[RSSL] Cyber Security Intern - Security Test

Firewall Log Analysis Summary Report

- **Purpose**

This document aims to provide a summary of the analysis conducted on the firewall logs for ABC Inc., highlighting key findings and recommendations to enhance network security.

- **Key Objectives**

Real-time Threat Detection - Identify potential threats and respond promptly.

Traffic Patterns Understanding - Enhance understanding of network traffic patterns.

Security Posture Improvement - Propose adjustments to firewall rules to improve the network's security posture.

Regulatory Compliance - Ensure compliance with industry regulations mandating security log monitoring and analysis.

- Findings and Insights

Local Broadcast (Log Entry 1)

Finding - Local broadcast attempts detected.

Insight - Local broadcast events may indicate potential internal network anomalies.

Recommendation - Further investigate the source and purpose of local broadcasts; adjust firewall rules accordingly.

SSH Attempt (Log Entry 2)

Finding - Blocked SSH attempt on port 22.

Insight - Possible SSH brute-force attack.

Recommendation - Strengthen SSH access controls, consider rate-limiting, or implement multi-factor authentication.

Client Hello (Log Entry 3)

Finding - Blocked TCP connection with Client Hello.

Insight - Possible attempt to establish unauthorized connections.

Recommendation - Investigate the source and destination, and validate the legitimacy of the connection.

SQL Server Access Attempt (Log Entry 4)

Finding - Blocked TCP connection on port 1433.

Insight - Potential SQL Server access attempt.

Recommendation - Review SQL Server security settings, and restrict access to trusted sources.

Destination Unreachable (Log Entry 5)

Finding - Blocked ICMP Destination Unreachable.

Insight - Possible network scanning or reconnaissance.

Recommendation - Monitor for similar ICMP activities, and consider implementing network segmentation.

SNMP Access Attempt (Log Entry 6)

Finding - Blocked UDP connection on port 161.

Insight - Potential SNMP access attempt.

Recommendation - Validate the need for SNMP, restrict access, and monitor SNMP-related activities.

- **Script Information**

get_latest_firewall_log - Retrieves the latest firewall log file from the specified folder.

analyze_firewall_log - Identifies and analyzes log entries with "BLOCK" actions.

- Extracts attack types based on the content of the "Info" field.

Usage -Run the script to automatically process the latest firewall log.

- The script provides detailed information about blocked activities and potential threats.

Conclusion

The provided script offers a preliminary analysis of the latest firewall log, highlighting instances of blocked actions and potential security threats. Regular use of this script, coupled with

proactive adjustments to firewall rules, will contribute to ABC Inc.'s efforts to fortify its network against cyber threats.