Name: M.A. Dilshara Sandeepani

Git Hub Link: <https://github.com/it21164576/Firewall->

This summary report is an overview of the findings and recommendations resulting from the analysis of firewall logs using the Simple Firewall Log Analyzing script. The primary objective of the analysis is to enhance the network security posture of ABC Inc. by proactively monitoring network traffic and responding to potential threats.

**SSH Unusual Attempts:**

* Identified abnormal SSH connection attempts on port 22.
* Excluded connections from private IP addresses.

**SQL Unusual Access:**

* Detected potential unusual SQL-related access attempts on port 1433.
* Filtered out connections from private IP addresses.

**Port 80 (HTTP) Attempts:**

* Analyzed attempts to access HTTP (port 80) connections.
* Excluded connections from private IP ranges.

**Allowed Connections:**

* Examined connections permitted by firewall rules.
* Provided insights into the types of permitted traffic.

**Blocked Connections:**

* Investigated connections blocked by the firewall.
* Identified potential threats or unwanted traffic.

**TCP and UDP Connections:**

* Differentiated and analyzed TCP and UDP connections separately.
* Provided insights into the distribution and characteristics of each protocol.

**Public Connection Attempts**:

* Filtered out connection attempts from private IP ranges.
* Focused on identifying connections from public IP addresses.

**Recommendations**

**Strengthen SSH Security:**

* Implement additional security measures for SSH, such as two-factor authentication.
* Monitor and respond to SSH connection attempts from public IP addresses more closely.

**SQL Access Controls:**

* Review and enhance access controls for SQL services.
* Regularly update and patch SQL servers to mitigate potential vulnerabilities.

**Web Traffic Monitoring:**

* Continue monitoring and analyzing web traffic on port 80 for any unusual patterns.
* Consider implementing a web application firewall (WAF) for added protection.

**Review Firewall Rules:**

* Regularly review and update firewall rules based on insights gained from the analysis.
* Consider adjusting rules to better align with the organization's security policies.

**Incident Response:**

* Develop and document an incident response plan for addressing identified threats.
* Establish protocols for real-time response to potential security incidents.

**Periodic Analysis:**

* Conduct regular periodic analysis of firewall logs to stay vigilant against evolving threats.
* Stay informed about emerging security trends and adjust analysis criteria accordingly.

**Conclusion**

The Simple Firewall Log Analyzing script provides valuable insights into network traffic, aiding in the identification of potential threats and the enhancement of ABC Inc.'s network security posture. The recommendations outlined aim to further strengthen the security measures and response capabilities of the organization.