Firewall Log Analysis Report Documentation

Objective:

The objective of this Firewall Log Analysis Report is to provide insights into the network traffic patterns, identify potential threats, and make recommendation to enchance the security posture of ABC inc.' network.

Log File Used:

- File name – firewalllog_2023_11_7.log

Analysis Overview:

The firewall log analysis script processed the log file, extract relevant information and provides a summary report on key insights and recommendations.

Insights:

Total Log Entries:

- The total number of log entries processed from the firewall log file is 13.

Action Distribution:

- **Breakdown of actions (Allow, Block)**
  - Allow – 7
  - Block – 6

```
~/test-04$ python3 main.py
2023-03-15 06:26:45 BLOCK UDP 192.168.1.105 192.168.1.255 138 138 229 - - Local Broadcast
2023-03-15 06:27:58 BLOCK TCP 192.168.1.105 203.0.113.5 44347 22 48 S - SSH Attempt
2023-03-15 06:30:05 BLOCK TCP 192.168.1.106 198.51.100.24 44348 80 52 S - Client Hello
2023-03-15 06:31:19 BLOCK TCP 192.168.1.108 203.0.113.10 44350 1433 40 S - SQL Server Access Attempt
2023-03-15 06:33:45 BLOCK ICMP 192.168.1.110 10.10.10.10 - - 84 - - Destination Unreachable
2023-03-15 06:35:27 BLOCK UDP 192.168.1.112 192.168.1.230 44353 161 60 - - SNMP Access Attempt
~/test-04$
```

Recommendations:

1. **Rule Adjustment**
    - Evaluate the necessity of rules allowing certain traffic patterns. Consider adjusting firewall rules to minimize unnecessary exposure.

2. **Anomaly Detection**
    - Implement anomaly detection mechanisms to identify unusual traffic patterns that might indicate a security threat.

3. **Regular Log Analysis**
    - Establish the routine for regular analysis of firewall logs to stay proactive in identifying potential threats.

4. **Incorporate Threat Intelligence**
    - Integrate threat intelligence feeds to stay updated on known malicious Ips and patterns.
5. **Enhanced Logging**
    - Enhance logging to capture additional information such as protocol types, source ports and destination ports.

Conclusion:

Preliminary analysis provides a basis for understanding network traffic and potential security threats. To achieve a more comprehensive view, further refinement of the protocol analysis mechanism and the incorporation of advanced analysis techniques are recommended.

Next Steps :

1. Refine Log Parsing: Ensure accurate parsing of all log entries by adjusting the log parsing function to match the actual log format.

2. Advanced Analysis: Explore the possibility of leveraging advanced log analysis tools or frameworks, such as the ELK stack (Elasticsearch, Logstash, Kibana), for more sophisticated analysis and visualization.

3. Continuous Improvement: Regularly update and improve the firewall log analysis script based on the evolving nature of network threats.