[Énumération/Réseau] Zmap

Introduction

Zmap est un outil qui permet de scanner très rapidement toute ou une partie de plage IPv4 d'Internet pour savoir lesquelles ont un ou plusieurs ports ouverts.

Installation

```
sudo apt update && sudo apt install -y zmap
```

Manuel

Syntaxe globale

```
sudo zmap -p <PORT> -o <FILE> <TARGET_IP>
```

Exemples d'utilisation

- Scanner tout internet sur le port 80 :

```
sudo zmap -p 80 -o scan_port_80_results.txt 0.0.0.0/0
```

- Balayer une plage d'IP sur plusieurs ports :

```
sudo zmap -p 22,80,443 -o scan_result.json 192.168.1.0/24
```

- Limiter l'utilisation de la bande passante :

```
sudo zmap -p 3389 -o rdp_results.csv -B 5M 10.0.0.0/16
```

Options courantes

Options	Descriptions
-p <PORT>	Spécifie le numéro de port à balayer.
-o <FILE>	Spécifie le fichier de sortie pour enregistrer les résultats.
-B <BYTES>	Limite la bande passante utilisée (par exemple, "-B 10M" pour limiter à 10 Mbps).
-f <FORMAT>	Spécifie le format de sortie (par exemple, **json** ou **csv**).
-q	Mode silencieux (supprime les avertissements)
-N	Définit le nombre de threads à utiliser pour le balayage.

Revision #2
Created 6 November 2023 15:29:00 by Elieroc
Updated 3 May 2024 14:37:31 by Elieroc