**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:

* Network
  + **Operating System**: Windows 10 Pro
  + **Purpose**: Hosts the Hyper V Network which hosts the other virtual machines
  + **IP Address**: 192.168.1.1
* Kali
  + **Operating System**: Kali Linux
  + **Purpose**: Used to launch attacks on other virtual machines (Target 1 and Target 2)
  + **IP Address**: 192.168.1.90
* ELK
  + **Operating System**: Ubuntu
  + **Purpose**: Hosts the ELK Stack and Kibana which can be used to view logs and data.
  + **IP Address**: 192.168.1.100
* Capstone
  + **Operating System**: Ubuntu
  + **Purpose**: Not used
  + **IP Address**: 192.168.1.105
* Target 1
  + **Operating System**: Debian
  + **Purpose**: First target of the Kali attack which hosts an Apache web server with WordPress
  + **IP Address**: 192.168.1.110
* Target 2
  + **Operating System**: Debian
  + **Purpose**: Second target of the Kali attack
  + **IP Address**: 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 Monitor**

Excessive HTTP Errors Monitor is implemented as follows:

* **Metric**: Packetbeat
* **Threshold**: HTTP response code >400 in 5 minutes
* **Vulnerability Mitigated**: Stealth exploitation of Enumerating Wordpress
* **Reliability**: Medium, there are a few false positives generated

**HTTP Request Size Monitor**

HTTP Request Size Monitor is implemented as follows:

* **Metric**: Packetbeat
* **Threshold**: >3500 per 1 minute
* **Vulnerability Mitigated**: Stealth Exploitation of Port Scanning
* **Reliability**: TODO: Does this alert generate lots of false positives/false negatives? Rate as low, medium, or high reliability.

**CPU Usage Monitor**

CPU Usage Monitoris implemented as follows:

* **Metric**: Packetbeat
* **Threshold**: >0.5 in 5 minutes
* **Vulnerability Mitigated**: DoS attack, running malicious scripts
* **Reliability**: Medium, there are a few false positives generated