# **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**

Network

Address Range: 192.168.1.0/24

Netmask:

255.255.255.0

Gateway:

192.168.1.10

Machines

IPv4: 192.168.1.90

OS: Kali Linux

Hostname: Kali

IPv4: 192.168.1.100

OS: Ubuntu Linux

Hostname: ELK

IPv4: 192.168.1.105

OS: Ubuntu Linux

Hostname: Capstone

IPv4: 192.168.1.110

OS: Linux

Hostname: Target 1

### **Description of Targets**

*TODO: Answer the questions below.*

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:

#### **CPU threshold Alert**

Alert 1 is implemented as follows:

* **Metric**:system.process.cpu.total
* **Threshold**: >0.5 in the last 5 minutes
* **Vulnerability Mitigated**: DDoS Vulns.
* **Reliability**: early detection is a plus but it would be easy to overload this alert. Consider adjusting after further evaluation, medium reliability

**HTTP request size**

Alert 2 is implemented as follows:

* **Metric**: HTTP request size
* **Threshold**: >3500 over the last 1 minute
* **Vulnerability Mitigated**: Port Scanning
* **Reliability**: High, brute port scanning is easy to detect as long as a proper baseline for the networks traffic is accurate

#### **Excessive HTTP Errors**

Alert 3 is implemented as follows:

* **Metric**: http.response.status.code
* **Threshold**: over top 5 that are over 400 in 5
* **Vulnerability Mitigated**: brute force attacks through failures
* **Reliability**: early detection is a plus but it would be easy to overload this alert. Consider adjusting after further evaluation, medium reliability