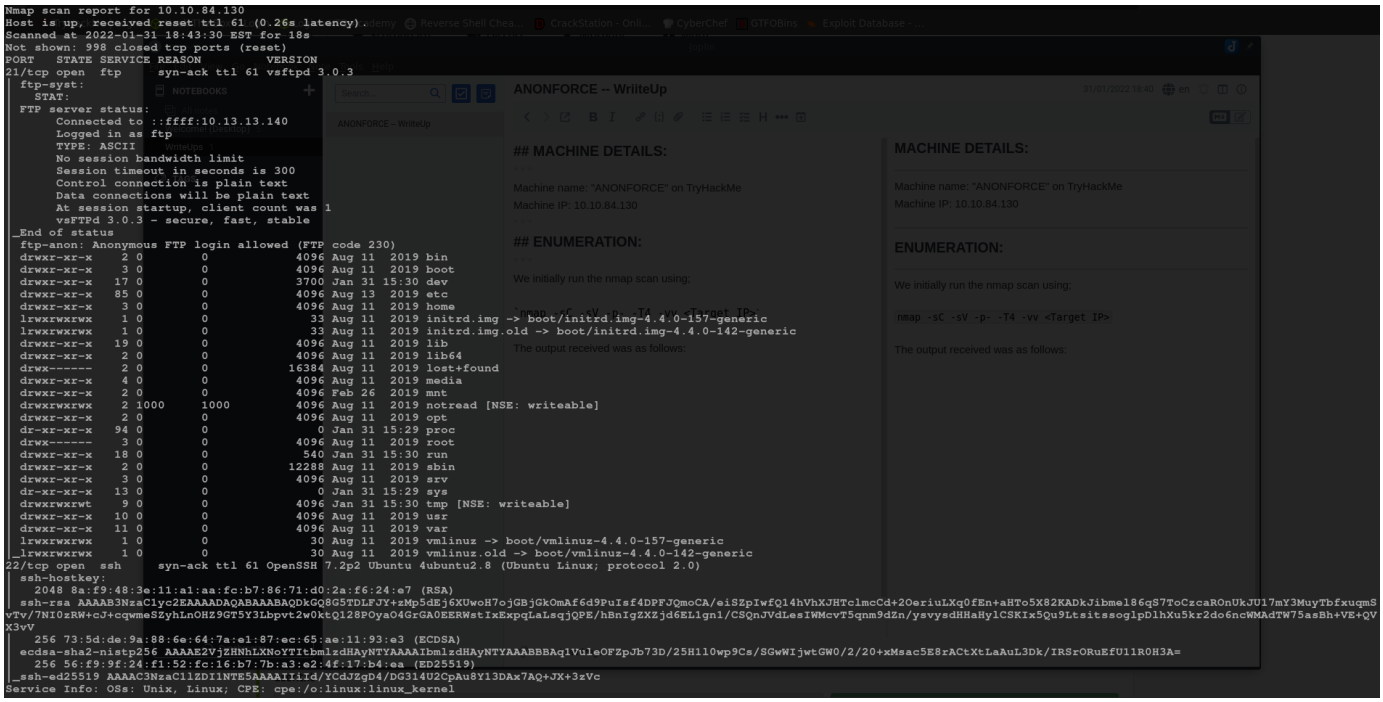
Machine name: "ANONFORCE" on TryHackMe
Machine IP: 10.10.84.130

ENUMERATION:

We initially run the nmap scan using;

`nmap -sC -sV -p- -T4 -vv <Target IP>`

The output received was as follows:



