**Blue Team: Summary of Operations**

**Table of Contents**

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

**Network Topology**

The following machines were identified on the network:

* Host Machine
  + **Operating System**: Windows 10
  + **Purpose**: Network Host
  + **IP Address**: 192.168.1.1
* Capstone
  + **Operating System**: Ubuntu Linux
  + **Purpose**: LTS Server
  + **IP Address**: 192.168.1.105
* ELK
  + **Operating System**: Ubuntu Linux
  + **Purpose**: ELK (Elasticsearch, Logstash, and Kibana) Stack for logging the network
  + **IP Address**: 192.168.1.100
* Kali
  + **Operating System**: Kali Linux
  + **Purpose**: Attacker Machine
  + **IP Address**: 192.168.1.90
* Target 1
  + **Operating System**: Debian Linux
  + **Purpose**: Web Server
  + **IP Address**: 192.168.1.110
* Target 2
  + **Operating System**: Debian Linux
  + **Purpose**: Web Server
  + **IP Address**: 192.168.1.115

**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. Other open ports include 111, 139, 445.

**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**: packetbeat
* **Threshold**: More than 400 HTTP errors in the past 5 minutes
* **Vulnerability Mitigated**: This alert helps identify brute force attacks
* **Reliability**: It is highly unlikely for this alert to generate any false positives and it is highly reliable

**HTTP Request Size Monitor**

HTTP Request Size Monitor is implemented as follows:

* **Metric**: packetbeat
* **Threshold**: HTTP requests exceeding 3500 bytes for the last 1 minute
* **Vulnerability Mitigated**: Identifies DDOS attacks
* **Reliability**: This alert is of a medium reliability and shouldn’t generate many if any false positives

**CPU Usage Monitor**

CPU Usage Monitor is implemented as follows:

* **Metric**: metricbeat
* **Threshold**: Will fire if the CPU is above 50% utilization for 5 minutes
* **Vulnerability Mitigated**: excessive CPU usage/ poor resource management
* **Reliability**: This alert is of a high reliability and shouldn’t generate any false positives