Network Security

Assignment: Network Telescope Analysis

Introduction

You are a network engineer and asked to perform a comprehensive analysis of network traffic captured by a telescope operated in your enterprise, using 12 PCAP files available for download on the Weblab platform. All the files consist of 30 minutes of consecutive traffic from the same network telescope. Your objective is to identify and visualize patterns indicative of scanning activities and connections targeting the network telescope. Focus your analysis on identifying scanning activities, such as port scans, IP scans, or reconnaissance activities, as well as connections observed within the network traffic. You can do the analysis on the entire packets, or if it does not fit in your memory feel free to split them and do the analysis on the chunks.

Important Note on Tools

Wireshark may not be suitable for this assignment. The provided PCAP files are large and may cause Wireshark to crash or become unresponsive. While Wireshark is a powerful tool for inspecting individual packets, it is not designed for large-scale or long-duration traffic analysis.

For this assignment, you are strongly encouraged to use **script-based tools**, such as:

- `tshark` (command-line version of Wireshark)
- Python libraries such as `scapy` or if there is still too much data `dpkt`.

These tools allow you to extract only the relevant fields, handle data in chunks, and process the entire dataset more efficiently. Avoid attempting to open the full PCAPs in Wireshark, as this is not a scalable or reliable approach for the volume of traffic in this assignment.

Assignment

1. **Data Analysis (40 Points)**
   - Analyze the 12 PCAP files to uncover TCP SYN and UDP scanning behavior. Provide Python scripts to answer the following:
     - **Top Scanners (10 points)** List the top 10 scanner IPs by packet count and their share of total traffic. *Max 50 words + table*
     - **Top Target Ports (10 points)** List the top 10 destination ports for TCP and UDP scans. *Max 50 words + table*
     - **Protocol Breakdown (5 points)** Count TCP vs UDP packets. *Max 30 words + pie or bar chart*
     - **Heavy Hitter Scanner (15 points)** Pick the scanner with the most packets. Report:

    - Number of packets
    - Number of destination IPs
    - Number of ports
    - Country (use geolocation)

  Max 100 words

2. **Visualization (30 Points)**
   - Create 3 clear plots:
     - **Time Series (10 points)** Show packet count over time (5 min bins).
     - **Port Distribution (10 points)** Plot top 10 scanned ports.
     - **Scanner Scope (10 points)** Plot number of IPs scanned by top 10 scanners.
3. **Interpretation Reasoning (30 Points)**
   - **Pattern Recognition (15 points)** Based on the data and plots:
     - Are scanners targeting specific ports or sweeping ranges?
     - Is scanning bursty or steady over time?

     Max 150 words and a descriptive visual
   - **Threat Assessment (15 points)** Choose one scanner. Based on its behavior, answer:
     - Is this likely a mass scanner, targeted probe, or misconfigured host?
     - What risk does it pose?

     Max 150 words and a descriptive visual
4. **Code Submission (Required, 0 Points)**
   - Submit all scripts and notebooks used in your analysis. Include:
     - A short README with instructions on how to run your code
     - Clear file names matching the analysis tasks (e.g., 'top_scanners.py')
     - Use comments in code where appropriate

     Failure to submit code will result in 0 for all technical sections.

Submission

Submit your Python scripts, README files, and a single PDF report containing visualizations and analysis results. Ensure that your scripts are well-commented, modular, and properly structured. Provide clear instructions on installing any dependencies required to run your scripts. Please compress all your findings into a (.tar/.zip) file when uploading them to Weblab.