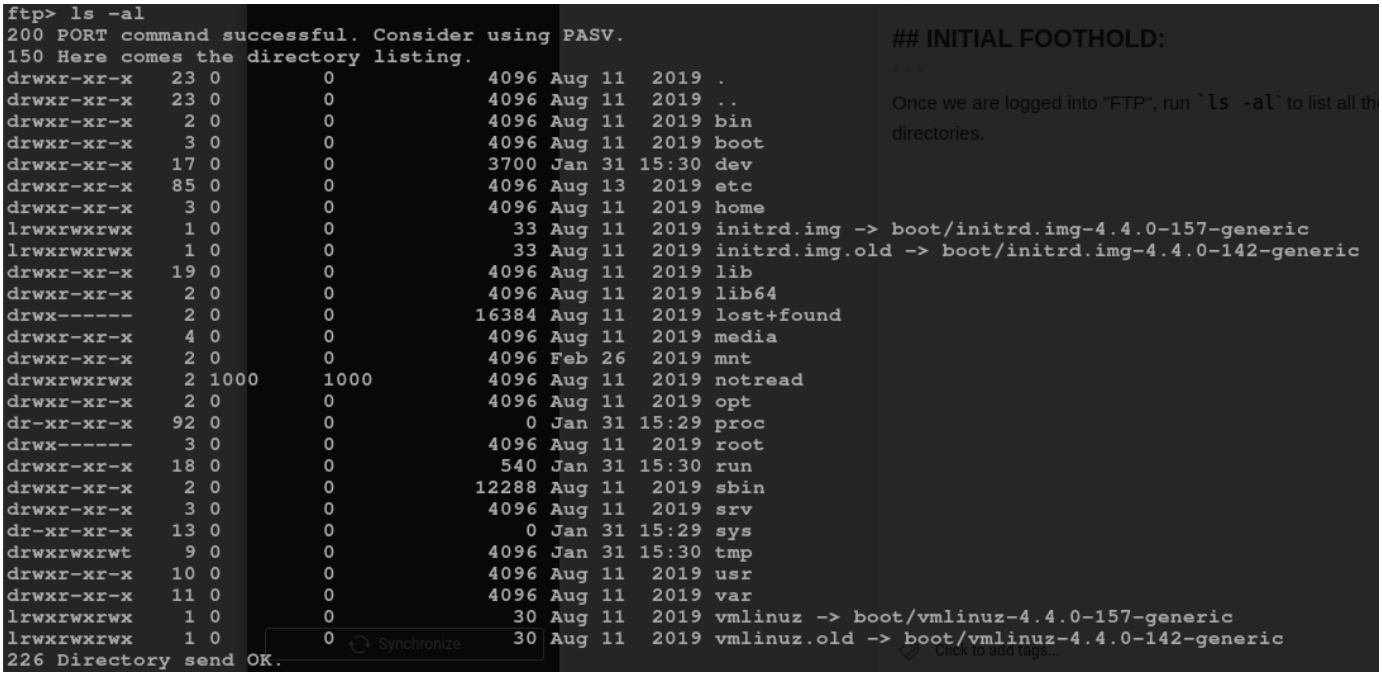
We can see that "FTP" and "SSH" are open, also anonymous login is allowed on the FTP service. We access FTP service using;

