BruteForce

- SSH2JOHN & John The Ripper - BruteForce de clé privée RSA
- DirBuster - Bruteforce web/applications

SSH2JOHN & John The Ripper - BruteForce de clé privée RSA

Introduction

SSH2JOHN est un outils qui permet de transformer une clé RSA dans un format utilisable par John The Ripper.

L'outil est retrouvable sur github, également disponible sur Kali Linux.

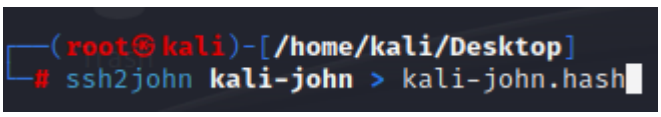
> La présentation de cette outil est purement dans un but d'apprentissage.

Utilisation

Dans un premier temps vous devez disposer d'une clé RSA chiffré par une passphrase. Dans l'exemple ci-dessous nous avons crée la clé RSA **kali-john**.

Dès lors que vous avez récupéré la clé, il faut exectuté la commande ci-dessous pour récupéré le hash que nous allons ensuite déchiffrer avec John The Ripper.

```
ssh2john [id_rsa] > [id_rsa.hash]
```



Une fois le fichier hashé récupéré, nous pouvons lancé le brute force avec la wordlist rockyou.txt.

```
john --wordlist=/usr/share/wordlists/rockyou.txt id_rsa.hash
```

```
┌──(root㉿kali)-[/home/kali/Desktop]
└─# john --wordlist=/usr/share/wordlists/rockyou.txt kali-john.hash
Using default input encoding: UTF-8
Loaded 1 password hash (SSH, SSH private key [RSA/DSA/EC/OPENSSH 32/64])
Cost 1 (KDF/cipher [0=MD5/AES 1=MD5/3DES 2=Bcrypt/AES]) is 2 for all loaded hashes
Cost 2 (iteration count) is 16 for all loaded hashes
Will run 8 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
```

