**Splunk SIEM Log Analysis Report**

**Project Title:** BOTSv1 Attack Log Analysis using Splunk  
**Prepared by:** Rachel  
**Date:** 26 May 2025

**1. Introduction**

This report documents the analysis of cybersecurity attack logs using the Splunk BOTSv1 dataset. The purpose of the project was to simulate a Security Operations Center (SOC) environment by investigating patterns of suspicious activity, generating visualizations, and applying SIEM techniques for incident detection and response.

**2. Tools & Dataset**

* **Tool Used:** Splunk Enterprise (Free Tier)
* **Dataset:** BOTSv1 (Boss of the SOC)
* **Log Sources:** System logs, endpoint logs, and network activity

**3. Methodology**

* The BOTSv1 logs were uploaded and indexed into Splunk.
* SPL (Search Processing Language) was used to extract error terms, host activity, and event trends.
* Visualization dashboards were created to illustrate patterns and detect anomalies.

**4. Dashboard Panels Created**

**4.1 Panel 1: Top Error Hosts**

**Query Used:**

index=botsv1 earliest=0 ("error" OR "fail\*")

| stats count by host

| sort -count

**Insight:**

* Host splunk-02 produced over 4,300 errors
* Hosts we9041srv and suricata-ids.waynecorpinc.local also showed high error activity

**4.2 Panel 2: Error Trends**

**Query Used:**

index=botsv1 earliest=0 ("error" OR "fail\*")

| timechart span=1h count by host

**Insight:**

* Spikes in error activity detected around specific time intervals, especially involving splunk-02 and suricata-ids hosts.
* These could suggest system instability or potential ongoing malicious scanning.

**4.3 Panel 3: Error Types**

**Query Used:**

index=botsv1 earliest=0

| rex field=\_raw "(?<error\_term>error|fail|critical|denied|timeout|refused|exception)"

| stats count by error\_term

**Insight:**

* timeout: 81,689 occurrences
* critical: 20,467 occurrences
* refused: 10,961 occurrences
* These terms typically indicate dropped packets, critical service failures, or denied access attempts.

**5. Threat Analysis Summary**

Although direct brute-force attack patterns (e.g., "Failed password") were not found in the logs, the extremely high volume of error events — especially timeouts and critical errors — is consistent with:

* Potential Denial-of-Service (DoS) attempts
* Network misconfiguration or instability
* Reconnaissance or scanning behavior by threat actors

The host splunk-02 may require investigation due to its dominant error rate, which far exceeds that of other systems in the network.

**6. Conclusion**

The Splunk BOTSv1 dataset was effectively used to simulate a real-world SOC environment. The dashboards helped visualize system-level anomalies and identify hosts with high risk behavior. These insights support the ability to proactively monitor enterprise infrastructure and detect early signs of attack.

**Skills demonstrated:**

* SIEM platform configuration (Splunk)
* Log ingestion and indexing
* SPL-based detection queries
* Security event correlation and reporting