`ftp <target IP>`

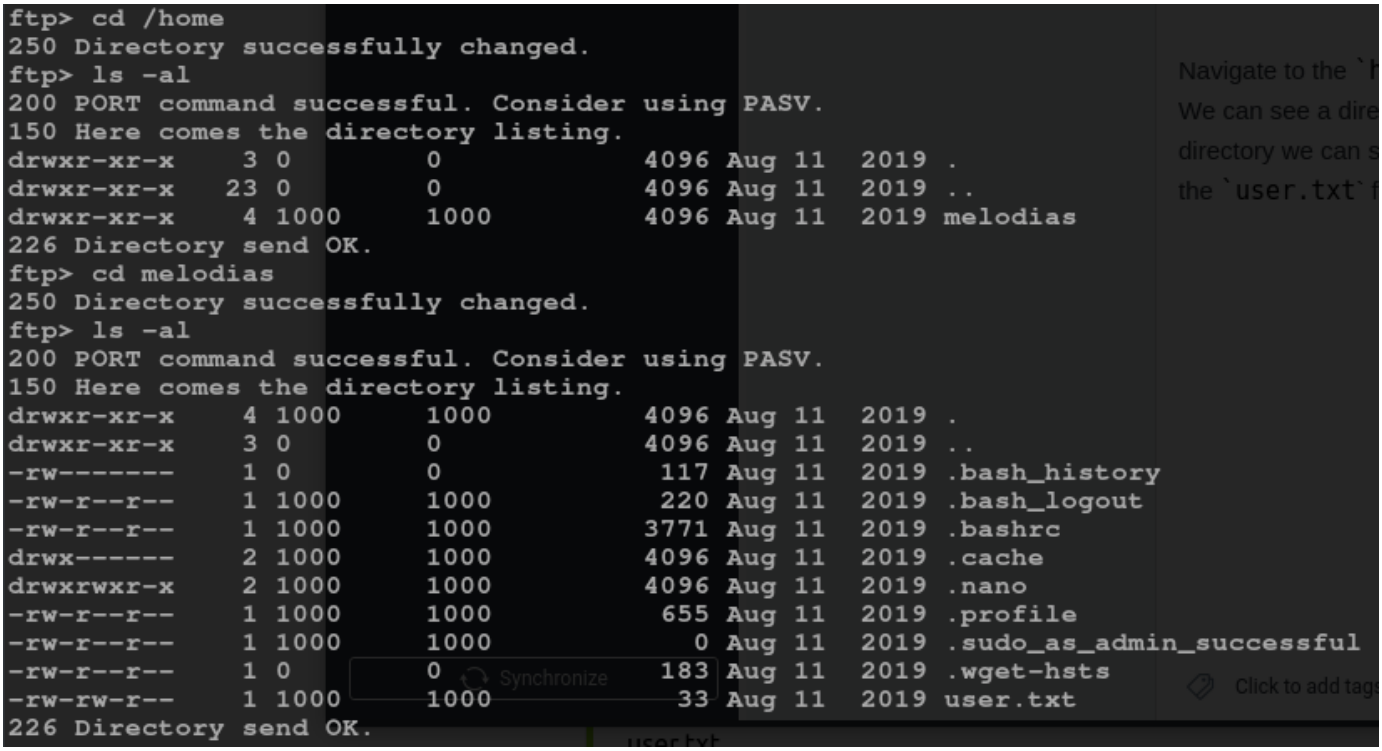
And enter "Username" as `Anonymous` and then hit enter when prompted for password, then you'll get into the `/` directory.

INITIAL FOOTHOLD:

Once we are logged into "FTP", run `ls -al` to list all the files and directories.



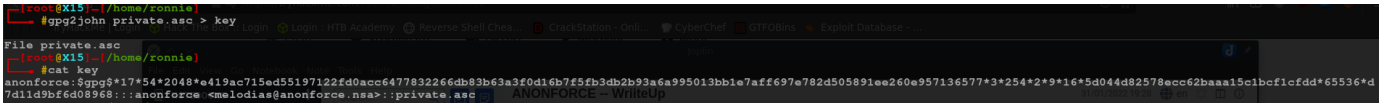
Navigate to the `home` directory using `cd /home` and list the contents. We can see a directory called `melodias` and when we move into the directory we can see a file called `user.txt`. Run `get user.txt` and the `user.txt` file gets downloaded onto your attacking OS.



PRIVELEGE ESCALATION:

