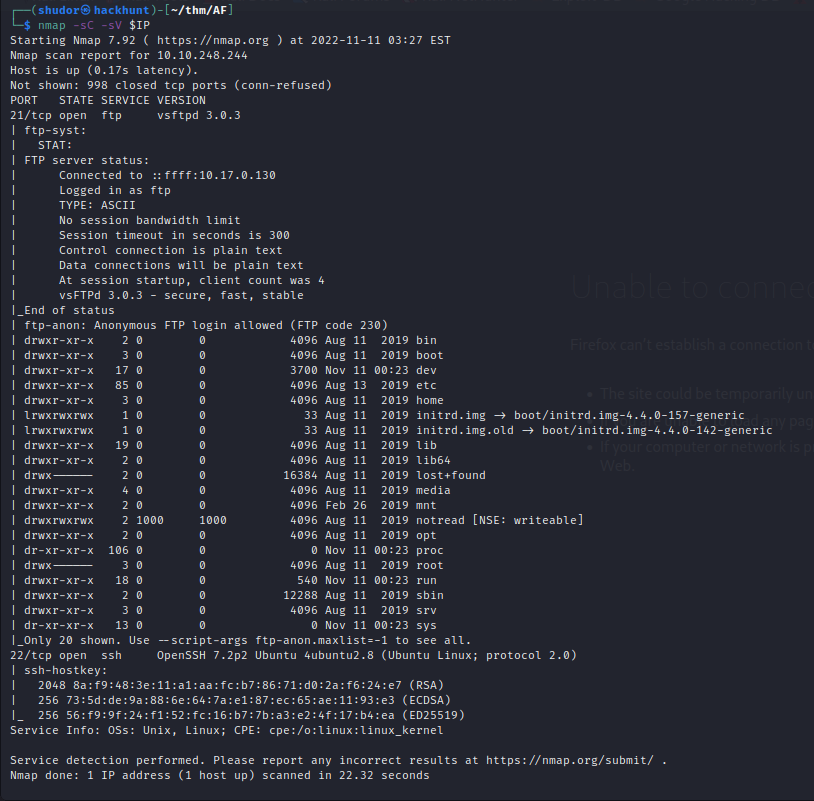
For this room to get user.txt and root.txt we do following steps:

1. We will run nmap scan on the ip address using below command

nmap -sC -sV $IP

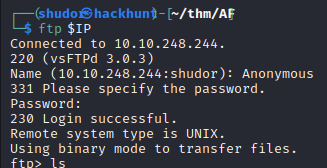


2. After scanning of ip address we get two open ports

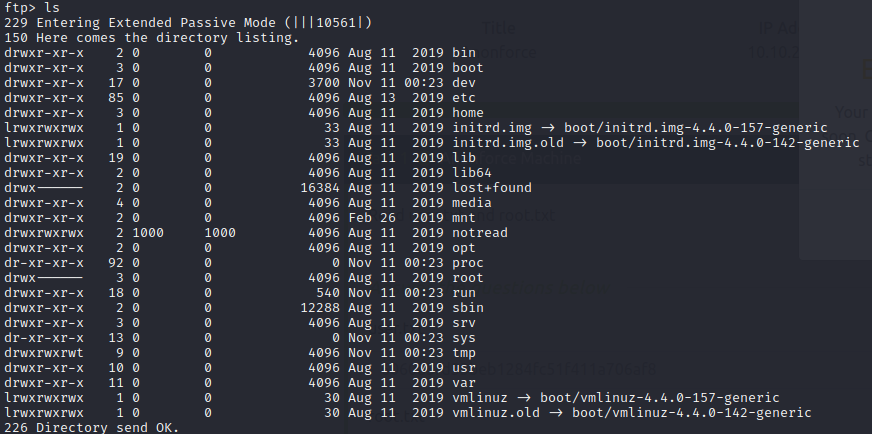
21/tcp

22/tcp

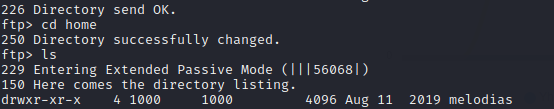
In port 21 there many directories so we can login in the port 21 using id Anonymous



3. We can look all the directories using ls command



4. We will open the home directory



Inside the home directory with the help of ls command we get one user directory name “melodias”

We will open the melodias directory

Text

Description automatically generated

Inside the melodias directory with the help of ls command we find the user text

With the help of get command we will extract the user text file from the melodias directory

Text

Description automatically generated

Now from here our one task finished because we get the user.txt

Graphical user interface, application, Teams

Description automatically generated

We will exit from home directory using cd .. command

Now our task is to find root.txt

5. In all the directories of 21 port notread looks suspicious. So we switch to that directory using cd notread command. And open the directory using ls command

Text

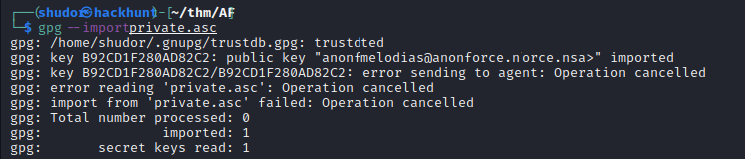
Description automatically generated

Here we find two files. With the help of get command we extracted both file and get exited from the port

Text

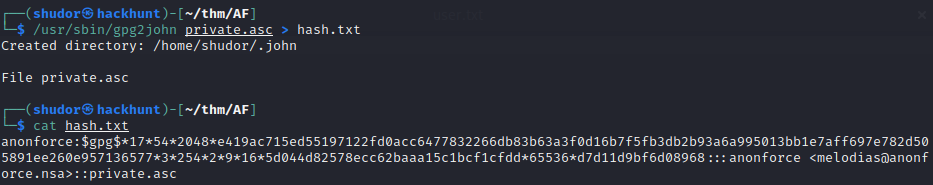
Description automatically generated

6. when I tried to open private.asc it is not accessible because it password protected and backup.pgp file is encrypted aso not able to understand anything.

