**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:

* Windows
  + **Operating System**: Windows
  + **Purpose**: Host of all virtual machines
  + **IP Address**: 192.168.1.1
* Elk
  + **Operating System**: Linux
  + **Purpose**: Data monitoring of traffic between other machines
  + **IP Address**: 192.168.1.100
* Kali
  + **Operating System**: Linux
  + **Purpose**: Machine we will be attacking with
  + **IP Address**: 192.168.1.90
* Target1
  + **Operating System**: Linux
  + **Purpose**: Machine we will be attacking
  + **IP Address**: 192.168.1.110

**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:

**Name of Alert 1:** HTTP Request Size Monitor

Alert 1 is implemented as follows:

* **Metric**: When sum() OF http.request.bytes OVER all documents IS ABOVE 3500 FOR THE LAST 1 minute
* **Threshold**: 3500 bytes
* **Vulnerability Mitigated**: Port scanning
* **Reliability**: Pretty reliable because you see big spikes in network traffic when performing a port scan

**Name of Alert 2:** Excessive HTTP Errors

Alert 2 is implemented as follows:

* **Metric**: WHEN count() GROUPED OVER top 5 ‘http.response.status\_code’ IS ABOVE 400 FOR THE LAST 5 minutes
* **Threshold**: 400
* **Vulnerability Mitigated**: Brute force attacks
* **Reliability**: Low reliability. No alerts were discovered; we will adjust the thresholds using the 50% technique. The threshold will be lowered by 50% each time until a reliable threshold is reached.

**Name of Alert 3:** CPU Usage Monitor

Alert 3 is implemented as follows:

* **Metric**: WHEN max() OF system.process.cpu.total.pct OVER all documents IS ABOVE 0.5 FOR THE LAST 5 minutes
* **Threshold**: 50%
* **Vulnerability Mitigated**: Finds programs that may be misusing resources
* **Reliability**: Not reliable because our CPU usage is so low, usage is running between 1 and 2 percent. We suggest changing the threshold to 0.0125 (12.5%) CPU usage.