# **Blue Team: Summary of Operations**

## **Table of Contents**

* Network Topology
* Description of Targets
* Monitoring the Targets
* Patterns of Traffic & Behavior
* Suggestions for Going Further

### **Network Topology**

*TODO: Fill out the information below.*

The following machines were identified on the network:

* Elk Stack
  + **Operating System**: Linux
  + **Purpose**: Kibana logging
  + **IP Address**: 192.168.1.100
* Capstone
  + **Operating System**: Linux
  + **Purpose**: machine to verify Kibana logging
  + **IP Address**: 192.168.1.105
* Target 1
  + **Operating System**: Linux
  + **Purpose**: apache web server
  + **IP Address**: 192.168.1.110
* Target 2
  + **Operating System**: Linux
  + **Purpose**: apache web server - hardened target
  + **IP Address**: 192.168.1.115
* Kali VM
  + **Operating System**: Linux
  + **Purpose**: red team
  + **IP Address**: 192.168.1.90

### **Description of Targets**

*TODO: Answer the questions below.*

The target of this attack was: Target 1 192.168.1.110 and Target 2 192.168.1.255

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**: greater than 400 count over a 5 minute interval
* **Vulnerability Mitigated**: ddos attacks/http flooding
* **Reliability**: High reliability

#### **HTTP Request Size Monitor**

HTTP Request Size Monitor is implemented as follows:

* **Metric**: metricbeat--http.request.bytes
* **Threshold**: greater than 3500 count in 1 minute interval
* **Vulnerability Mitigated**: DOS attacks
* **Reliability**: High reliability

#### **CPU Usage Monitor**

CPU Usage Monitor is implemented as follows:

* **Metric**: system.process.cpu.total.pct
* **Threshold**: greater than above 0.5 for the last 5 minutes
* **Vulnerability Mitigated**: Excessive CPU usage. Processes running in the background.
* **Reliability**: Medium reliability

### **Suggestions for Going Further (Optional)**

Alerts only detect the attack but they don’t prevent it.

The logs and alerts generated during the assessment suggest that this network is susceptible to several active threats. In addition to watching for occurrences of such threats, the network should be hardened against them. Below are some suggestions.

**Vulnerability 1: Brute Force Attacks**

● Patch: Invalid Credentials Lock out. Limit activity/Whitelist to a specified IP address or range. Monitor server logs. Reroute successful logins to a security question.

● Why It Works: It limits the number of attempts the attacker can commit. Only allows connections from trusted addresses. The extra added step of answering a security question could deter such attacks.

**Vulnerability 2: DOS Attacks**

● Patch: Install a Load Balancer. Also consider using a cloud based service provider.

● Why It Works: It distributes requests across a number of servers which lightens the traffic burden on each server. The cloud based service provider typically has more bandwidth than a private network. It also has software engineers who look specifically for dos attacks

**Vulnerability 3: Excessive CPU Usage**

● Patch: Create different levels of alert for CPU Usage. Limit cpu usage for each of the core operators.

● Why It Works: Different levels of alerts can help monitor CPU usage. An outside company may be needed to install software to help mitigate.