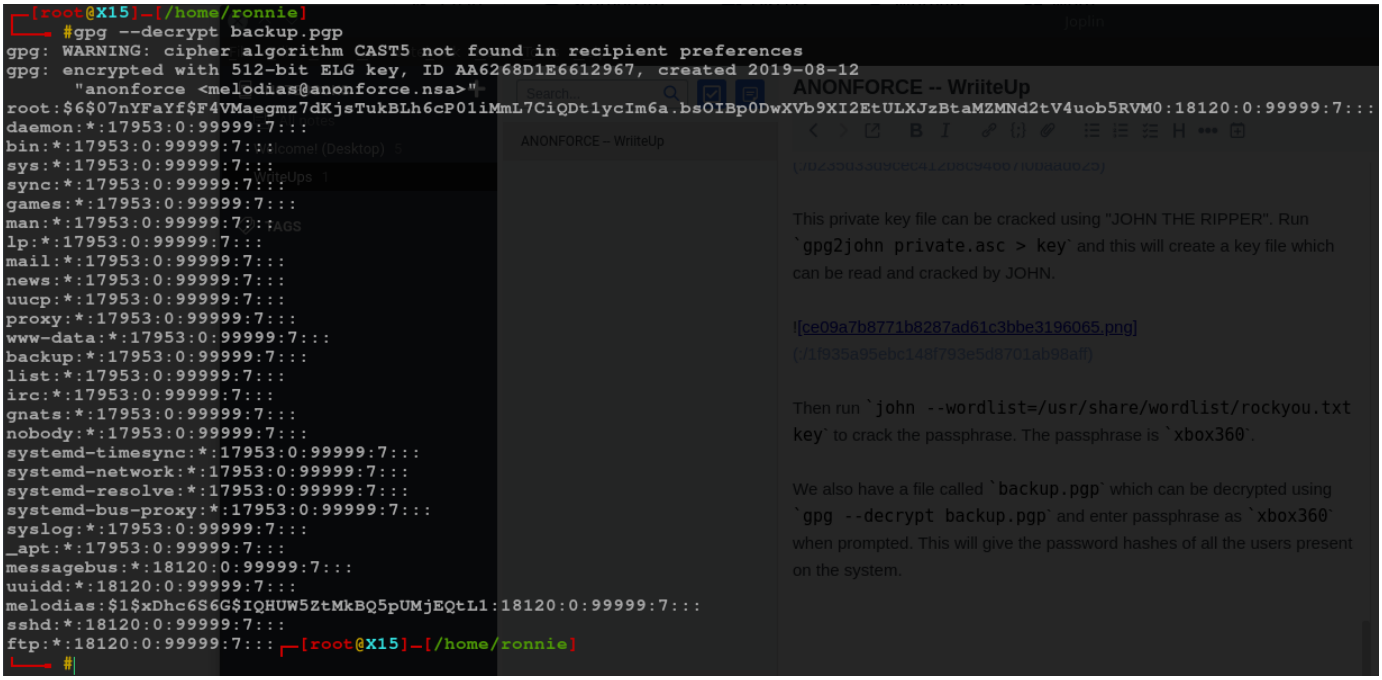
Going back to `/` directory, we can see a directory named `notread`. Moving into the directory we can see two files; `backup.pgp` and `private.asc`. After downloading both the files, we can see that `private.asc` is a `PGP private key` file.

This private key file can be cracked using "JOHN THE RIPPER". Run `gpg2john private.asc > key` and this will create a key file which can be read and cracked by JOHN.



