dirb

Qu’est-ce que DIRB ?

DIRB est un outil open source utilisé pour **scanner un site web à la recherche de répertoires et fichiers cachés**. Il fonctionne par **brute force** en envoyant des requêtes HTTP basées sur des listes de mots (wordlists).

Cas d’usage

- Pentesting (phase de reconnaissance)
- Audit de sécurité web
- Découverte de pages d’administration ou fichiers sensibles

Installation

Sous Linux (Debian/Ubuntu) :

```
sudo apt-get install dirb
```

Sous Kali Linux, il est généralement préinstallé.

Syntaxe de base

```
dirb <URL> [wordlist] [options]
```

- URL : site cible (ex. http://example.com)
- wordlist : fichier contenant les mots à tester (ex. /usr/share/dirb/wordlists/common.txt)
- options : paramètres supplémentaires (proxy, authentification, etc.)

Exemples simples

- Scan avec la wordlist par défaut :

```
dirb http://example.com
```

- Scan avec une wordlist spécifique :

```
dirb http://example.com /usr/share/dirb/wordlists/big.txt
```

Options principales

Option	Description
-a <agent>	Définit un User-Agent personnalisé
-p <proxy>	Utilise un proxy (ex. -p http://127.0.0.1:8080)
-u <user:pass>	Authentification HTTP Basic
-r	Ignore les redirections
-x <ext>	Ajoute des extensions (ex. -x .php,.html)

- Utiliser un proxy :

```
dirb http://example.com /usr/share/dirb/wordlists/common.txt -p http://127.0.0.1:8080
```

- Authentification HTTP :

```
dirb http://example.com /usr/share/dirb/wordlists/common.txt -u admin:password
```

Wordlists utiles

- Par défaut : /usr/share/dirb/wordlists/common.txt
- Autres sources :
    - https://github.com/danielmiessler/SecLists
    - OWASP DirBuster lists

Bonnes pratiques

- Limiter la charge : éviter de saturer le serveur (utiliser des délais si nécessaire).
- Filtrer les codes : ignorer les 404 pour réduire le bruit.
- Utiliser HTTPS : si le site est sécurisé.
- Compléter avec d'autres outils : Gobuster (plus rapide, multi-thread), WFuzz (plus flexible).

Comparaison rapide

Outil	Avantage
DIRB	Simple, efficace, inclus dans Kali
Gobuster	Plus rapide (Go, multi-thread)
WFuzz	Très flexible (fuzzing avancé)

OptionDescription-a <agent>Définit un User-Agent personnalisé-p <proxy>Utilise un proxy (ex. -p http://127.0.0.1:8080)-u <user:pass>Authentification HTTP Basic-rIgnore les redirections-x <ext>Ajoute des extensions (ex. -x .php,.html)-N <code>Ignore un code HTTP (ex. -N 404)-SMode silencieux (moins de sortie)-o <file>Sauvegarde le résultat dans un fichier

 6. Exemples avancés Ajouter des extensions : Shelldirb http://example.com /usr/share/dirb/wordlists/common.txt -x .php,.html,.bakAfficher plus de lignes Utiliser un proxy : Shelldirb http://example.com /usr/share/dirb/wordlists/common.txt -p http://127.0.0.1:8080Afficher plus de lignes Authentification HTTP : Shelldirb http://example.com /usr/share/dirb/wordlists/common.txt -u admin:passwordAfficher plus de lignes

 7. Wordlists utiles

Par défaut : /usr/share/dirb/wordlists/common.txt Autres sources :

https://github.com/danielmiessler/SecLists OWASP DirBuster lists

 8. Bonnes pratiques

Limiter la charge : éviter de saturer le serveur (utiliser des délais si nécessaire). Filtrer les codes : ignorer les 404 pour réduire le bruit. Utiliser HTTPS : si le site est sécurisé. Compléter avec d'autres outils : Gobuster (plus rapide, multi-thread), WFuzz (plus flexible).

 9. Comparaison rapide

OutilAvantageDIRBSimple, efficace, inclus dans KaliGobusterPlus rapide (Go, multi-thread)WFuzzTrès flexible (fuzzing avancé)

Veux-tu que je prépare un tableau récapitulatif des options avec exemples concrets, ou un script Bash automatisé pour lancer plusieurs scans avec DIRB ? Ou encore une comparaison détaillée avec Gobuster et WFuzz ? Fournissez vos commentaires sur BizChat