Documentation for Firewall Log Analyzer and Recommendations

Date Issued: 11/12/2023.

Executive Summary

With the increasing of information security potential hacking attempts in the organization, Security Operational Center (SOC) is thoroughly working on a concept of introducing new technologies for identifying security risks from outsiders. Which involves high programming concepts and software technologies. As a part of the mentioned project the team recommended developing software that can easily detect suspicious network traffic to the organization's infrastructure. Which will be efficient and faster than traditional methods.

The team has developed software using (Python) programming language and it is currently under the testing process. This document will give a summary of the work for far in the project, how this new method is efficient for the organization and what are other recommendations for future development.

Overview

This project consists of a Python script for analyzing traffic patterns by IP addresses. It basically counts repeated IP addresses in the Log file that could potentially be a DOS attack. This will help the monitoring team to find and respond to threats in real time. As inputs the users should provide the Firewall log file with default format as a separate file in the running environment. By getting the output of repeated source IP addresses the team of ABC will find DOS and other potential threats. Then the team can investigate that IP addresses to see whether it is malicious or merely a flood attempt. This will also be helpful for maintaining availability of the systems if the traffic is malicious after the investigation those IP addresses can be banned from the network or any other controls to mitigate unwanted traffic.

```
for ip, count in source_ip_counter.items():
    if count > 3:
```

As in the above figure more than 3-time repeated source IP addresses is categorized as suspicious and will be alerted as an output. Number 3 has selected hypothetically and should change as flexible for the infrastructure.

Future Development

As for the Future development for this project, few new areas have been selected to be implemented to make project more effective and useful. That areas include,

- Use Machine Learning to automate other processes of analyzing log patterns such as identifying particular malicious IP ranges of traffic, filter by destination IP addresses by giving more priority to critical systems.
- Identifying suspicious IP addresses or records by TCP flag values.
- Explore integration with Security Information and Event Management (SIEM) systems for more comprehensive security monitoring and correlation with other security events.
- Integrated alerting systems for SOC team.