

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 :

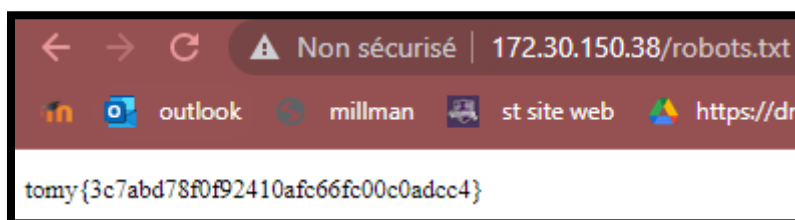
- sV : pour afficher toutes les informations liées aux services.
- vv : option `very verbose` pour afficher les informations en mode débogage

```
Terminal
File Edit View Search Terminal Tabs Help
[meta9@parrot:~/Downloads/groupe2]
$ gobuster dir -u http://172.30.150.38 -w /usr/share/wordlists/dirbuster/directory-list-lowercase-2.3-small.txt -t 50 -x html,txt,js -s "200,204,301,302,307,401,403"

=====
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
=====
[+] Url: http://172.30.150.38
[+] Method: GET
[+] Threads: 50
[+] Wordlist: /usr/share/wordlists/dirbuster/directory-list-lowercase-2.3-small.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.1.0
[+] Extensions: html,txt,js
[+] Timeout: 10s
=====
2022/12/01 15:40:26 Starting gobuster in directory enumeration mode
=====
/signup (Status: 200) [Size: 1425]
/css (Status: 301) [Size: 173] [--> /css/]
/test (Status: 200) [Size: 990]
/js (Status: 301) [Size: 171] [--> /js/]
Progress: 3015 / 244932 (1.23%) [ERROR] 2022/12/01 15:40:37 [!] Get "http://172.30.150.38/images": context deadline exceeded (Client.Timeout exceeded while awaiting headers)
Progress: 3447 / 244932 (1.41%) [ERROR] 2022/12/01 15:40:38 [!] Get "http://172.30.150.38/image": context deadline exceeded (Client.Timeout exceeded while awaiting headers)
/logout (Status: 302) [Size: 23] [--> /]
Progress: 4338 / 244932 (1.77%) [ERROR] 2022/12/01 15:40:43 [!] Get "http://172.30.150.38/cat": context deadline exceeded (Client.Timeout exceeded while awaiting headers)
Progress: 5601 / 244932 (2.29%) [ERROR] 2022/12/01 15:40:48 [!] Get "http://172.30.150.38/cd": context deadline exceeded (Client.Timeout exceeded while awaiting headers)
Progress: 11118 / 244932 (4.54%) [ERROR] 2022/12/01 15:41:10 [!] Get "http://172.30.150.38/ls": context deadline exceeded (Client.Timeout exceeded while awaiting headers)
/delete (Status: 200) [Size: 11]
```

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 réussi 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{61a0a024765dc715d0af0f65ddbdf915}
```

3. Le troisième flag :

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

⚠ Non sécurisé | 172.30.150.38/images/image3

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

(tomy{a98b5ce98ad49e5dba91a17652f49f4f})