# **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:

* Target 1
  + **Operating System**: Linux
  + **Purpose**: Expose vulnerable WordPress server
  + **IP Address**: 192.168.1.110
* Target 2
  + **Operating System**: Linux
  + **Purpose**: Target 2
  + **IP Address**: 192.168.1.115
* Kali
  + **Operating System**: Kali Linux
  + **Purpose**: Penetration test machine
  + **IP Address**: 192.168.1.90
* Capstone
  + **Operating System**: Ubuntu 18.04.1
  + **Purpose**: Alert testing / Attack target
  + **IP Address**: 192.168.1.105
* ELK
  + **Operating System**: Ubuntu 18.04.4
  + **Purpose**: Elasticsearch and Kibana stack
  + **IP Address**: 192.168.1.100

### **Description of Targets**

*TODO: Answer the questions below.*

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**: http.response.status\_code
* **Threshold**: Above 400 for last 5 minutes
* **Vulnerability Mitigated**: Brute Force Attacks
* **Reliability**: High Reliability

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

Alert 2 is implemented as follows:

* **Metric**: http.request.bytes
* **Threshold**: Above 3500 for last 1 minute
* **Vulnerability Mitigated**: DoS (Denial of service) attacks
* **Reliability**: High reliability.

#### **CPU Usage Monitor**

Alert 3 is implemented as follows:

* **Metric**: system.process.cpu.total.pct
* **Threshold**: Above 0.5 for last 5 minutes
* **Vulnerability Mitigated**: Excessive CPU usage
* **Reliability**: Medium reliability.

*TODO Note: Explain at least 3 alerts. Add more if time allows.*

### **Suggestions for Going Further (Optional)**

*TODO*:

* Each alert above pertains to a specific vulnerability/exploit. Recall that alerts only detect malicious behavior, but do not stop it. For each vulnerability/exploit identified by the alerts above, suggest a patch. E.g., implementing a blocklist is an effective tactic against brute-force attacks. It is not necessary to explain *how* to implement each patch.

The logs and alerts generated during the assessment suggest that this network is susceptible to several active threats, identified by the alerts above. In addition to watching for occurrences of such threats, the network should be hardened against them. The Blue Team suggests that IT implement the fixes below to protect the network:

* Vulnerability 1: Brute Force Attacks
  + **Patch**: Install WordPress Updates, Use WordPress plugins, Two-Factor authentication
  + **Why It Works**: Some brute force attacks target known vulnerabilities in older versions of WordPress. Updating often can help prevent use of these vulnerabilities. Firewall can help to limit amount of traffic. Two-Factor authentication can add additional protection even if a password is cracked.
* Vulnerability 2: DoS Attacks
  + **Patch**: Disable XML RPC in WordPress, Disable REST API in WordPress, Anti-DOS plugins
  + **Why It Works**: Disabling XML RPC will not allow 3rd party apps to interact with WordPress, Disabling REST APIT remove the ability for plugins to access WordPress data, update content, and/or delete it. Plugins can also be used to disable XML-RPC and WP REST API
* Vulnerability 3: Excessive CPU usage
  + **Patch**: TODO: Update WordPress, Update plugins, Install a caching plugin
  + **Why It Works**: Making sure WordPress and related plugins are updated can help reduce CPU usage, Installing caching plugins can reduce CPU load by caching static copies of your pages.