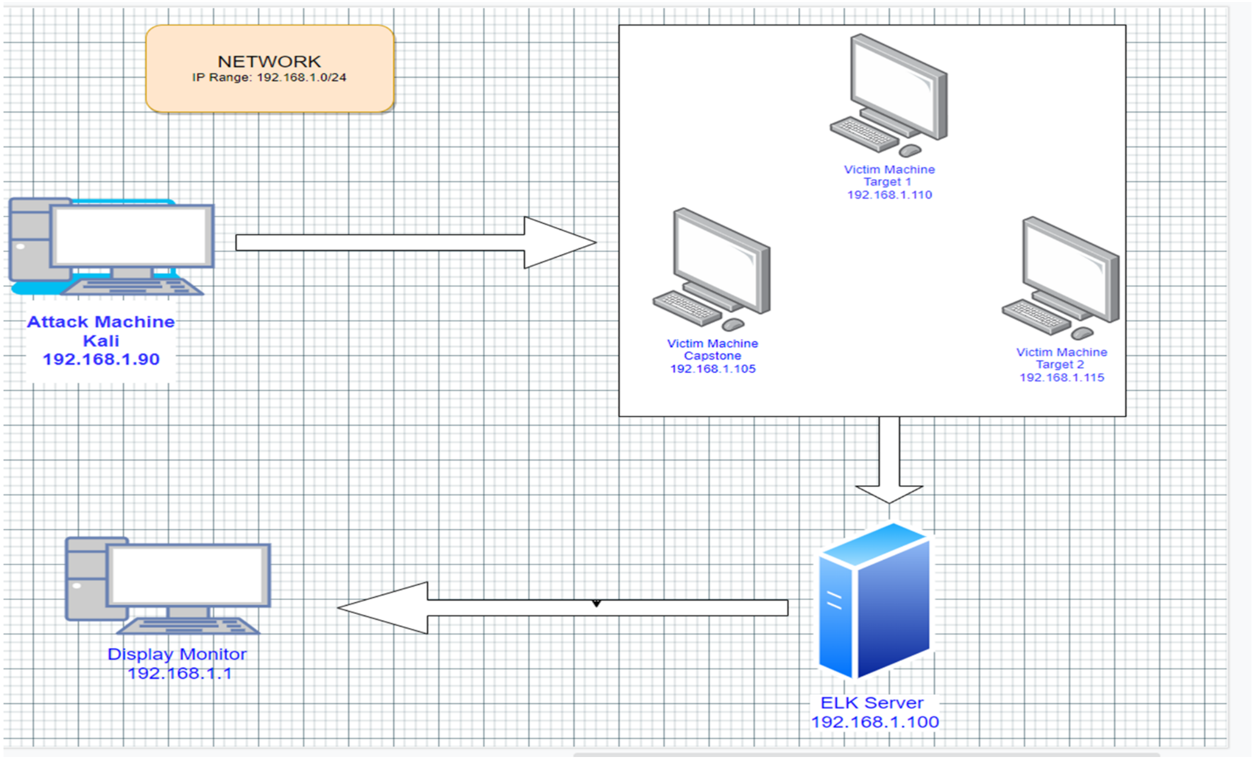
Blue Team: Summary of Operations

Table of Contents

Network Topology



The following machines were identified on the network:

- Kali
  - **Operating System: Linux**
  - **Purpose: Penetration Tester**
  - **IP Address: 192.168.1.90**
- ELK
  - **Operating System: Linux Ubuntu**

    - **Purpose: Log Server**
    - **IP Address:192.168.1.100**
- Capstone
    - **Operating System: Linux**
    - **Purpose: HTTP Server**
    - **IP Address: 192.168.1.105**
- Target 1
    - **Operating System: Linux**
    - **Purpose:**
    - **IP Address:192.168.1.110**

Description of Targets

The target of this attack was: Target 1 (192.168.1.110).

Target 1 is an Apache web server and has SSH enabled, so ports 80 and 22 are possible ports of entry for attackers. As such, the following alerts have been implemented:

Monitoring the Targets

Traffic to these services should be carefully monitored. To this end, we have implemented the alerts below:

Excessive HTTP Errors

Excessive HTTP Errors is implemented as follows:

- **Metric**: http:response.status_code
- **Threshold**: above 400 within last 5 minutes
- **Vulnerability Mitigated**: Failed access attempts
- **Reliability**: High

HTTP Size Request Monitor

HTTP Size Request Monitor is implemented as follows:

- **Metric**: http.request.bytes
- **Threshold**: 3500 hits within last 60 seconds
- **Vulnerability Mitigated**: Port Scans
- **Reliability**: Medium

CPU Usage Monitor

CPU Usage Monitor is implemented as follows:

- **Metric**: system.process.cpu.total.pct

- **Threshold**: .5 usage within last 5 minutes
- **Vulnerability Mitigated**: Target use
- **Reliability**: Medium