TASK 8: “Monitoring and Threat Detection”

Basic SIEM Setup and Log Monitoring Using Splunk Free

1. Introduction

This task demonstrates the installation and configuration of Splunk Free for log monitoring and threat detection. The objective is to simulate a basic SIEM (Security Information and Event Management) setup to monitor system logs, visualize activities using dashboards, and configure alerts for suspicious activities such as failed logins or privilege escalations.

The scope of this task includes:

- Installing Splunk Free on a Linux or Windows virtual machine
- Configuring log collection from system log files
- Creating a custom dashboard to visualize activity
- Setting up alerts for suspicious events

2. Installation: Splunk Free

2.1 System Requirements

- Supported Operating Systems:
    - Linux (Ubuntu/Debian or Red Hat-based systems)
    - Windows (Server and Desktop editions supported)
- Minimum Resources:
    - RAM: 2 GB (recommended 4 GB or more)
    - Disk Space: 10 GB (or more depending on logs ingested)
- Network Access:
    - Splunk Web UI accessible on port 8000

2.2 Download & Install Splunk

Steps for Linux (Ubuntu/Debian example):

1. Download the Splunk Enterprise Free Trial package from the Splunk official downloads page.
2. Install the downloaded .deb package:
3. sudo dpkg -i splunk_package_name.deb
4. Start Splunk service:
5. sudo /opt/splunk/bin/splunk start
6. Accept the license agreement.
7. Set up an admin username and password when prompted.

Access Splunk Web Interface:

- Open a browser and navigate to:
- http://localhost:8000
- Log in using the admin credentials configured.

3. Adding Log Data for Monitoring

Splunk allows ingestion of log files for continuous monitoring.

Steps:

1. Log in to the Splunk Web UI.
2. Click on "Add Data".
3. Select "Monitor" to configure real-time log monitoring.
4. Choose "Files & Directories".
    - Example: /var/log/ (for Linux system logs).
5. Provide a unique input name, e.g., linux_logs.
6. Assign data to an index (e.g., remotelogs).
7. Review configuration and click Submit.

At this stage, Splunk will continuously monitor the configured directory for new log entries.

4. Creating a Dashboard

Dashboards provide visual representations of log data.

Steps:

1. Open the Search & Reporting app in Splunk.
2. Run a query to summarize log activity, e.g.:
3. index=remotelogs | stats count by sourcetype, host
4. Save the search as a dashboard panel:
    - Click Save As > Dashboard Panel
    - Provide a name, e.g., *Linux Log Monitoring*
    - Choose a new or existing dashboard.
5. Open the dashboard to view activity statistics.

This creates a custom monitoring view of incoming log data.

5. Setting Up Alerts for Suspicious Activity

One of the most important SIEM capabilities is detecting abnormal behavior. Splunk provides alerts triggered when certain conditions are met.

Common Suspicious Patterns:

- Multiple failed SSH login attempts (brute force attack indicator)
- Creation of new user accounts (potential persistence)
- Privilege escalation events (use of sudo or admin rights)

Example: Alert for Multiple Failed SSH Logins

Steps:

1. Navigate to Search & Reporting.
2. Run the following search query:
3. index=remotelogs "Failed password"
4. Save search as an Alert:
    - Condition: Trigger when Number of Results > 5 within 10 minutes

    - Actions:
        - Send email notification (requires mail server configuration), or
        - Log the event in Splunk for review.
5. Name and save the alert (e.g., *Failed SSH Login Alert*).

Example: Alert for New User Creation

Search Query:

```
index=remotelogs "useradd" OR "new user"
```

Configure alert to trigger if any results are detected.

Example: Alert for Privilege Escalation

Search Query:

```
index=remotelogs "sudo" OR "root access"
```

Trigger alert on any unexpected escalation activity.

6. Results and Verification

- Dashboard Creation: Successfully created a custom dashboard displaying log activity by source and host.
- Alerts Configured:
    - Alert for multiple failed SSH logins
    - Alert for suspicious user creation
    - Alert for privilege escalation
- SIEM Capability: Splunk Free successfully simulated a lightweight SIEM environment capable of detecting and reporting basic threats.

7. Recommendations

- Configure email notifications for alerts to ensure prompt response.
- Regularly refine queries to detect emerging threats.
- Extend log collection to include application logs, web server logs, and database logs.
- Consider upgrading to Splunk Enterprise for advanced correlation, scalability, and enterprise-grade features.

8. Conclusion

This exercise demonstrated the deployment of Splunk Free as a basic SIEM solution for monitoring system logs and detecting suspicious activities. By configuring log ingestion, dashboards, and alerts, Splunk provided visibility into system events and enhanced threat detection capabilities.

The setup forms a foundational security monitoring framework that can be further expanded with additional data sources and advanced Splunk features.