# 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:

- Name of VM 1 Kali

- \*\*Operating System\*\*: Linux

- \*\*Purpose\*\*: Used as attacking machine

- \*\*IP Address\*\*:192.168.1.110

- Name of VM 2 Capstone

- \*\*Operating System\*\*: Linux

- \*\*Purpose\*\*: Used as testing system for alerts

- \*\*IP Address\*\*:192.168.1.105

- Name of VM 2 ELK

- \*\*Operating System\*\*: Linux

- \*\*Purpose\*\*: Used for gathering information from the victim machine using Metricbeat,

Filebeats, and Packetbeats

- \*\*IP Address\*\*:192.168.1.100

- Name of VM 2 Target 1

- \*\*Operating System\*\*: Linux

- \*\*Purpose\*\*: The VM with Wordpress as a vulnerable server

- \*\*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

Excessive HTTP Errors is implemented as follows:

- \*\*Metric\*\*: http.response.status\_code > 400

- \*\*Threshold\*\*: grouped http response status codes above 400 every 5 minutes

- \*\*Vulnerability Mitigated\*\*:

1. Utilized intrusion detection/prevention for attacks

2. IPS would block any suspicious IP’s

3. Utilize Account Management to lock or request user accounts to change the passwords every 60 days

4. Filter and disable or close port 22

- \*\*Reliability\*\*: No, this alert will not generate an excessive amount of false positives identifying brute force attacks.

#### #### CPU Usage Monitor

Cpu usage monitor is implemented as follows:

- \*\*Metric\*\*: system.process.cpu.total.pct

- \*\*Threshold\*\*: The maximum cpu total percentage is over .5 in 5 minutes

- \*\*Vulnerability Mitigated\*\*: Controlling the CPU usuage percentage at 50%, it will trigger a memory alert only if CPU remains at or above 50% consistently for 5 minutes.

- \*\*Reliability\*\*: Yes, this alert can generate a lot of false positives due to CPU spikes occurring when specific integrations are initiated at the start of processing.

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

Http request size monitor is implemented as follows:

- \*\*Metric\*\*: http.request.bytes

- \*\*Threshold\*\*: The sum of the requested bytes is over 3500 in 1 minute

- \*\*Vulnerability Mitigated\*\*: By controlling the number of http request size through a filter, protection is enabled to detect or prevent against DDOS attacks for IPS/IDS.

- \*\*Reliability\*\*: No, this alert doesn't generate an excessive amount of false positives because DDOS attacks submit requests within seconds not within minutes.