**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:

* Attacker Machine
  + **Operating System**: Kali Linux
  + **Purpose**: Attacking Machine
  + **IP Address**:192.168.1.90
* ELK Stack
  + **Operating System**: Linux Ubuntu
  + **Purpose**: Feeding logs to Kibana
  + **IP Address**:192.168.1.100
* Target 1
  + **Operating System**: Linux
  + **Purpose**: Wordpress Host
  + **IP Address**:192.168.1.110
* Target 2
  + **Operating System**: Linux
  + **Purpose**: Wordpress Host
  + **IP Address**:192.168.1.115

**Description of Targets**

The target of this attack was: 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**

**CPU Usage Monitor**

Alert 1 is implemented as follows:

* **Metric**: WHEN max() OF system.process.cpu.total.pct OVER
* **Threshold**: .5 FOR last 5 minutes
* **Vulnerability Mitigated**: TODO
* **Reliability**: Medium. Not entirely accurate. The alert could be triggered when users are using more cpu to perform tasks. Not indication of an attack.

**Excessive HTTP Errors**

Alert 2 is implemented as follows:

* **Metric**: WHEN count () GROUPED OVER 5 ‘http.response.status.code
* **Threshold**: IS ABOVE 400 FOR LAST 5 MINUTES
* **Vulnerability Mitigated**: Potential Brute forcing
* **Reliability**: High Reliability. This alert is very reliable based on the amount of errors generated. Would be indication of brute force attack.

**HTTP Request Size Monitor**

Alert 3 is implemented as follows:

* **Metric**: WHEN sum() OF http.request.bytes OVER all documents
* **Threshold**: IS ABOVE 3500 FOR THE LAST 1 minute
* **Vulnerability Mitigated**: excessive sized file activity on network.
* **Reliability**: Medium. This alert may not be entirely accurate depending on what users are performing.