Guide Utilisateur - Toolbox de Cybersécurité

Introduction

La Toolbox de Cybersécurité est une plateforme web complète qui regroupe des outils de test de pénétration et d'analyse de sécurité populaires. Elle offre une interface centralisée pour faciliter l'utilisation de ces outils.

Fonctionnalités

- Interface Unifiée : Tous les outils sont accessibles depuis une même interface web.
- Authentification Sécurisée : Gestion des utilisateurs via Keycloak.
- Architecture Microservices : Chaque outil fonctionne dans un conteneur indépendant.
- Sauvegarde et Restauration : Enregistrement et récupération des configurations et des résultats.
- Système de Logs : Journalisation complète pour l'audit et la résolution des problèmes.

Outils Intégrés

- Metasploit Web Interface
- Nmap Scanner
- OWASP ZAP
- WPScan
- Gobuster
- TCPdump Analyzer
- SQLmap
- Hydra
- Nikto
- John the Ripper
- TheHarvester
- Subfinder

Guide Utilisateur - Toolbox de Cybersécurité

- Auto-Sécurité

- Analyseur de Trafic Réseau

Prérequis

- OS Linux (Kali recommandé)

- Python 3.13+

- Docker et Docker Compose

- Poetry (gestionnaire de dépendances)

Installation

1. Cloner le dépôt :

--- Commandes ---

git clone https://github.com/Amineb-sio/Toolbox.git

cd Toolbox

--- Fin des commandes ---

2. Installer Poetry :

--- Commandes ---

curl -sSL https://install.python-poetry.org | python3 -

--- Fin des commandes ---

3. Installer les dépendances :

--- Commandes ---

poetry install

--- Fin des commandes ---

4. Installer Docker et Docker Compose :

--- Commandes ---

sudo apt-get update && sudo apt-get install -y docker.io

sudo apt install docker-compose

--- Fin des commandes ---

5. Lancer les services Docker :

--- Commandes ---

docker-compose up -d

--- Fin des commandes ---

6. Configurer OWASP ZAP :

--- Commandes ---

cd /usr/share

sudo git clone https://github.com/ParrotSec/zaproxy

sudo /usr/share/zaproxy/zap.sh -daemon -port 8090 -config api.key=monapikey

--- Fin des commandes ---

7. Lancer la Toolbox :

--- Commandes ---

poetry run bash ./start_all.sh

--- Fin des commandes ---

Accessible sur : http://127.0.0.1:5000

Analyseur de Trafic Réseau

1. Démarrer l'analyseur :

--- Commandes ---

poetry run bash ./start_network_analyzer.sh

--- Fin des commandes ---

Guide Utilisateur - Toolbox de Cybersécurité

2. Interface accessible via : http://127.0.0.1:5022

Fonctionnalités :

- Analyse de fichiers PCAP
- Capture réseau en temps réel
- Détection d'anomalies
- Rapports en JSON, CSV, HTML
- Interface web intuitive

Authentification et Services

- Keycloak pour la gestion des comptes : http://localhost:8080
- Portainer (port 9000)
- PostgreSQL (port 5432)
- pgAdmin (port 5050)

Maintenance & Dépannage

- Mettre à jour les dépendances : poetry update
- Redémarrer les services :

```
--- Commandes ---
  docker-compose down
  docker-compose up -d
  poetry run bash ./start_all.sh
--- Fin des commandes ---
```

- Logs disponibles dans : ./logs

- Sauvegardes : ./backups

- Clés : ./secure_keys

Navigateurs Recommandés

- Google Chrome (recommandé)

- Firefox

- Edge

Développeurs

- Amine Boukherouba

- Stéphane YE

- Jeremy Corinthe