Aperçu général

Ce script Python analyse le trafic réseau capturé dans des fichiers .txt générés par des outils comme tcpdump. Il détecte les anomalies, génère des rapports statistiques et visualise la distribution des protocoles à travers des graphiques. Les résultats sont présentés dans des formats HTML et CSV pour une analyse détaillée.

Prérequis

1. Bibliothèques Python: Assurez-vous d'avoir installé les bibliothèques Python suivantes:

- pandas
- re
- datetime
- matplotlib
- base64
- io
- webbrowser
- os
- collections
- csv

Installez les bibliothèques manquantes avec: `pip install <nom-bibliothèque>`.

2. Fichier d'entrée: Le fichier d'entrée doit être un fichier .txt contenant des journaux de trafic réseau (ex: capturés via tcpdump).

Fonctionnalités du Script

1. Analyse du Trafic Réseau (analyze_tcpdump)

- Entrée: Chemin du fichier .txt.
- Sortie:

- Résumé statistique de l'activité réseau.

- Anomalies identifiées dans le trafic.

- Fonctionnalités clés:

- Détecte les paquets suspects (ex: drapeaux TCP comme [S], [SF]).

- Analyse les adresses IP, protocoles et informations des paquets.

- Calcule les pics de trafic et signale les IP avec comportement anormal.

2. Visualisation de la Distribution des Protocoles (generate_protocol_chart)

- Crée un graphique circulaire des 10 protocoles les plus utilisés.

- Encode le graphique en image Base64 pour l'intégration HTML.

3. Génération de Rapports:

- Rapport CSV (generate_csv_report):

- Résume les statistiques réseau, anomalies et distribution des protocoles dans un fichier .csv.

- Rapport HTML (generate_html_report):

- Fournit un rapport HTML détaillé et stylisé, comprenant:

- Un aperçu des statistiques réseau.

- Un graphique circulaire de la distribution des protocoles.

- Un tableau des anomalies détectées.

4. Visualisation HTML Interactive

- Ouvre automatiquement le rapport HTML généré dans le navigateur web par défaut.

Comment Utiliser

Étape 1: Préparer le Fichier d'Entrée

- Assurez-vous que le fichier .txt contenant les journaux de trafic réseau est dans le même répertoire que le script ou fournissez son chemin complet.

Étape 2: Exécuter le Script

- Exécutez le script en utilisant:

```
python projet_final.py
```

Étape 3: Consulter les Rapports

- Le script va:

  - Analyser le fichier d'entrée.

  - Générer un rapport CSV (rapport_analyse.csv).

  - Ouvrir automatiquement le rapport HTML (rapport_projet_final.html) dans votre navigateur.

Configuration

Fichier d'Entrée par Défaut

- Le script utilise fichier182.txt comme fichier d'entrée par défaut. Pour analyser un fichier différent:

  1. Remplacez `file_path = 'fichier182.txt'` dans la fonction main() avec le chemin de votre fichier.

  2. Sauvegardez les modifications et réexécutez le script.

Fichiers de Sortie

- CSV: rapport_analyse.csv

- HTML: rapport_projet_final.html

Gestion des Erreurs

Si le script rencontre des problèmes (ex: fichier non trouvé, entrée mal formée), il affichera un message d'erreur et se terminera.

Personnalisation

Vous pouvez adapter le script pour:

- Utiliser d'autres sources de données.

- Étendre les règles de détection d'anomalies en modifiant la fonction detect_anomalies.

- Ajuster les seuils pour les pics de trafic dans la fonction analyze_tcpdump.