Security Monitoring Project Outline

1. Basic Security Monitoring Setup

Tools Used:

- **Graylog** (a simple log monitoring tool with a web interface).

- **Linux system logs** (e.g., /var/log/syslog for system events and /var/log/auth.log for authentication).

- **Mock data** (pretend logs for testing).

Steps to Set Up:

1. **Install Graylog**:

   - Use a virtual machine or a basic server to install Graylog.

   - Follow simple online tutorials for installation (e.g., set up Elasticsearch and MongoDB, which Graylog uses).

2. **Configure a Log Forwarder**:

   - Use **rsyslog** (a built-in Linux tool) to send logs from a test machine to your Graylog server.

3. **Create a Dashboard**:

   - Use Graylog's interface to create a simple dashboard showing:

   - Login attempts.

   - Errors in the system logs.

2. Detection Rules and Alerts

Use Case: Failed Login Attempts

- **What Are We Looking For?**

  - A user fails to log in more than 3 times in 2 minutes (like someone guessing passwords).

- **How to Set It Up**:

  1. Look at /var/log/auth.log for "Failed password" messages.

2. Set a **Graylog alert**:

    - If there are more than 3 failed logins from the same IP in 2 minutes, send an email alert.

- **Data**:

```
Jan 22 15:20:01 sshd[12345]: Failed password for user1 from 192.168.1.50 port 2222 ssh2

Jan 22 15:20:10 sshd[12345]: Failed password for user1 from 192.168.1.50 port 2222 ssh2

Jan 22 15:20:20 sshd[12345]: Failed password for user1 from 192.168.1.50 port 2222 ssh2
```

- **Alert**:
    - If this happens, Graylog will send you an email with the details.

Prioritization:

- Low: 1-2 failed attempts.
- Medium: 3-5 failed attempts.
- High: More than 5 failed attempts (potential brute-force attack).

3. Incident Response Scenario

Scenario: Repeated Failed Login Attempts

- **What Happened?**
    - Graylog sends an alert saying someone tried logging in multiple times from 192.168.1.50.

- **Response**:

1. **Block the Attacker**:
    - Use a command to block their IP: sudo iptables -A INPUT -s 192.168.1.50 -j DROP
2. **Secure the System**:
    - Disable password login for SSH and only allow login with SSH keys.
3. **Document the Incident**:
    - Write down what happened, what you did, and how to prevent it in the future.

- **Lessons Learned**:
    - Set up stronger password policies.
    - Add multi-factor authentication for better protection.

Evidence of Functionality

1. **Alert Trigger**:
    - Show a screenshot of the Graylog alert for failed logins.
2. **Response Steps**:
    - Include screenshots or a list of commands used to block the attacker.
3. **Logs**:
    - Save and include a file with example logs showing the failed login attempts.