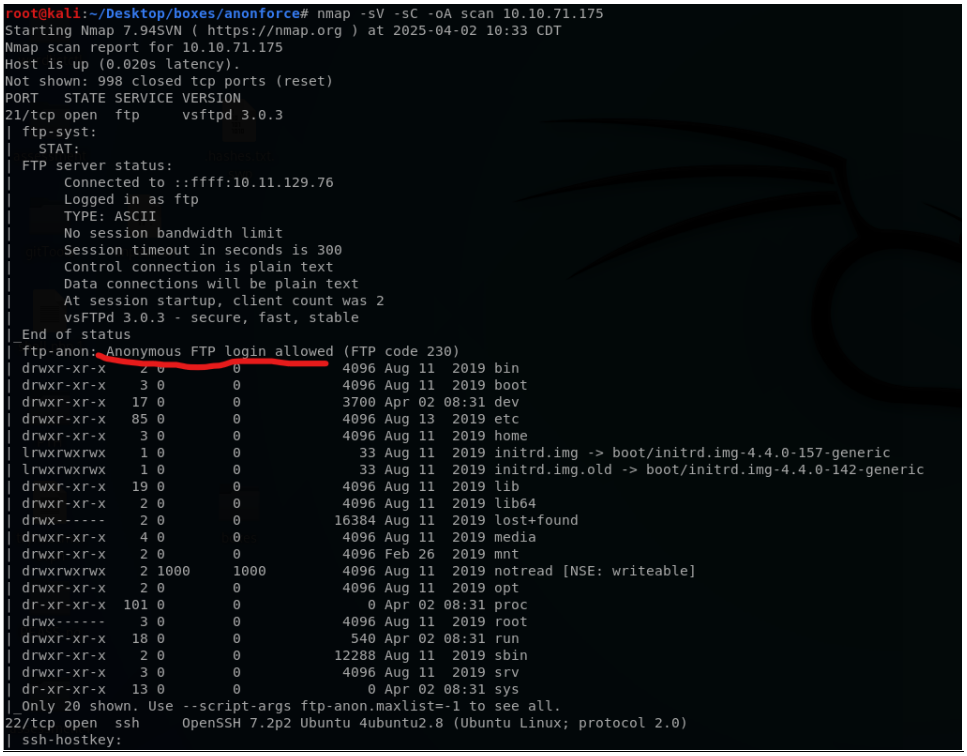
Starting with an Nmap scan, we find open SSH and FTP ports, with FTP allowing anonymous login.

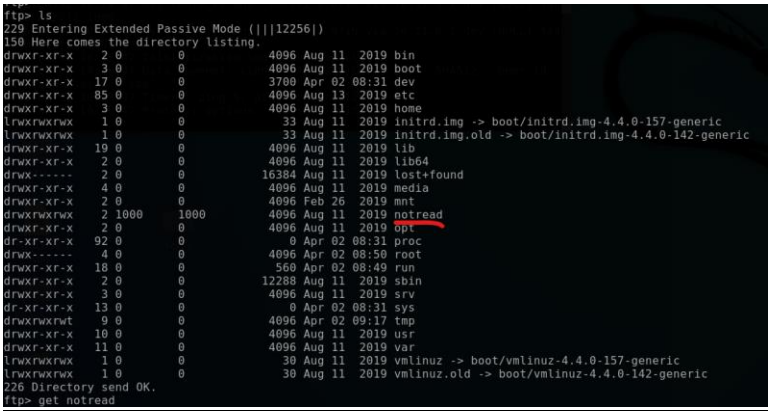


Logging into FTP anonymously, we discover three interesting files:

