# **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
  + **Operating System**: Kali Linux 2.6.32
  + **Purpose**: Attacking Machine
  + **IP Address**: 192.168.1.90
* Name of VM 2
  + **Operating System**: Ubuntu 18.04.4
  + **Purpose**: ELK used for the aggregation of logs on all devices
  + **IP Address**: 192.168.1.100
* Name of VM 3
  + **Operating System**: Ubuntu 18.04.01
  + **Purpose**: Capstone acting as another webserver
  + **IP Address**: 192.168.1.105
* Name of VM 4
  + **Operating System**: Linux 3.2 - 4.9
  + **Purpose**: Target machine 1 apache webserver
  + **IP Address**: 192.168.1.110
* Name of VM 5
  + **Operating System**: Linux 3.2 - 4.9
  + **Purpose**: Target machine 2 apache webserver
  + **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:

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

#### Alert 1 is implemented as follows:

* **Metric**: http.request.bytes w/ packetbeat
* **Threshold**: when the sum of HTTP request bytes exceeds 3500 in 1 minute
* **Vulnerability Mitigated**: The Alarm is set to monitor scans for payloads or malicious files
* **Reliability**: Low Reliability. This alarm will catch those trying to send malicious files, but without a baseline of normal packets, this alarm may not be reliable.

#### **Excessive HTTP Errors**

Alert 2 is implemented as follows:

* **Metric**: http.response.status\_code w/metricbeat
* **Threshold**: When the count of the top 5 HTTP response codes is above 400 FOR THE LAST 5 minutes
* **Vulnerability Mitigated**: The Vulnerability meant to be mitigated is Bruce Force attacks
* **Reliability**: High Reliability. This alert is has a threshold that will catch brute force attacks and won’t trigger off of an accidental password fail from a user.

#### **CPU Usage Monitor**

Alert 3 is implemented as follows:

* **Metric**: system.process.cpu.total.pct w/filebeat
* **Threshold**: When the system CPU totals over 50% within the last 5 minutes (0.5 FOR THE LAST 5 minutes)
* **Vulnerability Mitigated**: This Alarm is mitigation against Dos attacks
* **Reliability**: Medium Reliability. This alarm will trigger in the event of a Dos attack but also high Website usage.

### 

### **Suggestions for Going Further**

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- **OpenSSH**
  + **Patch**: Disable this service and implement a VPN instead
  + **Why It Works**: Disabling the ssh service will prevent unauthorized users from remotely accessing the webserver. A VPN will still allow for remote connection but only from authorized users and in a more secure way.
* Vulnerability 2 - **Privilege Escalation**
  + **Patch**: Remove unnecessary users from the sudoer permissions file, and install a monitor for attempts to run root privileges.
  + **Why It Works**: Preventing an unnecessary user from using Sudo privileges reduces the risk of privilege escalation. A monitor system will help alert against possible compromised accounts.
* Vulnerability 3 - **Weak Password**
  + **Patch**: Implement a strong password policy for all users
  + **Why It Works**: By creating a strong password policy, accounts with crucial information will be less likely to become compromised. The password should be changed frequently and be strong enough to prevent guessing or a brute force attack.