# **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**

The following machines were identified on the network:

* Kali
  + Operating System: Debian Linux 5.4.0
  + Purpose: Penetration Testing
  + IP Address: 192.168.1.90
* ELK
  + Operating System: Ubuntu 18.04
  + Purpose: The elastic stack (Elasticsearch and Kibana)
  + IP Address: 192.168.1.100
* Target 1
  + Operating System: Debian GNU/Linux 8
  + Purpose: The WordPress Host (Victim)
  + IP Address: 192.168.1.110
* Capstone
  + Operating System: Ubuntu 18.04
  + Purpose: The Vulnerable webserver
  + IP Address: 192.168.1.105

### **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**

Alert 1 is implemented as follows:

* Metric: WHEN count() GROUPED OVER top 5 ‘http.response.status\_code’
* Threshold: IS ABOVE 400 FOR THE LAST 5 MINUTES
* Vulnerability Mitigated: Enumeration/Brute Force
* Reliability: Reliable - Measuring by 400 error codes will filter out any normal access activity. If there are more than 400 errors in 5 minutes we can be sure that an attack is taking place.

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

Alert 2 is implemented as follows:

* Metric: WHEN sum() of http.request.bytes OVER all documents
* Threshold: IS ABOVE 3500 FOR THE LAST 1 minute
* Vulnerability Mitigated: Code Injection in http requests (XSS and CRLF) or DDOS
* Reliability: This alert is prone to false positives. It will require extensive monitoring and adjusting to reach optimal efficiency.

#### **CPU Usage Monitor**

Alert 3 is implemented as follows:

* Metric: WHEN max() OF system.process.cpu.total.pct OVER all documents
* Threshold: IS ABOVE 0.5 FOR THE LAST 5 minutes
* Vulnerability Mitigated: Malicious Software, processes that are running and taking up resources.
* Reliability: This alert is reliable but may sometimes return a false positive. Some adjustment may be required depending on normal cpu use.