SOC Analyst Investigation Report using Splunk

**Subject: Investigation of Exchange Exploit Attempts, Lateral Movement, and Persistence Using Splunk**

**Date: April 29, 2025**

**Analyst: SOC Analyst**

**Summary:**

I conducted a focused investigation using Splunk to monitor Exchange exploit attempts, lateral movement, and persistence mechanisms within our environment. Leveraging data from Sysmon and Windows Event Logs, I aimed to detect suspicious activities and respond effectively to potential threats.

**Detection Focus:**

I monitored Exchange server logs and network traffic in Splunk to identify exploit attempts targeting known vulnerabilities.

I tracked lateral movement by analyzing authentication events and unusual access patterns across endpoints.

I examined persistence mechanisms by reviewing process creation and service installation events captured by Sysmon.

**Response Actions:**

I investigated potential data exfiltration patterns by correlating outbound network traffic with unusual file access events.

I analyzed credential dumping activities by searching for suspicious process executions and event IDs associated with credential theft in Windows Event Logs.

**Tools Employed:**

Splunk: Centralized platform for aggregating and analyzing logs, enabling real-time detection and correlation of suspicious activities.

Sysmon: Provided detailed system activity logs, including process creation and network connections, critical for identifying persistence and lateral movement.

Windows Event Logs: Offered additional context on authentication events and system changes relevant to the investigation.

**Conclusion:**

By utilizing Splunk alongside Sysmon and Windows Event Logs, I was able to detect and investigate Exchange exploit attempts, lateral movement, and persistence tactics effectively. My response actions focused on identifying data exfiltration and credential dumping, helping to mitigate potential damage and strengthen our security posture.