# **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:

* Azure Labs Machine
  + **Operating System**: Windows 10
  + **Purpose**: Windows Hyper-V Host
  + **IP Address**:192.168.1.1
* Kali
  + **Operating System**: Kali
  + **Purpose**: Attack Box
  + **IP Address**: 192.168.1.90
* Elk
  + **Operating System**: Ubuntu
  + **Purpose**: ELK
  + **IP Address**: 192.168.1.100
* Capstone
  + **Operating System**: Ubuntu
  + **Purpose**:?
  + **IP Address**: 192.168.1.105
* Target 1
  + **Operating System**: Debian
  + **Purpose**: Target 1
  + **IP Address**: 192.168.1.110
* Target 2
  + **Operating System**: Debian
  + **Purpose**: Target 2
  + **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**

Excessive HTTP Errors is implemented as follows:

* **Metric**: http.response.status\_code
* **Threshold**: > 400 in the last 5 minutes
* **Vulnerability Mitigated**: Bruteforce password attacks or directory scanning
* **Reliability**: Accurate given the threshold set correctly for normal operation with slight overhead buffer for normal usage growth. Threshold should be checked periodically to ensure the value is still logical for the purpose.

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

HTTP Request Size Monitor is implemented as follows:

* **Metric**: http.request.bytes
* **Threshold**: > 3500 in the last minute
* **Vulnerability Mitigated**: Abnormally large file access, potential remote execution
* **Reliability**: Accurate given the threshold set correctly for normal operation with slight overhead buffer for normal usage growth. Threshold should be checked periodically to ensure the value is still logical for the purpose.

#### **CPU Usage Monitor**

CPU Usage Monitor is implemented as follows:

* **Metric**: system.process.cpu.total.pct
* **Threshold**: > 50% for the last 5 minutes
* **Vulnerability Mitigated**: Network scanning or excessive resource hogging due to dos or slow loris attack
* **Reliability**: Relatively accurate under normal operating circumstances however false positives generated during startup and shutdown and during anytime the machine is under abnormal load eg. updating software packages.

### 

### **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
  + **Patch**: TODO: E.g., *install special-security-package with apt-get*
  + **Why It Works**: TODO: E.g., *special-security-package scans the system for viruses every day*
* Vulnerability 2
  + **Patch**: TODO: E.g., *install special-security-package with apt-get*
  + **Why It Works**: TODO: E.g., *special-security-package scans the system for viruses every day*
* Vulnerability 3
  + **Patch**: TODO: E.g., *install special-security-package with apt-get*
  + **Why It Works**: TODO: E.g., *special-security-package scans the system for viruses every day*