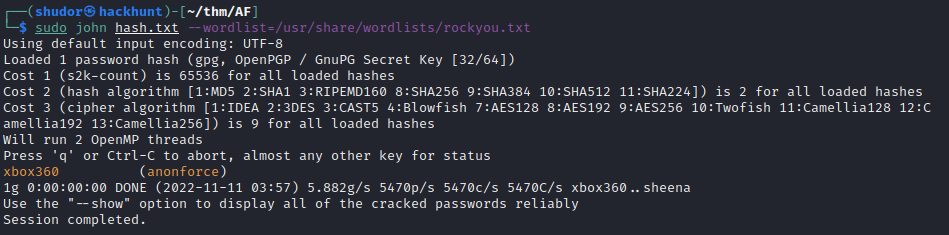


7. We need jhonreeper to extract the passphrase to open private.asc.

For that first we need to convert private.asc into hash file which will be readable by jhonthereeper

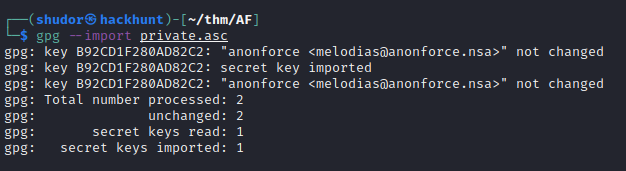


With the help of hash file we will extract the passphrase with the help of jhonthe ripper

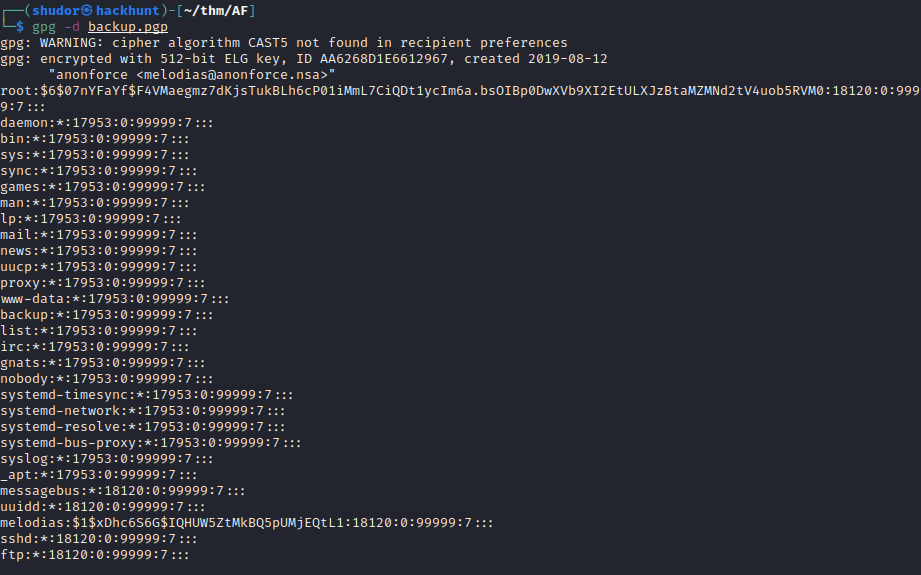


We got the passphrase

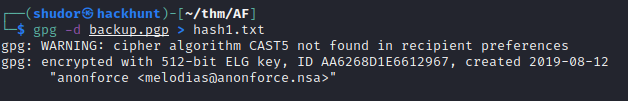
8. With the help of passphrase we will open the private.asc



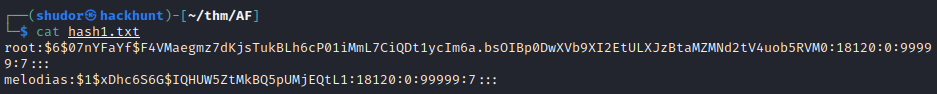
9. Now we have open the private.asc with the help it we can decrypt backup.pgp



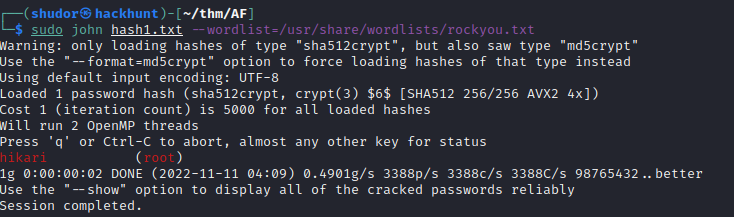
We will extract the decrypted backup.pgp into hash file



We will remove other data only keep root and user hash



10. With the help of johnthe reeper we will extract the passphrase to login in the root



11. We got the passphrase we will login in the root and get the root.txt

