TCPDump Analysis Tool – User Manual

This tool analyzes network capture files (TCPDump) to detect potential security threats such as Buffer Overflows, SQL Injections, and XSS. It automatically generates reports in HTML, CSV, and Markdown formats. You need to have Python 3.8 or higher is required.

1. Prerequisites

Before running the script, ensure your environment is set up correctly:

- Python: You must have Python installed on your machine.
- Libraries: You need to install the markdown library. Open your terminal or command prompt and run one of the following commands:
    - pip install markdown
    - Python -m pip install markdown (forces your terminal to use python to find the library)
- Source File: Ensure you have your TCPDump text file ready (e.g., DumpFile.txt).

2. Configuration

The script requires a minor modification to locate your specific file before execution.

1. Open the Python script (import re.py or the name you gave it) in a code editor.
2. Scroll to the very bottom of the file (around line 285 in the original, or the final line in the provided code).
3. Locate the function call: generer_analyse(r"C:\Users\...\DumpFile.txt").
4. **Action:** Replace the file path inside the quotes with the actual location of your TCPDump file on your computer.

3. Running the Analysis

1. Run the Python script.
2. The script will process the data and display "Analyse terminée avec succès" (Analysis completed successfully) in the console.
3. Your default web browser will automatically open a local .html dashboard.

4. Understanding the Reports

The tool generates three types of files in the same directory as the script:

A. HTML Dashboard (dashboard_securite.html)

This is the interactive view that opens automatically. It includes :

- Statistics: A summary of total events and critical threats.
- Visuals: A donut chart showing the distribution of threats.
- Live Feed: A table listing the top 20 detected events.
- Export Buttons: Links to download the CSV or Markdown versions.

B. Markdown Report (RAPPORT_SECURITE.md)

A text-based summary suitable for documentation, listing the date, synthesis of alerts, and a log table.

C. CSV Report (RAPPORT_MENACES.csv)

A raw data file containing all details (Source, Target, Threat, Severity) intended for spreadsheet analysis.

5. Advanced Analysis with Excel

To visualize the data further, you can import the CSV results into Microsoft Excel.

Step 1 : Import the Data

1. On the HTML dashboard, click the "CSV" button to download the file.
2. Save the file (e.g., RAPPORT_MENACES.csv).
3. Open the file in Excel.

Step 2: Create a Severity Chart

To replicate the charts shown in the original documentation:

1. Select the data columns you wish to analyze (e.g., Severity and Menace columns).
2. Go to the "INSERT" (Insertion) tab and select "Recommended Charts".
3. Choose a Clustered Column Chart or Bar Chart.
4. The chart will display the number of hours or events per severity level (e.g., CRITIQUE vs. INFO).

Step 3: Filter Data

You can use Excel's Pivot Table features to filter by specific threats, such as:

- *Buffer Overflow (Padding)* - CRITIQUE.
- *SSH Traffic (Admin or BruteForce)* - INFO.

By using the selection pane on the right of Excel, you can toggle fields like "Source," "Cible" (Target), or "Gravité" (Severity) to customize your view.

Contact me if you have any questions:

- Github: /IRTBA