

# Solution challenge 1 : Easy Peasy

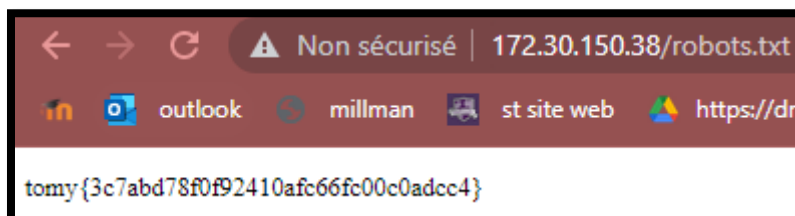
## 1. Le premier flag :

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.

```
packets transmitted, 4 received, 0% packet loss, time 3003ms
min/avg/max/mdev = 55.063/69.439/94.996/15.319 ms
meta9@parrot:~/Downloads/groupe2$
$ nmap -sV -vv 172.30.150.38
Starting Nmap 7.92 ( https://nmap.org ) at 2022-12-01 15:16 CET
: Loaded 45 scripts for scanning.
Initiating Ping Scan at 15:16
Scanning 172.30.150.38 [2 ports]
Completed Ping Scan at 15:16, 0.06s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 15:16
Completed Parallel DNS resolution of 1 host. at 15:16, 0.07s elapsed
Initiating Connect Scan at 15:16
Scanning 172.30.150.38 [1000 ports]
Completed open port 80/tcp on 172.30.150.38
Completed open port 22/tcp on 172.30.150.38
Completed Connect Scan at 15:17, 8.53s elapsed (1000 total ports)
Initiating Service scan at 15:17
Scanning 2 services on 172.30.150.38
Completed 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.
Initiating NSE at 15:17
Completed NSE at 15:17, 0.76s elapsed
: Starting runlevel 2 (of 2) scan.
Initiating NSE at 15:17
Completed NSE at 15:17, 1.07s elapsed
TCP scan report for 172.30.150.38
Host is up, received syn-ack (0.092s latency).
Scanned at 2022-12-01 15:16:51 CET for 17s
Shown: 996 filtered tcp ports (no-response)
T STATE SERVICE REASON VERSION
tcp open ssh syn-ack OpenSSH 7.9p1 Debian 10+deb10u2 (protocol 2.0)
tcp open http syn-ack Apache httpd 2.4.38 ((Debian))
80/tcp closed http-alt conn-refused
80/tcp closed http-proxy conn-refused
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Read data files from: /usr/bin/./share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 17.53 seconds
```

```
Terminal
File Edit View Search Terminal Tabs Help
Terminal x Terminal x Terminal x Terminal x Terminal x
[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]
```



## 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 cherchez le flag dans fichier.txt

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

## 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



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

