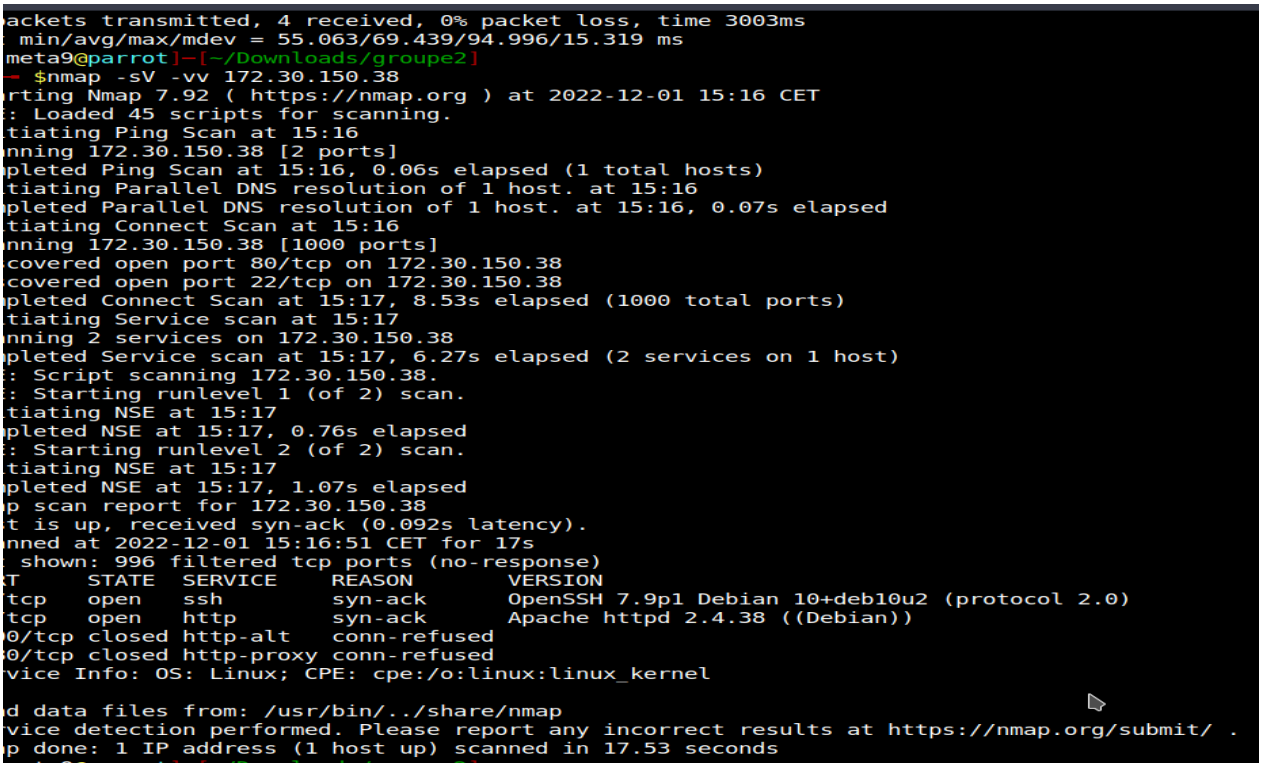
Solution challenge 1 : Easy Peasy

1. *Le premier flag :*

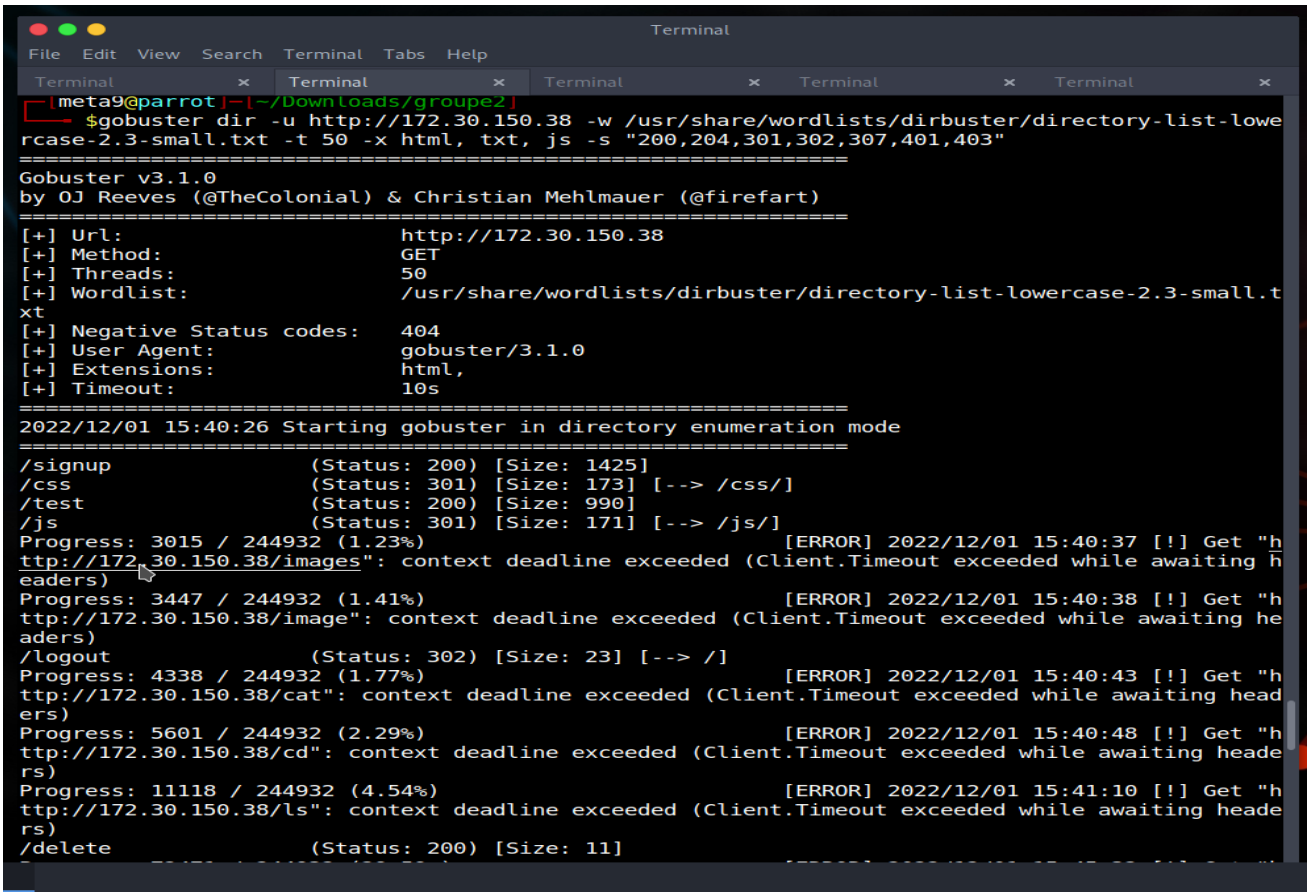
Reconnaissance avec Nmap pour découvrir le serveur Web puis effectuer une Web Directory Numération avec Gobuster pour trouver le premier flag dans ip/robots.txt de la page tomygrpCmd.com.



On remarque dans la commande nmap les options suivantes :

-sV : pour afficher toutes les informations liées aux services.

-vv : option very verbose pour afficher les informations en mode débogage



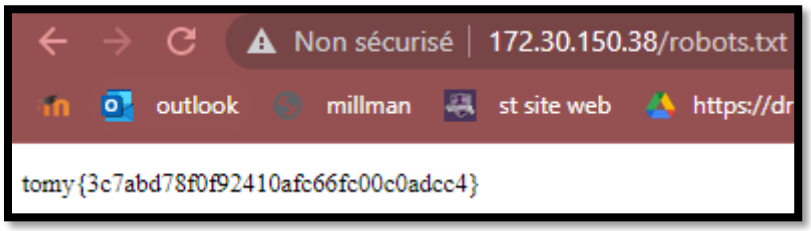
Les options :

-u : le lien du site

-w : pour récupérer la liste qu'on va utiliser

-t : pour déterminer le nombre des threads

-x : pour déterminer les extensions des fichiers recherchés



2. *Le deuxième flag :*

Faire un brute force login avec Hydra pour avoir l'accès au tomygrpCmd.com qui été conçu par les développeurs pour faire des tests uniquement. Après avoir réussir l'authentification utilisé la ligne de commandes pour trouver le deuxième flag sous forme du fichier texte et le lire.

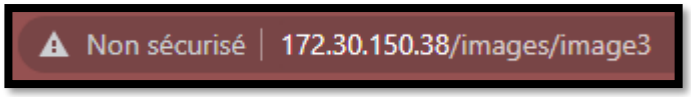
Connectez-vous avec le login admin et le mot de passe trouvé par Hydra et cherché le flag dans fichier.txt

```
root@tomy: ~/folder$ cat fichier.txt
tomy{61a0a824765dc715d0af0f65ddbdf915}
```

3. *<u>Le troisième flag :</u>*

Utiliser le lien ip/images/image3 pour récupérer un fichier png qui cache le troisième flag. Utilisé un outil de stéganographie qui permet de lister toutes les informations de cette image ainsi que le flag 3.

En accédant à ce chemin on aura



Le flag trouvé par stegonline (exemple d'un outil de stéganographie)