Notice for Using the Network Traffic Analysis Code

Summary

Python code

Creating and Applying Filters in Excel (CSV)

Python code

This document provides a step-by-step guide on how to use the provided Python code for analyzing network traffic data. The code is designed to process a tcpdump file, extract relevant information such as IP addresses, ports, and suspicious activities, and generate visualizations and reports. Additionally, it includes a Flask web application to interactively explore the results.

Prerequisites

Before running the code, ensure that you have the following installed on your system:

1. **Python 3.x**: The code is written in Python, so you need to have Python installed. You can download it from python.org.

2. Required Python Libraries: The code uses several Python libraries such as **Flask, matplotlib, markdown and collections.** You can install these libraries using pip:

pip install flask matplotlib markdown collections

3. Network Data File: The code expects a tcpdump file named DumpFile.txt in the same directory as the script. This file should contain the network traffic data you want to analyze.

Steps to Run the Code

1. Prepare the Input File

- Ensure that your tcpdump data is saved in a file named DumpFile.txt in the same directory as the script.

- If your file has a different name or location, update the input_file variable in the script to point to the correct file.

2. Run the Script

- Open a terminal or command prompt.

- Navigate to the directory where the script is located.

- Run the script using Python:

  python script_name.py

  Replace script_name.py with the actual name of your script file.

3. Analyze the Output

The script will generate several outputs:

- Markdown Report: A file named Resumé_Markdown.md will be created, containing a summary of the analysis, including the top IP addresses, top ports, and any suspicious activities detected.

- CSV File: A file named Donnees_csv.csv will be created, containing detailed information about each network packet, such as timestamps, source and destination IPs, flags, and packet lengths.

- Visualizations: The script will generate three graphs:

  - top_ips.png: A bar chart showing the top 10 IP addresses by occurrence.

  - top_ports.png: A bar chart showing the top 10 ports by occurrence.

  - port_distribution.png: A pie chart showing the distribution of the top 10 ports.

  These images will be saved in the static folder.

4. Launch the Flask Web Application

The script includes a Flask web application that allows you to interactively explore the analysis results.

- After running the script, the Flask app will start automatically.

- Open a web browser and navigate to http://127.0.0.1:5000/.

- You will see a web page displaying the analysis results and visualizations.

- You can filter the results by IP address or port using the provided form fields.

5. Stopping the Flask Application

- To stop the Flask application, go back to the terminal where the script is running and press Ctrl+C.

Customization

- Suspicious Ports: The script considers certain ports (22, 80, 443, 50019) as suspicious. You can modify the suspicious_ports set in the script to include or exclude ports based on your needs.

- File Paths: If you want to change the names or locations of the input or output files, update the input_file, markdown_output, and csv_output variables accordingly.

- Visualizations: You can customize the appearance of the graphs by modifying the matplotlib code in the script.

Troubleshooting

- File Not Found: If you encounter a FileNotFoundError, ensure that the DumpFile.txt is in the correct location and that the file path in the script is accurate.

- Missing Libraries: If you get an error about missing libraries, make sure you have installed all the required libraries using pip.

- Flask App Not Starting: If the Flask app does not start, ensure that no other application is using port 5000. You can change the port by modifying the app.run(debug=True) line to app.run(debug=True, port=5001) or another available port.

Conclusion

This script provides a comprehensive tool for analyzing network traffic data, generating reports, and visualizing key metrics. By following this guide, you should be able to run the script, interpret the results, and customize it to suit your specific needs.

Creating and Applying Filters in Excel (CSV)

This guide explains how to create and apply filters to the file Donnees_csv.csv using Microsoft Excel. Filters will allow you to extract specific information, such as packets from a particular IP address, packets destined for a specific port, or packets larger than a certain size.

Step 1: Open the CSV File in Excel

1. Open Excel.

2. Go to File > Open.

3. Select the file Donnees_csv.csv in the file explorer.

4. If Excel asks how to import the file, choose the Delimited option and ensure the delimiter is a comma (,). Click Finish.

Step 2: Apply Filters

Once the file is open, you can apply filters to analyze the data.

1. Select the column headers:

- Click on the first row (the headers: Time, Source IP, Destination IP, Flag, Packet Length).

2. Enable filters:

- Go to the Data tab in the toolbar.

- Click on the Filter button. Filter arrows will appear next to each column header.

Step 3: Use Filters

1. Filter by Source IP:

- Click the arrow next to Source IP.

- Uncheck Select All to deselect all IP addresses.

- Check the IP address you want to filter (for example, 192.168.1.1).
- Click OK. Only rows matching this IP address will be displayed.

2. Filter by Destination IP:

- Click the arrow next to Destination IP.
- Uncheck Select All.
- Check the destination IP address you want to filter.
- Click OK.

3. Filter by Port (if available):

If you have a Port column in your CSV file:

- Click the arrow next to Port.
- Uncheck Select All.
- Check the port number you want to filter (for example, 80 for HTTP).
- Click OK.

4. Filter by Packet Length:

- Click the arrow next to Packet Length.
- Select Number Filters.
- Choose an option, for example, Greater Than.
- Enter a value (for example, 100 to filter packets larger than 100 bytes).
- Click OK.

5. **Filter by Flag:**

- Click the arrow next to Flag.
- Uncheck Select All.
- Check the flag you want to filter (for example, S for SYN packets).
- Click OK.

Step 4: Save Filtered Data

1. After applying your filters, the data displayed in Excel will only include rows matching your criteria.

2. To save this filtered data:

   - Select all visible rows (using the mouse or Ctrl + A).

   - Copy the data (Ctrl + C).

   - Open a new Excel file or a new sheet.

   - Paste the data (Ctrl + V).

3. Save the new file under a different name (for example, Filtered_Data.csv).

Additional Tips

1. Combine Multiple Filters:

   You can apply multiple filters at the same time. For example:

   - Filter by Source IP = 192.168.1.1.

   - Filter by Packet Length > 100.

   - Only rows matching both criteria will be displayed.

2. Clear Filters:

   To remove all filters and display all data again:

   - Go to the Data tab.

   - Click Clear in the Sort & Filter group.

3. Use Advanced Filters:

   If you need more complex filtering criteria, you can use the Advanced Filter feature in Excel:

   1. Go to the Data tab.

   2. Click Advanced in the Sort & Filter group.

   3. Configure your filtering criteria in the dialog box.

Conclusion

By using filters in Excel, you can easily analyze the data in the Donnees_csv.csv file and extract the information you need. Whether you want to filter by IP address, port, packet length, or flag, Excel provides simple and powerful tools to help you explore your network data.