# 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:

- Name of VM 1

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

- \*\*Purpose\*\*: First Target

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

### Description of Targets

\_TODO: Answer the questions below.\_

The target of this attack was: `Target 1` 192.168.1.110

Target 1 is a 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 Reliability



**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: Denial of Service Attacks.
* Reliability: High Reliability.



**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: Excessive CPU Usage
* Reliability: Medium Reliability.



### 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. 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: Invalid Credentials Lock out.
* Why It Works: It limits the number of attempts the attacker can commit.

**Vulnerability 2: DOS Attacks**

* Patch: Deploy a Load Balancer
* Why It Works: Distributes connection to a number of servers to reduce the load

**Vulnerability 3: Excessive CPU Usage**

* Patch: Limit max cpu usage for each core.
* Why It Works: To avoid server resource constraints and failure of server functionality due to server utilization