**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:

* VM 1 Target 1
  + **Operating System**: Linux
  + **Purpose**: Target 1
  + **IP Address**: 192.168.1.110
* VM 2 ELK
  + **Operating System**: Linux
  + **Purpose**: Collects information from servers
  + **IP Address**: 192.168.1.100
* VM 3 Kali
  + **Operating System**: Linux
  + **Purpose**: Attacker
  + **IP Address**: 192.168.1.90
* VM 4 Capstone
  + **Operating System**: Linux
  + **Purpose**: Test Machine
  + **IP Address**: 192.168.1.105

**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***

Alert 1 is implemented as follows:

* **Metric**: Packetbeat
* **Threshold**: WHEN count() GROUPED OVER top 5’http.response.status\_code’ IS ABOVE 400 FOR THE LAST 5 minutes
* **Vulnerability Mitigated**: Identifies an abnormal number of http error codes in a 5 minute
* **Reliability**: Medium: This alert will not generate an excessive number of false positives/false negatives.

***HTTP Request Size Monitor***

Alert 2 is implemented as follows:

* **Metric**: Packetbeat
* **Threshold**: WHEN sum() of http.request.bytes OVER all documents IS ABOVE 3500 FOR THE LAST 1 minute
* **Vulnerability Mitigated**: This alert will alarm if there is DDoS attack.
* **Reliability**: Medium: This generally does not cause excessive false positives since the number of requests would have to be large amount.

***CPU Usage Monitor***

Alert 3 is implemented as follows:

* **Metric**: Metricbeat
* **Threshold**: WHEN max() OF system.process.cpu.total.pct OVER all documents IS ABOVE 0.5 FOR THE LAST 5 minutes.
* **Vulnerability Mitigated**: This alert will alarm if the CPU is above 0.5 for 5 minutes. High CPU usage could be indicative of an attack, virus or malware.
* **Reliability**: Low: Yes, this alert can trigger false alarms whenever the CPU fluctuates over 0.5 for 5 minutes.