

Manuel d'Utilisation de Gobuster

Table des Matières

1. Introduction
2. Installation
3. Modes de Fonctionnement
4. Utilisation de base
5. Options Avancées
6. Exemples d'Utilisation
7. Résolution des Problèmes
8. Références

Introduction

Gobuster est un outil en ligne de commande conçu pour la découverte de contenu sur des serveurs web. Il est principalement utilisé pour le brute-forcing de répertoires et de fichiers sur des serveurs web ainsi que pour la découverte de sous-domaines. Il est rapide et efficace, grâce à son utilisation de Go.

Installation

Prérequis

- **Go** : Gobuster est écrit en Go, vous devez donc installer Go avant d'installer Gobuster.

Étapes d'Installation

1. Installez Go en suivant les instructions de téléchargement officiel.
2. Clonez le dépôt Gobuster depuis GitHub :

```
git clone https://github.com/OJ/gobuster.git
```

3. Naviguez dans le répertoire Gobuster :

```
cd gobuster
```

4. Construisez Gobuster avec Go :

```
go build
```

5. Gobuster est maintenant prêt à être utilisé. Vous pouvez le vérifier en exécutant :

```
./gobuster -h
```

Modes de Fonctionnement

Gobuster propose plusieurs modes de fonctionnement principaux :

1. **Mode répertoire (dir)** : Pour découvrir des répertoires et des fichiers.
2. **Mode DNS (dns)** : Pour découvrir des sous-domaines.
3. **Mode Virtual Host (vhost)** : Pour découvrir des hôtes virtuels.

Utilisation de Base

Brute-forcing de Répertoires et de Fichiers

Pour lancer un brute-forcing de répertoires et de fichiers sur un site web :

```
./gobuster dir -u http://example.com -w /chemin/vers/votre/dictionnaire.txt
```

Options courantes :

- `-u` : URL de la cible.
- `-w` : Chemin vers le fichier de dictionnaire.

Brute-forcing de Sous-domaines

Pour découvrir des sous-domaines :

```
./gobuster dns -d example.com -w /chemin/vers/votre/dictionnaire.txt
```

Options courantes :

- `-d` : Domaine cible.
- `-w` : Chemin vers le fichier de dictionnaire.

Brute-forcing d'Hôtes Virtuels

Pour découvrir des hôtes virtuels :

```
./gobuster vhost -u http://example.com -w /chemin/vers/votre/dictionnaire.txt
```

Options courantes :

- `-u` : URL de la cible.
- `-w` : Chemin vers le fichier de dictionnaire.

Options Avancées

Gobuster propose plusieurs options avancées pour affiner vos recherches :

- `-t` : Nombre de threads à utiliser.
- `-e` : Afficher toutes les extensions.
- `-x` : Spécifier des extensions de fichiers à rechercher.
- `-k` : Ignorer les erreurs de certificat SSL.
- `-o` : Enregistrer la sortie dans un fichier.

Par exemple, pour lancer une recherche avec 50 threads et enregistrer la sortie :

```
./gobuster dir -u http://example.com -w /chemin/vers/votre/dictionnaire.txt -t 50 -o sortie.txt
```

Exemples d'Utilisation

Découverte de Répertoires avec des Extensions

```
./gobuster dir -u http://example.com -w /chemin/vers/votre/dictionnaire.txt -x php,html,txt
```

Recherche avec Ignorance des Erreurs SSL

```
./gobuster dir -u https://example.com -w /chemin/vers/votre/dictionnaire.txt -k
```

Recherche de Sous-domaines avec enregistrement de la sortie

```
./gobuster dns -d example.com -w /chemin/vers/votre/dictionnaire.txt -o sous-domaines.txt
```

Résolution des Problèmes

Problème : Gobuster ne trouve aucun résultat

- Vérifiez que l'URL cible est correcte.
- Assurez-vous que le dictionnaire utilisé contient des mots valides.
- Essayez d'augmenter le nombre de threads pour améliorer la vitesse de recherche.

Problème : Gobuster plante ou se ferme de manière inattendue

- Vérifiez les permissions et assurez-vous que Gobuster peut accéder au fichier de dictionnaire et à la cible.
- Assurez-vous que votre système dispose de suffisamment de ressources (RAM, CPU) pour exécuter Gobuster avec le nombre de threads spécifié.

Références

- Dépôt GitHub de Gobuster
- Documentation de Go : <https://golang.org/doc/>

Ce manuel devrait vous aider à utiliser Gobuster efficacement pour la découverte de contenu web. Pour plus de détails, référez-vous à la documentation officielle et aux ressources communautaires.