# 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 Kali 5.4.0

Purpose:

Red Team - Pen Tester

IP Address:

192.168.1.90

- ELK

Operating System:

Ubuntu 18.04

Purpose:

ELK Stack

IP Address:

192.168.1.100

- Target 1

Operating System:

Debian GNU/Linux 8

Purpose:

WordPress

IP Address:

192.168.1.110

- Capstone

Operating System:

Ubuntu 18.04

Purpose:

Filebeat/Metricbeat Web Server

IP Address:

192.168.1.105

### Description of Targets

The target of this attack was: 192.168.1.110 (Target 1).

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:

- Excessive HTTP Errors

Metric: WHEN count() GROUPED OVER top 5'http.response.status\_code'

Threshold: IS ABOVE 400 FOR THE LAST 5 minutes

Vulnerability: Brute Force

Reliability: Should not generate false positives or negatives. High reliability.

- HTTP Request Size Monitor

Metric: WHEN sum() of http.request.bytes OVER all documents Threshold: IS ABOVE 3500 FOR THE LAST 1 minute

Vulnerability: DDoS or Injection

Reliability: Could create some false positives. Medium reliability.

- CPU Usage Monitor

Metric: WHEN max() OF system.process.cpu.total.pct OVER all documents

Threshold: IS ABOVE 0.5 FOR THE LAST 5 minutes

Reliability: This should not create much in the way of false positives. This should be a High reliability.