BlackPyReconX - Manuel d'Utilisation

1. Introduction

BlackPyReconX est un framework de sécurité offensif modulaire conçu pour assister les professionnels de la sécurité et les chercheurs dans les différentes phases d'un test d'intrusion. Il intègre des outils de reconnaissance, de scan, d'exploitation et de reporting au sein de trois interfaces distinctes : une interface web, un bot Telegram interactif et une interface en ligne de commande (CLI) puissante.

Ce document détaille l'installation, la configuration et l'utilisation de chacune de ces interfaces.

2. Installation et Lancement

2.1. Prérequis

- Python 3.10 ou supérieur

- Git

2.2. Installation

1. **Clonez le dépôt :**

   ```bash

   git clone <URL_DU_PROJET> BlackPyReconX
   ```

cd BlackPyReconX

```

2. **Installez les dépendances :**

Créez un environnement virtuel (recommandé) puis installez les paquets nécessaires.

```bash

python -m venv venv

# Sur Windows:

venv\Scripts\activate

# Sur macOS/Linux:

# source venv/bin/activate

pip install -r requirements.txt

```

3. **Configuration des clés API :**

Copiez `.env.example` vers `.env` et remplissez les clés API pour Shodan, AbuseIPDB et Telegram.

2.3. Lancement du Framework

Pour démarrer l'interface web et le bot Telegram, exécutez le script principal :

```
python start_all.py
```

- L'interface web sera accessible à l'adresse `http://127.0.0.1:5000`.
```

- Le bot Telegram sera automatiquement mis en ligne.

3. L'Interface Web

L'interface web fournit un tableau de bord complet pour contrôler le framework. En haut de la page, des **voyants de statut** vous informent en temps réel de l'état de TOR et du bot Telegram (Vert = actif, Rouge = inactif).

3.1. Panneau de Contrôle Principal

- **Cible** : Entrez l'IP, le domaine ou l'URL à analyser.
- **Modules de Scan** : Cochez les modules à exécuter (OSINT, Scan Réseau, Analyse Web) et cliquez sur "Lancer les Scans".
- **Génération de Rapport** : Crée le rapport final à partir des résultats des scans.
- **Exfiltration** : Compresse et chiffre les données du dossier `outputs`.
- **Basculer TOR** : Active ou désactive l'utilisation du réseau TOR pour les modules qui le supportent.
- **Bot Telegram** : Ouvre un lien vers votre bot dans un nouvel onglet.

3.2. Attaque DoS

- **Port Cible** : Choisissez un port commun dans la liste déroulante.
- **Durée** : Spécifiez la durée de l'attaque en secondes.

3.3. Attaque par Brute-Force

Ce module propose deux modes d'attaque :

1. **Attaque par Dictionnaire** (par défaut) :
   - **Service** : Sélectionnez le service à attaquer (SSH, FTP, etc.).
   - **Listes de fichiers** : Spécifiez les chemins vers vos listes d'utilisateurs et de mots de passe.

Vous pouvez utiliser les listes par défaut ou **téléverser vos propres fichiers `.txt`** grâce au bouton "Téléverser".

2. **Attaque par Force Brute Pure** :
   - **Nom d'utilisateur** : Le login unique à tester.
   - **Jeu de caractères** : Le type de caractères à utiliser pour générer les mots de passe (ex: alphanumérique, numérique, etc.).
   - **Longueur Min/Max** : La plage de longueur pour les mots de passe à générer.

4. Le Bot Telegram

Le bot offre un contrôle à distance du framework.

1. **Démarrez la conversation** : Envoyez `/start` à votre bot.
2. **Choisissez un module** : Utilisez les boutons du menu principal (OSINT, Scan, etc.).
3. **Spécifiez la cible** : Envoyez l'IP ou le domaine en message.
4. **Confirmez** : Validez le lancement de l'analyse.

Le bot vous enverra les résultats sous forme de messages et de fichiers directement dans la conversation.

5. L'Interface en Ligne de Commande (CLI)

Le CLI (`main.py`) est l'outil le plus puissant et le plus flexible pour l'automatisation.

5.1. Syntaxe de Base

```
python main.py --target <cible> [options_module...]
```

5.2. Arguments Généraux

- `--target <IP/Domaine>` : (Obligatoire pour la plupart des modules) La cible de l'analyse.
- `--tor` : Active le routage via TOR pour la session en cours.

5.3. Modules de Scan

- `--osint` : Lance la reconnaissance OSINT.
- `--scan` : Lance le scan de ports et services.
- `--web` : Lance l'analyse de vulnérabilités web.
- `--exploit` : Tente une exploitation système (nécessite une configuration préalable).
- `--report` : Génère manuellement le rapport final.

5.4. Module d'Attaque DoS

- `--dos` : Active le module DoS.

- `--port <numéro>` : (Obligatoire) Le port à attaquer.
- `--duration <secondes>` : Durée de l'attaque (défaut: 60).

Exemple :

```
python main.py --target 1.1.1.1 --dos --port 80 --duration 120
```

5.5. Module d'Attaque par Brute-Force

Le module `--bruteforce` s'utilise avec l'un des deux modes suivants.

- `--service <nom>` : (Obligatoire) Spécifie le service (ssh, ftp, web, etc.).
- `--port <numéro>` : (Obligatoire) Le port du service.

Mode 1 : Attaque par Dictionnaire (par défaut)

Utilise des listes de mots.

- `--attack-type dictionary` (Optionnel, car c'est le défaut).
- `--userlist <chemin>` : Chemin vers la liste d'utilisateurs (défaut: `data/usernames.txt`).
- `--passlist <chemin>` : Chemin vers la liste de mots de passe (défaut: `data/passwords.txt`).

Exemple :

```
python main.py --target 192.168.1.22 --bruteforce --service ssh --port 22 --userlist
custom_users.txt
```

Mode 2 : Force Brute Pure

Génère toutes les combinaisons possibles.

- `--attack-type bruteforce` : **(Obligatoire pour activer ce mode)**.
- `--username <nom>` : (Obligatoire) Le nom d'utilisateur unique à tester.
- `--charset <set>` : Jeu de caractères (`alphanum`, `digits`, ou personnalisé `abc123`) (défaut: `alphanum`).
- `--min-len <num>` : Longueur minimale du mot de passe (défaut: 4).
- `--max-len <num>` : Longueur maximale du mot de passe (défaut: 6).

Exemple :

```
python main.py --target 192.168.1.22 --bruteforce --attack-type bruteforce --service ssh
--port 22 --username root --min-len 5 --max-len 5 --charset digits
```

6. Avertissement Éthique

Cet outil est conçu à des fins éducatives et pour les professionnels de la sécurité dans le cadre de tests d'intrusion autorisés. L'utilisation de cet outil sur des systèmes ou des réseaux sans autorisation explicite est illégale. Les auteurs ne sont pas responsables de toute utilisation malveillante.