# **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:

* Name of VM 1: Kali
  + Operating System:Kali
  + Purpose: Red team usage; use to attack Target 1 and 2
  + IP Address: 192.168.1.90
* Name of VM 2: Target 1
  + Operating System: Linux 3.2-4.9
  + Purpose: Hosts website RavenSecurity
  + IP Address: 192.168.1.110
* Name of VM 3: Target 2
  + Operating System: Linux 3.2-4.9
  + Purpose: Second Box to attack
  + IP Address: 192.168.1.115
* Name of VM 4: ELK
  + Operating System: No scans on NMAP
  + Purpose: Generates logs
  + IP Address: 192.168.1.100
* Name of VM 5: Capstone
  + Operating System: Linux 3.2-4.9
  + Purpose: Practice alerts
  + IP Address: 192.168.1.105

### **Description of Targets**

The target of this attack was: Target 1 (TODO: 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:

#### **Name of Alert 1**

*TODO: Replace Alert 1 with the name of the alert.*

Alert 1 is implemented as follows:

* Metric: HTTP response code
* Threshold: Above 400
* Vulnerability Mitigated: Determines an alert based on http response code.
* Reliability: Medium, depending on how active the site is used. There were a few pings that triggered this alert.

#### **Name of Alert 2**

Alert 2 is implemented as follows:

* Metric: Packetbeat: HTTP request bytes threshold
* Threshold: 3500
* Vulnerability Mitigated: Data accessing thresholds.
* Reliability: Low: The majority of alerts, if I am correctly reading my Kibana, is from request bytes.

#### **Name of Alert 3**

Alert 3 is implemented as follows:

* Metric: Metricbeat: CPU process power
* Threshold: Over 0.5%
* Vulnerability Mitigated: Mitigates excessive task power which might seem abnormal to regular functions.
* Reliability: High: most of the pings were of less than .3% of cpu utilization.