# **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:

* Attacker
  + Operating System: Kali
  + Purpose: Gain access to targets
  + IP Address: 192.168.1.90
* Capstone
  + Operating System:
  + Purpose:
  + IP Address: 192.168.1.105
* ELK
  + Operating System:
  + Purpose:
  + IP Address: 192.168.1.100
* Target 1
  + Operating System: Apache Web Server
  + Purpose: Target
  + IP Address: 192.168.1.110
* Target 2
  + Operating System:
  + Purpose: Target
  + 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. 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: packetbeat-\*
* Threshold: Is above 400 for the last 5 minutes
* Vulnerability Mitigated: Alerts developer if a rapid increase of failure codes or success codes is seen.
* Reliability: Medium reliability; Due to the fact that when investigating the packets you can see the target URI and issued response code.

#### **HTTP request size monitor**

Alert 2 is implemented as follows:

* Metric: packetbeat-\*
* Threshold: Is above 3500 for the last minute
* Vulnerability Mitigated: DoS attack alerting and manual mitigation
* Reliability: Medium reliability; Manual investigation would be needed to determine the legitimacy of inbound traffic.

#### **CPU Usage Monitor**

Alert 3 is implemented as follows:

* Metric: metricbeat-\*
* Threshold: Is above 0.5 for the last 5 minutes
* Vulnerability Mitigated: Malware alerting
* Reliability: Low reliability; Due to how the computer resources work, the CPU will spike any time a process starts up or if an intensive process is being run.