**Installation and Configuration**

**1. Install and Configure Sysmon on Windows 10**

**Sysmon** (System Monitor) is a Windows system service and device driver that logs system activity to the Windows Event Log. Follow these steps:

1. **Download Sysmon** from the official Microsoft Sysinternals website.
   * [Sysmon Download Link](https://docs.microsoft.com/en-us/sysinternals/downloads/sysmon)
2. **Install Sysmon** with a configuration file:

sysmon -accepteula -i sysmonconfig.xml

The sysmonconfig.xml file should include configuration rules for logging events like process creation, network connections, etc.

1. **Verify Sysmon installation** by checking for event logs in the Event Viewer:
   * Navigate to: Applications and Services Logs > Microsoft > Windows > Sysmon

**2. Set Up Splunk Enterprise on Kali Linux**

1. **Download and Install Splunk**:
   * Download the Splunk Enterprise package from the official Splunk website.
   * Install the downloaded package:

sudo dpkg -i splunk\_package.deb

* + Enable Splunk to start at boot and start the service:

sudo /opt/splunk/bin/splunk enable boot-start

sudo /opt/splunk/bin/splunk start

1. **Access Splunk Web Interface**:
   * Open a web browser and go to http://localhost:8000.
   * Login using your Splunk credentials (default: admin/changeme).
2. **Create an Index in Splunk**:
   * Go to the **Settings** > **Indexes** page.
   * Create a new index named win10.

**3. Install and Configure Universal Forwarder**

1. **Download the Universal Forwarder** from Splunk’s website and install it on Windows 10.
   * Splunk Universal Forwarder Download
2. **Configure the Universal Forwarder** to forward Sysmon logs:
   * Open a command prompt and navigate to the installation directory of the Universal Forwarder.
   * Run the following command to configure the forwarder to send logs to the Splunk server:

splunk add forward-server <Kali\_IP>:<Port> -auth admin:changeme

1. **Add Sysmon Logs for Monitoring**:
   * Navigate to the Universal Forwarder directory and edit the inputs configuration file:

notepad C:\Program Files\SplunkUniversalForwarder\etc\system\local\inputs.conf

* + Add the following configuration:

[WinEventLog://Microsoft-Windows-Sysmon/Operational]

disabled = 0

index = win10

1. **Restart the Universal Forwarder**:

splunk restart

**4. Configure Splunk to Receive Logs**

1. **Open a Listening Port in Splunk**:
   * Go to **Settings** > **Data Inputs** > **TCP** > **New TCP**.
   * Select a port (e.g., 9997) and open it for receiving data.
2. **Verify Data Ingestion**:
   * Go to **Search & Reporting** in Splunk.
   * Run a search query for the win10 index to verify that Sysmon logs are being ingested:

splunk

index="win10"

**5. Configure Alerts for Authentication Failures**

1. **Create a Search Query for Authentication Failures**:
   * Navigate to **Search & Reporting** in Splunk.
   * Run a search query to detect authentication failures:

index="win10" EventCode=4625

This search will filter out failed login attempts based on Windows Event Code 4625.

1. **Set Up an Alert**:
   * After running the query, click **Save As** > **Alert**.
   * Set the following parameters:
     + **Alert Type**: Scheduled or Real-time (based on your preference).
     + **Trigger Conditions**: For example, trigger if the number of failed logins exceeds a threshold.
     + **Actions**: Set up email notifications or run scripts when the alert is triggered.
2. **Test the Alert**:
   * Force a few failed login attempts on your Windows 10 machine and verify that the alert is triggered in Splunk.

**Testing**

After configuration, test the setup by generating events on the Windows 10 machine. For example:

* Open applications to trigger process creation events.
* Open network connections to generate network logs.
* Simulate failed login attempts to trigger the authentication failure alert.

Monitor the logs in the **Splunk Search & Reporting** tool by searching the win10 index.

**Sample Queries:**

1. **View all logs from Sysmon**:

splunk

index="win10"

1. **Filter logs by event type (e.g., process creation)**:

splunk

index="win10" EventID=1

1. **Authentication failure logs**:

splunk

index="win10" EventCode=4625

**Future Enhancements**

* **Add Dashboards**: Set up dashboards in Splunk to visualize data from Sysmon logs.
* **Additional Alerts**: Create alerts for other suspicious activities, such as privilege escalations or file changes.
* **Additional Data Sources**: Add more data sources like Windows Security logs for comprehensive monitoring.