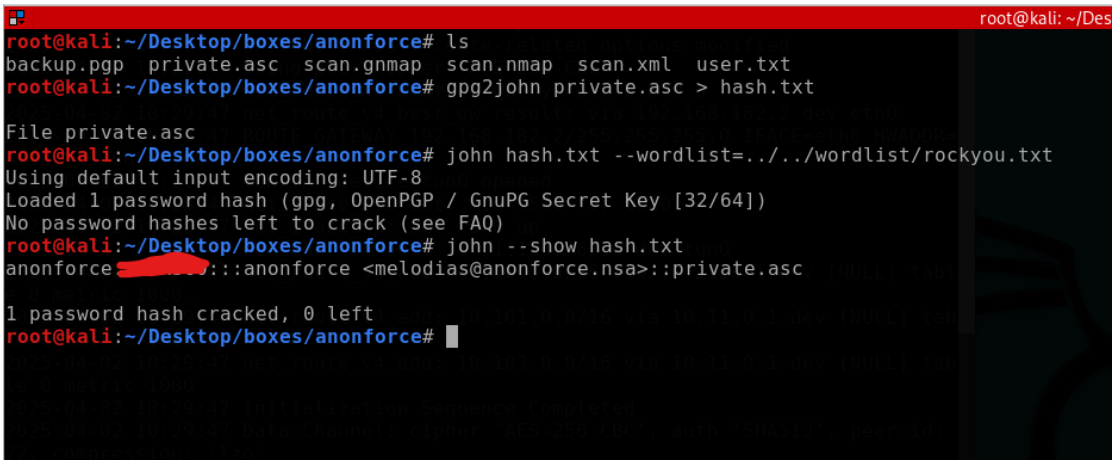
/notread/backup.pgp

/notread/private.asc

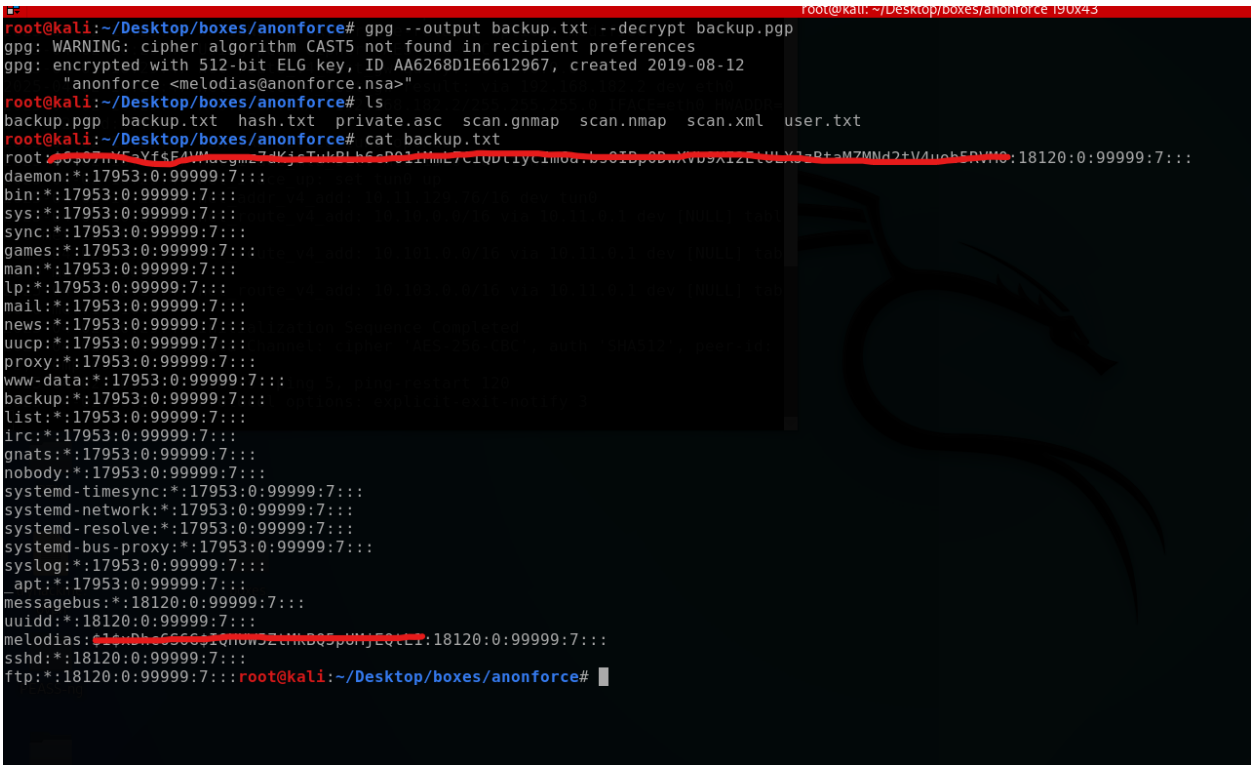
/home/melodias/user.txt



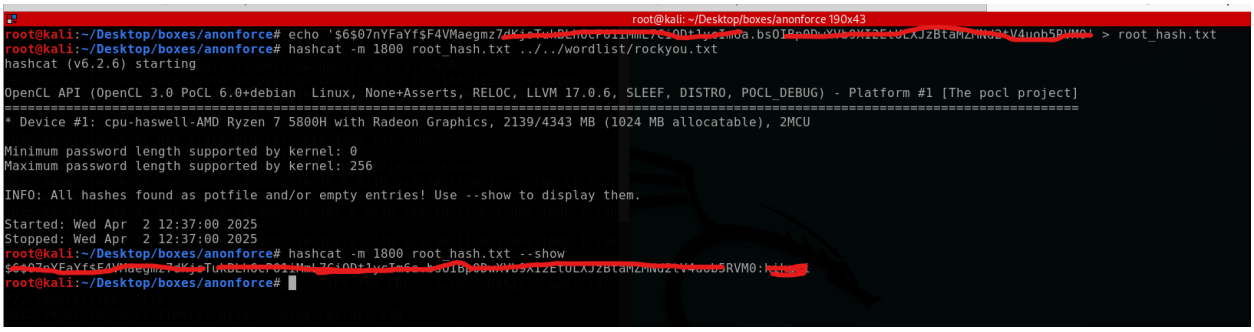
We download both backup.pgp and its private key (private.asc). To decrypt backup.pgp, we first need the passphrase of the private key. Using gpg2john, we extract a hash from private.asc, then crack it with John the Ripper to reveal the passphrase.



With the passphrase obtained, we decrypt backup.pgp using the gpg tool. The decrypted file contains system user hashes, including the hashes for the root and melodias users.



We save the root hash to a file and crack it using Hashcat with mode 1800 (sha512crypt).



Finally, using the cracked root password, we SSH into the server as root and obtain root.txt.