[Énumération/Web] Cheat-sheet

Introduction

Des outils permettent l'énumération de serveur web comme **Gobuster**, **Dirbuster**, **Nikto** ou **WFuzz**.

Gobuster

Files and directories

Voici comment utiliser gobuster pour trouver les **fichiers** et **répertoires** sur un serveur web :

```
gobuster dir -w <WORDLIST_PATH> -u <URL>
```

Subdomains

Voici comment utiliser gobuster pour trouver les **sous-domaines** sur un serveur web :

```
gobuster dns -w <WORDLIST_PATH> -u <URL>
```

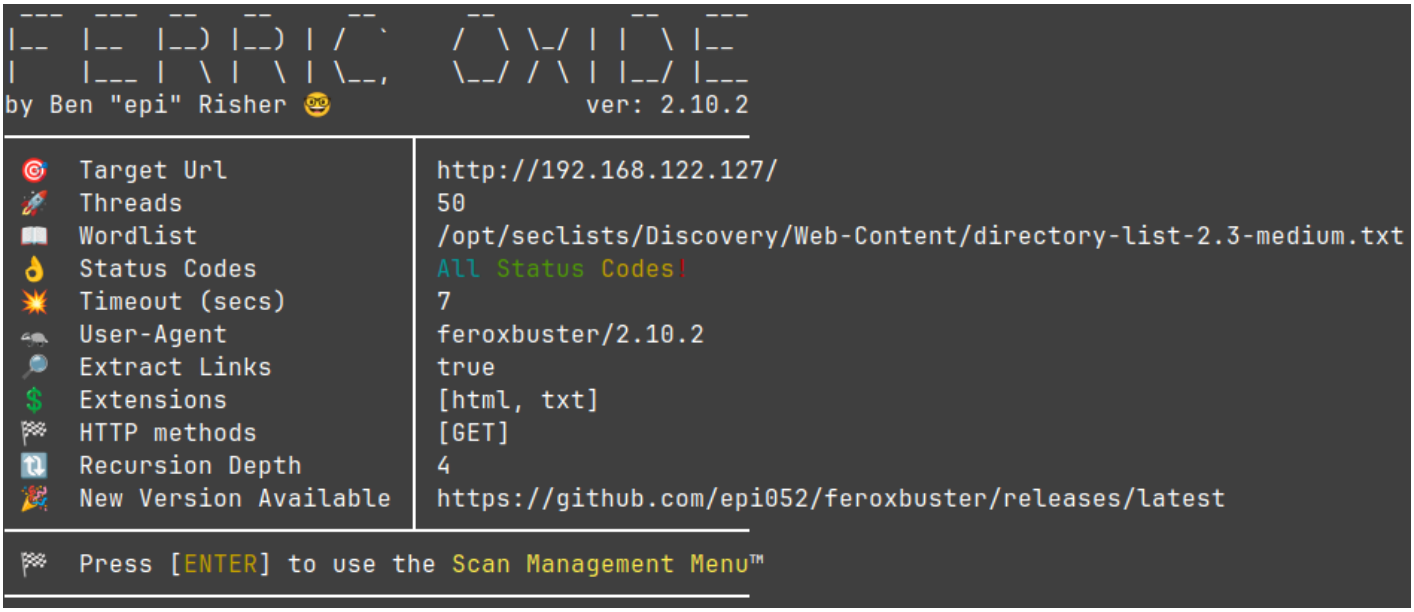
Fuzzing

Voici comment utiliser gobuster pour tester des **paramètres** sur un serveur web :

```
gobuster dns -w <WORDLIST_PATH> -u <URL/<PAGE>.php?PARAMETER=FUZZ>
```

Feroxbuster

- https://github.com/epi052/feroxbuster



L'outil se veut être un clone de gobuster en allant plus vite et avec une interface plus agréable.

Directories

```
feroxbuster -w <WORDLIST> --url <URL>
```

Files

```
feroxbuster -w <WORDLIST> --url <URL> -x <EXT1> [EXT2]
```

> Par exemple vous pouvez utiliser les options suivantes : **-x html php js txt** .

> La wordlist sélectionnée doit correspondre à ce que vous cherchez (fichiers/dossiers).

WFuzz

Voici comment faire du fuzzing :

```
wfuzz -c -z file,<WORDLIST> --hc 404 <URL>
```

Revision #7
Created 11 October 2023 15:15:25 by Elieroc
Updated 28 June 2024 08:17:41 by Elieroc