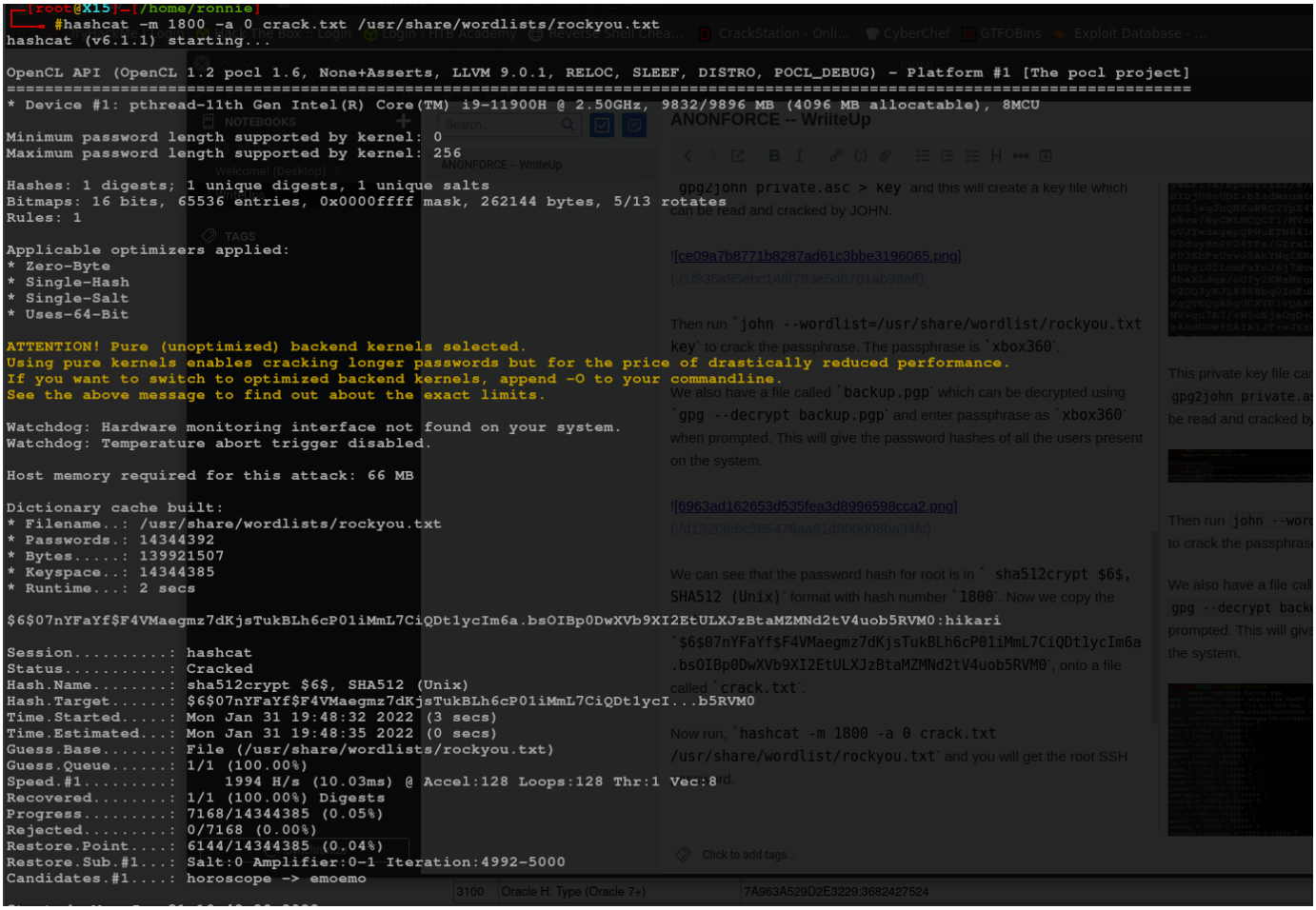
Then run `john --wordlist=/usr/share/wordlist/rockyou.txt key` to crack the passphrase. The passphrase is `xbox360`.

We also have a file called `backup.pgp` which can be decrypted using `gpg --decrypt backup.pgp` and enter passphrase as `xbox360` when prompted. This will give the password hashes of all the users present on the system.



We can see that the password hash for root is in `sha512crypt $6$, SHA512 (Unix)` format with hash number `1800`. Now we copy the hash, `$6$07nYFaYf$F4VMaegmz7dKjsTukBLh6cP01iMmL7CiQDt1ycIm6a.bsOIBp0DwXVb9XI2EtULXJzBtaMZMNd2tV4uob5RVM0`, onto a file called `crack.txt`.

Now run, `hashcat -m 1800 -a 0 crack.txt /usr/share/wordlist/rockyou.txt` and you will get the root SSH password.



Now you can SSH into the root account and extract the contents of `root.txt`.

/MACHINE ROOTED/