Ensuite il suffit d'attendre pour obtenir un résultat. Si le résultat est positif vous allez obtenir ceci :

```
┌──(root㉿kali)-[/home/kali/Desktop]
└─# john --wordlist=/usr/share/wordlists/rockyou.txt kali-john.hash
Using default input encoding: UTF-8
Loaded 1 password hash (SSH, SSH private key [RSA/DSA/EC/OPENSSH 32/64])
Cost 1 (KDF/cipher [0=MD5/AES 1=MD5/3DES 2=Bcrypt/AES]) is 2 for all loaded hashes
Cost 2 (iteration count) is 16 for all loaded hashes
Will run 8 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
medical          (kali-john)
1g 0:00:01:22 DONE (2024-02-08 14:26) 0.01209g/s 104.4p/s 104.4c/s 104.4C/s kalani..brigitte
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

Nous pouvons donc voir que la passphrase lier à la clé RSA est **medical**.

Si le résultat est négatif vous pouvez essayer une autre wordlist.

DirBuster - Bruteforce web/applications

Introduction

DirBuster est une application Java multithread conçue pour forcer les noms de répertoires et de fichiers sur les serveurs web/applications.

L'outil est retrouvable sur gitlab, également disponible sur Kali Linux.

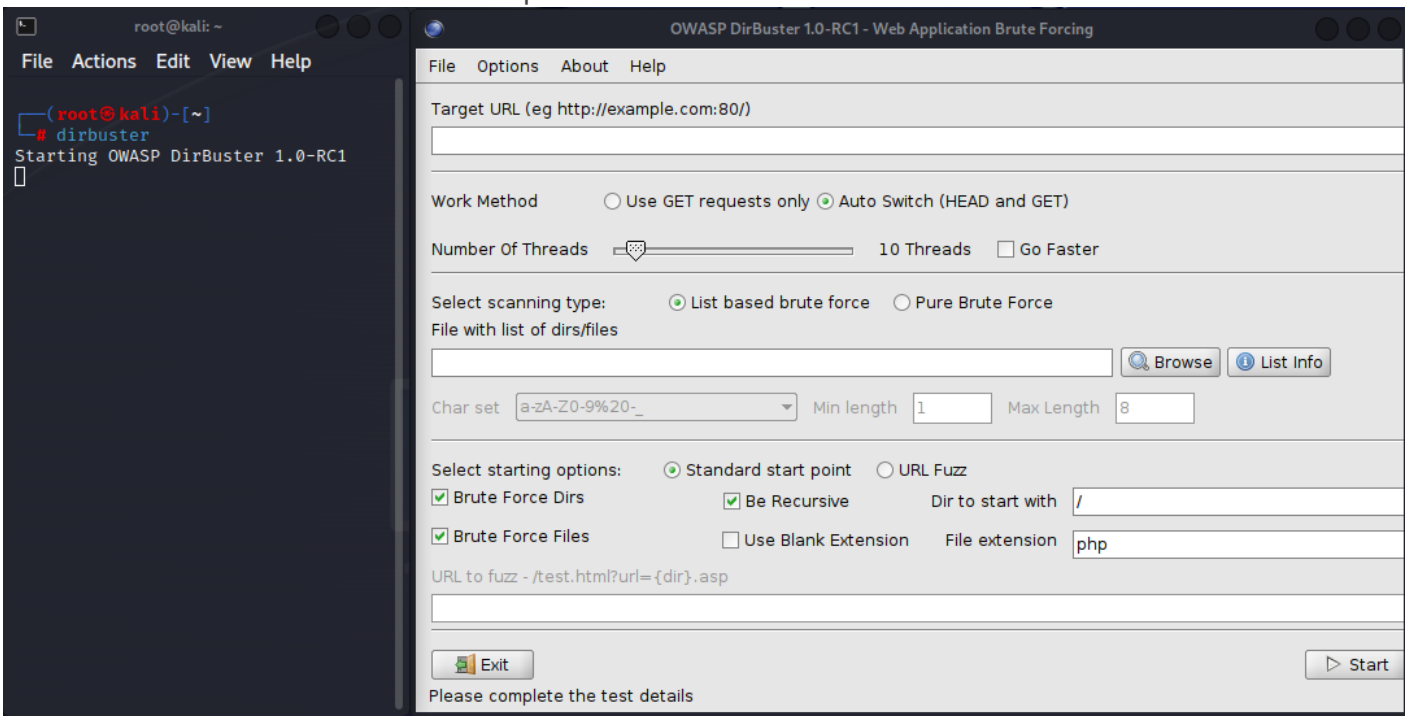
Cet outil est conçu pour aider à identifier les répertoires et fichiers cachés ou non référencés sur les serveurs web. Il fonctionne en lançant une attaque de bruteforce, utilisant des listes de mots (wordlists) pour deviner les noms de répertoires et de fichiers qui ne sont pas directement liés ou visibles depuis la page principale d'un site web. L'objectif est de découvrir des ressources cachées qui pourraient révéler des vulnérabilités ou des informations sensibles.

> La présentation de cette outil est purement dans un but d'apprentissage.

Disclaimer
L'utilisation de DirBuster peut générer un volume élevé de trafic sur le réseau cible et peut être détectée comme une attaque par les systèmes de surveillance ou de protection des applications web. Il est crucial de n'utiliser cet outil que dans un cadre légal, idéalement sur des systèmes dont vous avez l'autorisation explicite de tester, pour éviter toute implication légale ou éthique.

