Background

ABC Inc., a mid-sized software development company, has recently been the target of multiple attempted cyber-attacks. With an increase in sophisticated threats, the company has decided to proactively monitor their network traffic. ABC utilizes a Linux-based infrastructure, with the majority of their servers hosted on-premise and a few critical services on AWS. The IT security team needs a robust mechanism to analyze the logs generated by their firewalls to quickly identify and respond to potential threats.

The security of ABC network is paramount. The firewall serves as the first line of defence, regulating incoming and outgoing network traffic based on an applied rule set. The logs generated by the firewall provide valuable data that can be analyzed to detect anomalies, identify patterns of malicious activity, and aid in fortifying the network against attacks.

Why This is Important

By analyzing the firewall logs, ABC hopes to achieve the following objectives

- Detect and respond to threats in real-time.
- Enhance their understanding of the traffic patterns.
- Improve their network's security posture by adjusting firewall rules based on the insights gained from the logs.
- Comply with industry regulations that mandate the monitoring and analysis of security logs.

Task Details

You, as the security intern, are tasked with developing a Simple Firewall Log Analyzing script that will help ABC Tech achieve these goals. Your script will need to process logs generated by ip tables on Linux servers as well as logs from AWS security groups. Sample log file is given below.

Develop the script using Python(Or any language).

Deliverables

- A script(Python or any language) for parsing and analysis.
- Documentation for a summary report with insights and recommendations.

Expected Outcome

By the end of the week, ABC Tech expects to have a preliminary version of the script ready for testing. The script should be able to process a sample log file, detect potential threats, and present the analysis in a meaningful way. This will allow the security team to evaluate the effectiveness of the current firewall rules and adjust them as necessary to better protect the network.

Sample Firewall Log File - firewalllog_2023_11_7.log

Submit your solution to a github repository with a README file and share the repository link with Random Software within a week (Reply to the email thread)