פרויקט: מנתח לוגים של תעבורת רשת

שלב 5 - אינטגרציה: המערכת השלמה

מטרת השלב

בשלבים הקודמים בנינו את כל חלקי המערכת בנפרד. עכשיו נחבר הכל יחד למערכת שלמה שמקבלת קובץ לוג ומייצרת דוח חשודים.

דרישות שלב 5

1 מונה סטטיסטיקות גלובלי

הגדירו משתנים גלובליים לספירת סטטיסטיקות:

- סה"כ שורות שנקראו
- סה"כ שורות חשודות
- ספירה לכל סוג חשד

כתבו פונקציה שמעדכנת את המונים תוך כדי עיבוד (השתמשו ב-`global`).

2 פונקציית עיבוד ראשית

כתבו פונקציה `analyze_log(filepath)` שמחברת את כל השלבים:

- קריאת הקובץ עם generator
- בדיקת חשדות לכל שורה
- בניית מילון IP → רשימת חשדות

- עדכון הסטטיסטיקות

3 יצירת דוח סיכום

כתבו פונקציה `generate_report(suspicious_dict)` שמייצרת מחרוזת עם דוח מסודר:

דוגמה לפלט:

```
========================================
       דוח תעבורה חשודה
========================================

סטטיסטיקות כלליות:
- שורות שנקראו: 10,000
- שורות חשודות: 847
- EXTERNAL_IP: 523
- SENSITIVE_PORT: 312
- LARGE_PACKET: 198
- NIGHT_ACTIVITY: 156

IPs עם רמת סיכון גבוהה (3+ חשדות):
- 45.33.32.156: EXTERNAL_IP, SENSITIVE_PORT, LARGE_PACKET, NIGHT_ACTIVITY
- 87.120.5.22: EXTERNAL_IP, SENSITIVE_PORT, NIGHT_ACTIVITY

IPs חשודים נוספים:
- 203.0.113.50: EXTERNAL_IP, LARGE_PACKET
- 91.189.88.142: EXTERNAL_IP
...
```

4 כתיבה לקובץ פלט

כתבו פונקציה `save_report(report, filepath)` ששומרת את הדוח לקובץ טקסט.

5 פונקציית main

כתבו פונקציה `main()` שמפעילה את כל התהליך:

```python
def main():
    # קריאה וניתוח
    suspicious = analyze_log("network_traffic.log")

    # יצירת דוח
    report = generate_report(suspicious)

    # הדפסה למסך
    print(report)

    # שמירה לקובץ
    save_report(report, "security_report.txt")

if __name__ == "__main__":
    main()
```

הפלט הסופי של הפרויקט

בסיום השלב, המערכת שלכם תהיה מסוגלת:

- לקרוא קובץ לוג בכל גודל (בזכות generators)
- לזהות 4 סוגי חשדות שונים (מבנה דינאמי - קל להוסיף עוד)
- לייצר דוח מסודר עם סטטיסטיקות
- לשמור את הדוח לקובץ

זו מערכת אמיתית שיכולה לשמש בסיס לכלי ניטור אבטחה!

משימות בונוס

בונוס א': הוספת סוג חשד חמישי

הוסיפו את החשד `FREQUENT_ACCESS` - יותר מ-10 פניות מאותו IP.

בדקו כמה קל להוסיף אותו למערכת בזכות המבנה הדינאמי שבניתם.

בונוס ב': תצוגה גרפית של הדוח

הציגו את הדוח בצורה ויזואלית. בחרו אחת מהאפשרויות הבאות:

אפשרות 1: matplotlib - גרפים

הציגו את הסטטיסטיקות כגרפים:

- עוגה (pie chart) - התפלגות סוגי החשדות
- עמודות (bar chart) - 10 כתובות ה-IP עם הכי הרבה חשדות

```
import matplotlib.pyplot as plt

# התקנה: pip install matplotlib
```

אפשרות 2: tkinter - חלון גרפי

צרו חלון עם ממשק משתמש שמציג:

- טבלה של IPs חשודים
- כפתור לטעינת קובץ לוג
- כפתור לייצוא הדוח

```
import tkinter as tk
from tkinter import ttk

# מובנה בפייתון - לא צריך התקנה
```

אפשרות 3: Rich - טרמינל צבעוני

הציגו את הדוח בטרמינל עם צבעים וטבלאות מעוצבות:

- טבלה צבעונית של IPs
- צבעים שונים לרמות סיכון
- progress bar בזמן העיבוד

```
from rich.console import Console
from rich.table import Table

# התקנה: pip install rich
```

אפשרות 4: pygame - לוח בקרה

צרו "לוח בקרה" גרפי עם:

- מפת חום של פעילות לפי שעות
- אנימציה של נתונים זורמים
- התראות מהבהבות על חשדות ברמה גבוהה

```
import pygame

# התקנה: pip install pygame
```

טיפ: התחילו מהאפשרות שנראית לכם הכי פשוטה. אם יש זמן - נסו עוד אחת!