Utilisation

Pour commencer lancer DirBuster depuis un terminal.

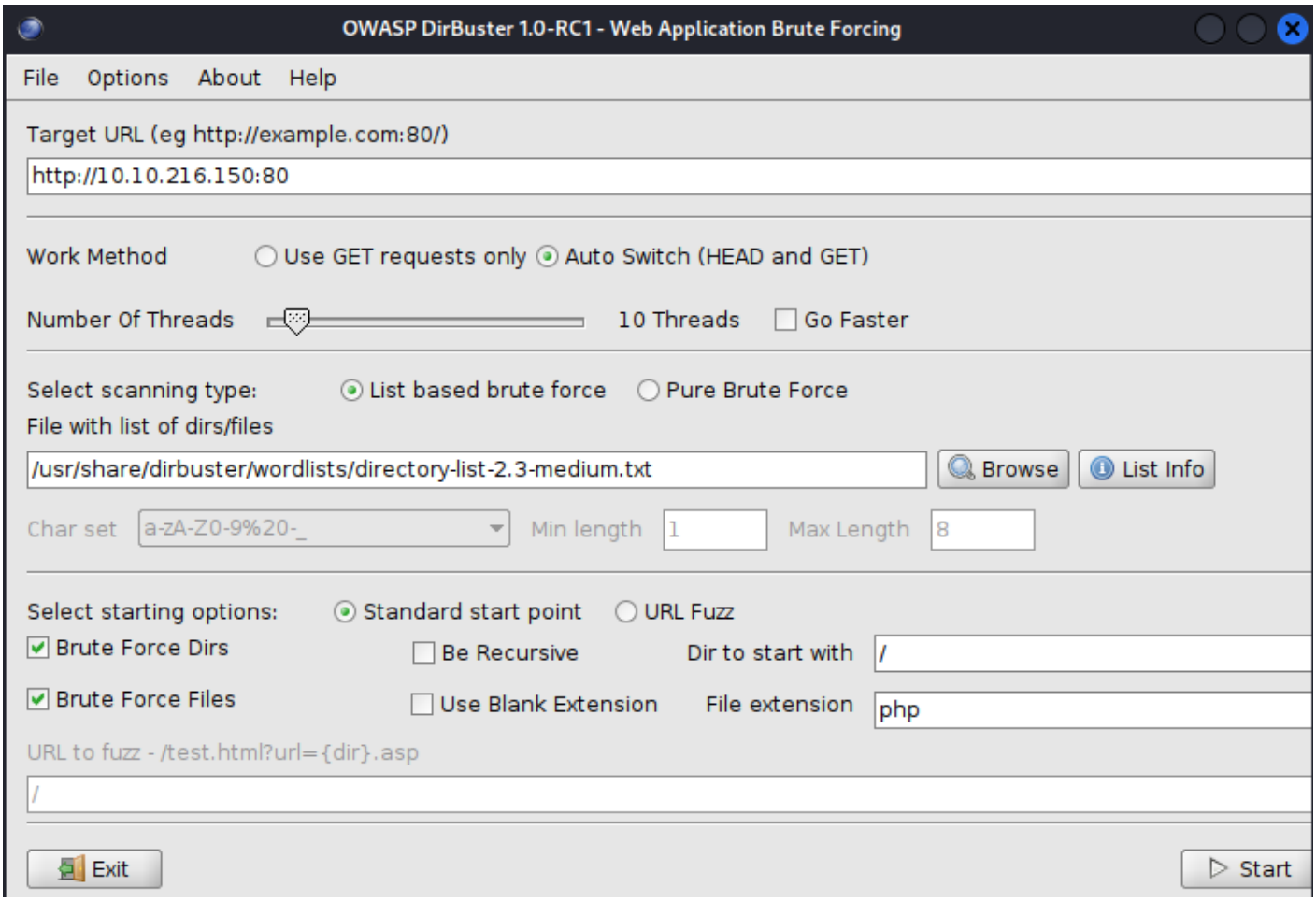


Dans la partie **Target URL** renseignez l'adresse du site et le port même si celui-ci est le port par défaut.
Dans la partie **Number of Threads** vous pouvez réglé le nombre de threads qui seront utilisé par le bruteforce.
Dans la partie **Select scanning type** vous pouvez choisir la méthode par **attaque de wordlist** ou **pure bruteforce**.

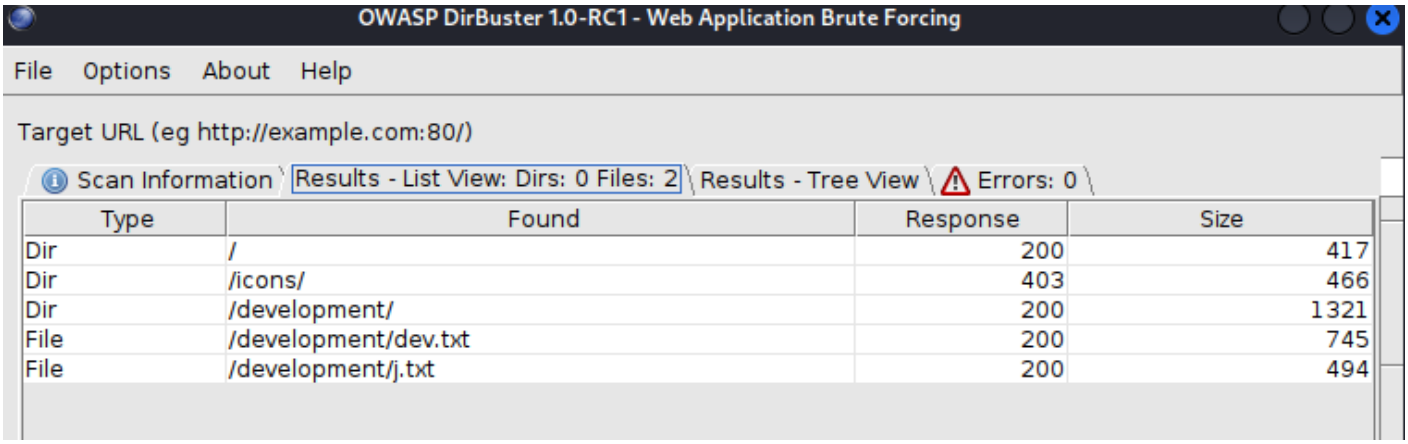
Passons aux options :

Option	Description
Brute Force Dirs	Cela recherchera les dossiers non repertoriés
Brute Force Files	Cela recherchera les fichiers non repertoriés
Be recursive	La récursivité, attention cela peut créer des boucles
Use Blank Extension	n/a
Dir to start with	Ou la recherche va commencer
File extension	Les fichiers utilisant les extensions seront récupérés

Exemple


OWASP DirBuster 1.0-RC1 - Web Application Brute Forcing
File Options About Help
Target URL (eg http://example.com:80/)
http://10.10.216.150:80
Work Method
Use GET requests only
Auto Switch (HEAD and GET)
Number Of Threads
10 Threads
Go Faster
Select scanning type:
List based brute force
Pure Brute Force
File with list of dirs/files
/usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt
Browse
List Info
Char set
a-zA-Z0-9%20-_
Min length
1
Max Length
8
Select starting options:
Standard start point
URL Fuzz
Brute Force Dirs
Be Recursive
Dir to start with
/
Brute Force Files
Use Blank Extension
File extension
php
URL to fuzz - /test.html?url={dir}.asp
/
Exit
Start

Résultat


OWASP DirBuster 1.0-RC1 - Web Application Brute Forcing
File Options About Help
Target URL (eg http://example.com:80/)
Scan Information
Results - List View: Dirs: 0 Files: 2
Results - Tree View
Errors: 0
Type
Found
Response
Size
Dir / 200 417
Dir /icons/ 403 466
Dir /development/ 200 1321
File /development/dev.txt 200 745
File /development/j.txt 200 494