**Blue Team: Summary of Operations**

Madeleine Simpson

**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:**

**Host Name: Target 1:**

**OS:** Linux

**IP:** 192.168.1.110

**Host Name: Target 2**

**OS:** Linux

**IP:** 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 Errors
* Threshold: above 400 for the last 5 minutes
* Vulnerability Mitigated: Brute Force Attacks
* Reliability: High

**HTTP Request Size Monitor**

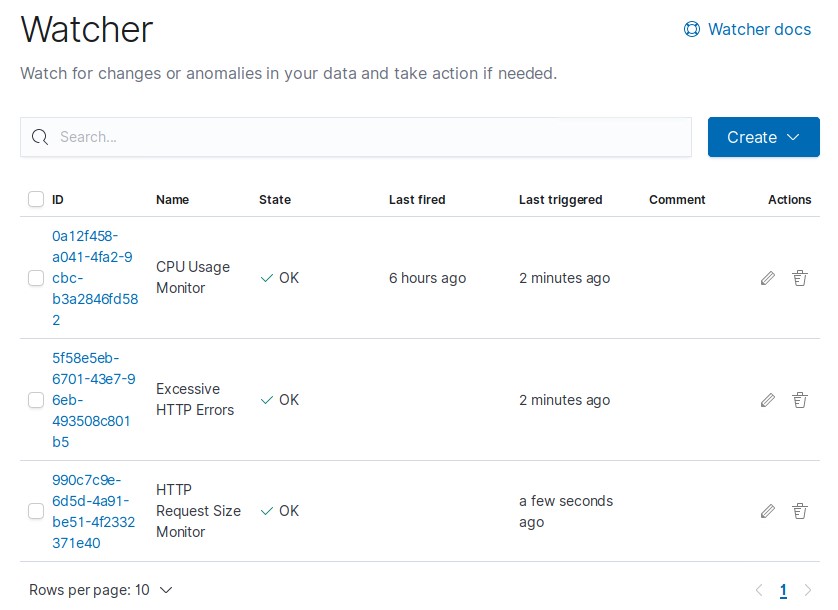
‘HTTP Request Size Monitor’ is implemented as follows:

* Metric: http.request.bytes
* Threshold: above 3500 for the last minute
* Vulnerability Mitigated: DOS (Denial of Service) attacks
* Reliability: High

**CPU Usage Monitor**

‘CPU Usage Monitor’ is implemented as follows:

* Metric: system.process.cpu.total.pct
* Threshold: above 0.5 for the last 5 minutes
* Vulnerability Mitigated: Resource management, excessive CPU usage
* Reliability: Medium



**Suggestions for Going Further**

- 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.

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:** : Invalid Credentials Lockout Threshold. Lock accounts after 10 failed logins.
* **Why It Works:** : Limits amount of attempts an attacker can make to crack logins through brute force.

**- Vulnerability 2: DOS Attacks**

* **Patch:** : Load Balancer
* **Why It Works:** : Distributes requests across multiple servers thereby lightening traffic burden on each respective server.

**- Vulnerability 3: Excessive CPU Usage**

* **Patch:** : Limit max allowable CPU usage for each core
* **Why It Works:** : Prevents CPU usage exceeding pre-set levels, thereby preventing excessive usage.