1.1 Install Graylog

To begin, you'll need to install **Graylog** along with **MongoDB** (for storing configurations and metadata) and **Elasticsearch** (for storing and querying log data).

You can install Graylog on a Linux machine. Here's a quick setup on an Ubuntu server:

Install MongoDB:
bash
Copy
```
sudo apt update
sudo apt install -y mongodb
```

1.

Install Elasticsearch: Download and install the Elasticsearch package suitable for your system. Example:
bash
Copy
```
wget
https://artifacts.elastic.co/downloads/elasticsearch/elasticsearch-7.9
.3-amd64.deb
sudo dpkg -i elasticsearch-7.9.3-amd64.deb
sudo systemctl start elasticsearch
sudo systemctl enable elasticsearch
```

2.

Install Graylog: Download and install Graylog:
bash
Copy
```
wget
https://packages.graylog2.org/releases/graylog-4.0/graylog-4.0.0.tgz
tar -xvzf graylog-4.0.0.tgz
cd graylog-4.0.0
sudo ./bin/graylogctl start
```

3.
4. **Access Graylog**: Open your browser and go to `http://<your-server-ip>:9000/`. The default login credentials are `admin`/`admin`.

1.2 Configure Input for Log Data Collection

To collect log data, you'll need to configure an **Input** in Graylog. For this demo, let's use **Syslog UDP** as the input type.

1. In Graylog, go to **System > Inputs**.
2. Click on **Launch new input**.
3. Select **Syslog UDP** and click **Launch new input**.
4. Configure the input (e.g., UDP port 514) and start it.

Now, Graylog is ready to receive logs.

1.3 Simulate Mock Data

We will create mock logs for an SSH brute-force attack, which Graylog will collect and analyze. You can simulate the logs by generating them via a local syslog generator or a simple bash script.

Example Bash Script:

bash
Copy

```
#!/bin/bash

for i in {1..10}; do
  logger "Failed password for invalid user admin from 192.168.1.$i
port 22 ssh2"
done
```

Run this script to simulate multiple failed SSH login attempts from different IP addresses.

Step 2: Create Detection Rules

Now, we'll create a **detection rule** to catch potential brute-force attacks based on a series of failed login attempts.

2.1 Create a Stream for SSH Logs

1. In Graylog, go to **Streams** and create a new stream for SSH logs (e.g., `SSH Failed Login Attempts`).
2. Define the stream rule:
    - **Source**: Select `syslog`.

- **Condition**: Choose a condition like `Message contains 'Failed password'`.

2.2 Create a Dashboard with Alerts

You'll want to visualize the alerts for faster detection.

1. Create a **Dashboard** to display events related to failed login attempts.
2. Add widgets to the dashboard for things like:
   - Total number of failed logins
   - Count of unique source IPs
3. Set up **Alerting** to trigger an alert when the number of failed login attempts exceeds a threshold (e.g., 5 failed attempts within 10 minutes).

2.3 Define Alert Prioritization Process

Graylog provides flexibility in alerting. We can set up a prioritization system based on the severity of the detected incident. For example:

- **Low Priority**: Single failed login attempt.
- **Medium Priority**: Multiple failed login attempts from a single IP.
- **High Priority**: Failed login attempts from multiple IPs targeting critical services.

Step 3: Document Incident Response Scenario

In this section, we will simulate an **Incident Response** scenario based on the detection of a brute-force attack on SSH.

3.1 Incident Classification

- **Incident ID**: 2025-01-29-01
- **Incident Type**: Brute-force attack (SSH)
- **Severity**: High
- **Classification**: Unauthorized Access Attempt

3.2 Response Steps

1. **Alert Detection**: The Graylog alert system detects 10 failed login attempts in a 5-minute window from multiple IP addresses targeting the SSH service.
2. **Investigation**:
   - **Query Logs**: The security analyst queries the logs for the IP addresses involved in the attack. The logs indicate that these are external IP addresses.
   - **Correlate Events**: The analyst checks for any successful logins from these IPs and finds none.

    - **Review Other Logs**: Check for any other suspicious behavior or access attempts from the same IPs in other services (e.g., web server logs, database logs).
3. **Containment**:
    - The IP addresses involved in the attack are added to a firewall blocklist.
    - The affected user account is temporarily locked out.
4. **Eradication**:
    - The analyst checks the server for any signs of compromise (e.g., unusual processes, new user accounts).
    - No malware is found, and the server is secured.
5. **Recovery**:
    - The user account is unlocked after ensuring that no unauthorized access occurred.
    - Any suspicious configuration changes are reverted.
6. **Post-Incident Activities**:
    - **Root Cause Analysis**: The attack was a brute-force attempt against weak SSH credentials.
    - **Lessons Learned**:
        - Enforce strong password policies.
        - Use multi-factor authentication (MFA) for SSH.
        - Limit SSH access to trusted IPs.

3.3 Documentation of Incident Response

Here is a basic template for documenting the incident:

markdown
Copy

```
### Incident Report: Brute-Force SSH Attack

**Incident ID**: 2025-01-29-01
**Classification**: Brute-force attack
**Severity**: High
**Impact**: Potential unauthorized access to server resources

---

**Incident Timeline**:
- **12:34 PM**: 10 failed SSH login attempts detected from multiple external IP addresses targeting `user: admin`.
- **12:40 PM**: Alert triggered by Graylog based on configured detection rule.
- **12:45 PM**: IP addresses blocked at firewall, account locked.
```

```
**Response Actions**:
1. Investigated logs for any signs of successful login or compromise.
2. Blocked malicious IP addresses at the firewall.
3. Account locked out, and further analysis showed no breach.
4. Passwords were reset, and server configurations were checked.

**Lessons Learned**:
- Use complex passwords and implement MFA for SSH access.
- Limit SSH access by IP address and implement fail2ban or similar
defense tools.
```

Step 4: Evidence of Functionality

To demonstrate the functionality of this setup, you should provide:

- **Graylog Dashboards**: Screenshots of the dashboards showing the failed login attempts.
- **Alert Logs**: A snapshot or export of Graylog alerts generated from the detected brute-force attack.
- **Incident Report**: The markdown documentation of the incident response.