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.

```
ackets transmitted, 4 received, 0% packet loss, time 3003ms
.min/avg/max/mdev = 55.063/69.439/94.996/15.319 ms
meta9@parrotl-[-/Downloads/groupe2]
- $mmap -sV -vv 172.30.150.38
rting Nmap 7.92 (https://nmap.org ) at 2022-12-01 15:16 CET
: Loaded 45 scripts for scanning.
tiating Ping Scan at 15:16
nning 172.30.150.38 [2 ports]
pleted Ping Scan at 15:16, 0.06s elapsed (1 total hosts)
tiating Parallel DNS resolution of 1 host. at 15:16
pleted Parallel DNS resolution of 1 host. at 15:16
overed open port 80/tcp on 172.30.150.38
covered open port 80/tcp on 172.30.150.38
covered open port 22/tcp on 172.30.150.38
pleted Connect Scan at 15:17, 8.53s elapsed (1000 total ports)
tiating Service scan at 15:17, 6.27s elapsed (2 services on 1 host)
: Script scanning 172.30.150.38.
starting runlevel 1 (of 2) scan.
tiating NSE at 15:17
pleted NSE at 15:17, 0.76s elapsed
: Starting runlevel 2 (of 2) scan.
tiating NSE at 15:17
pleted NSE at 15:17, 1.07s elapsed
: Starting runlevel 2 (of 2) scan.
tiating NSE at 15:17
pleted NSE at 15:17 to 76s elapsed
: Starting runlevel 2 (of 2) scan.
tiating NSE at 15:17
pleted NSE at 15:17 to 76s elapsed
: Starting runlevel 2 (of 2) scan.
tiating NSE at 15:17
pleted NSE at 15:17 to 76s elapsed
: Starting runlevel 2 (of 2) scan.
tiating NSE at 15:17
pleted NSE at 15:17 to 76s elapsed
: Starting runlevel 2 (of 2) scan.
tiating NSE at 15:17
pleted NSE at 15:17 to 76s elapsed

Shown: 996 filtered tcp ports (no-response)

The starting runlevel 2 (of 2) scan.

To poen ssh syn-ack (0.092s latency).
The open ssh syn-ack (0.092s latency).
The o
```

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

```
meta9@parrot
 sgobuster 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)
                                                                                                             http://172.30.150.38
               Method:
                                                                                                             GET
                Threads:
                                                                                                              50
              Wordlist:
                                                                                                              /usr/share/wordlists/dirbuster/directory-list-lowercase-2.3-small.t
              Negative Status codes:
User Agent:
                                                                                                             404
                                                                                                              aobuster/3.1.0
             Extensions:
Timeout:
                                                                                                               html,
                                                                                                              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 "h
ttp://172_30.150.38/images": context deadline exceeded (Client.Timeout exceeded while awaiting h
Progress: 3447 / 244932 (1.43%)
 Progress: 3447 / 244932 (1.41%) [ERROR] 2022/12/01 15:40:38 [!] Get "h
ttp://172.30.150.38/image": context deadline exceeded (Client.Timeout exceeded while awaiting he
aders)
/logout
/logou
 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 heade
 rs;
Progress: 11118 / 244932 (4.54%) [ERROR] 2022/12/01 15:41:10 [!] Get "h
ttp://172.30.150.38/ls": context deadline exceeded (Client.Timeout exceeded while awaiting heade
 /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 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)

(tomy{a98b5ce98ad49e5dba91a17652f49f4f}