**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:

* Hyper-V Manager

ML-REFVM-684427

* Name of VM 1: Kali
  + **Operating System**: kali linux machine
  + **Purpose**: Penetration test
  + **IP Address**: 192.168.1.90
* Name of VM 2: Capstone
  + **Operating System**: Linux
  + **Purpose**: Test Alerts
  + **IP Address**: 192.168.1.105
* Name of VM3: Elk
  + **Operating System**: Linux
  + **Purpose**: Set up Alerts
  + **IP Address**: 192.168.1.100
* Name of VM4: Target 1
  + **Operating System**: Linux
  + **Purpose**: Exposes a vulnerable WordPress server
  + **IP Address**: 192.168.1.110
* Name of VM5: Target 2
  + **Operating System**: Linux

**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**: WHEN count() GROUPED OVER top 5 'http.response.status\_code' IS ABOVE 400 FOR THE LAST 5 minutes
* **Threshold**: Above 400
* **Vulnerability Mitigated**: Brute force attacks
* **Reliability**:High Reliability since the threshold is set above 400, it will not generate false positives.

**HTTP Request Size Monitor**

Alert 2 is implemented as follows:

* **Metric**: WHEN sum() of http.request.bytes OVER all documents IS ABOVE 3500 FOR THE LAST 1 minute
* **Threshold**: Above 3500
* **Vulnerability Mitigated**: Prevent DDoS attacks
* **Reliability**: High Reliability since it doesn’t generate false positives**.**

**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**: Above 0.5
* **Vulnerability Mitigated**: CPU usage at 50% for the last 5 mins
* **Reliability**: Medium Reliability since it creates false positives.

**Alert Explanation**:

**Excessive HTTP Errors**

* It works by blocking request to users helps mitigate against user enumeration attacks.
* Easy way to implement patches or fixes to exploits/vulnerabilities.

**HTTP Request Size Monitor**

* It helps protect against malicious data
* Setting Limits can include a number of things:
  + Maximum URL Length
  + Maximum length of a query string
  + Maximum size of a request
* Implementation of HTTP Request Limit on the web server

**CPU Usage Monitor**

* The antiviruses specialize in removal, detection and overall prevention of malicious threats against computers.
  + Any modern antivirus usually covers more than viruses and are a robust solution to protecting a computer in general.
* HIDS monitors and analyzes internals of computing systems.
  + They also monitor and analyze network packets.