**Detection Engineering Report**

**Title:**  
Detection Engineering Rule: Unauthorized Network Scanning Activity

**1. Objectives**

The primary goal of this report is to describe the detection techniques used to spot unauthorized network scanning activity. Such activity is often a precursor to more serious attacks and involves systematically probing network ports and services.

**2. Detection Logic**

Our detection is based on identifying a high volume of SYN packets—commonly seen in Nmap scans or similar reconnaissance tools. The following Splunk query is used:

pgsql

CopyEdit

tag=network\_traffic protocol=TCP TCP\_flags=SYN

| stats count by src\_ip

| search count > 50

This query aggregates SYN packets by source IP and triggers an alert if any IP exceeds 50 packets within a designated timeframe (e.g., 10 minutes). The threshold is adjustable to fit the network’s normal traffic profile.

**3. Analysis**

Upon alert, the following steps are taken:

* **Examine Traffic Patterns:** Analyze the distribution and frequency of SYN packets to determine if they align with scanning behavior.
* **Port & Service Assessment:** Identify targeted ports and services to gauge the potential impact of the scan.
* **Threat Correlation:** Compare the source IP against known threat databases to determine if it is linked to scanning tools or threat actors.
* **Incident Follow-up:** Investigate any subsequent connections or data breaches that may have occurred.

**4. Alert Settings**

To implement this detection in Splunk:

* **Create a New Alert:**
  + Open the 'Search & Reporting' app.
  + Enter the detection query and verify its output.
  + Click “Save As” > “Alert.”
* **Configure Alert Properties:**
  + **Title:** "Unauthorized Network Scanning Activity"
  + **Alert Type:** Choose either Real-time or Scheduled monitoring.
  + **Trigger Condition:** For example, set “Number of Results” greater than 100 (or as per your threshold).
  + **Alert Frequency:** Decide whether to trigger the alert once or for each result.
* **Set Alert Actions:**
  + Define actions such as sending an email or SMS to notify the security team, including key details from the alert.
* **Review & Enable:**
  + Confirm all settings, save the alert, and enable monitoring.

**5. Conclusion**

This detection framework is designed to catch unauthorized network scanning by monitoring for excessive SYN packets. Regular review and calibration of thresholds and alert settings are essential to adapt to changing network conditions. Timely alerts allow the security team to quickly investigate and mitigate potential threats, significantly reducing the risk of exploitation.