# **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:

* ML-RefVm-684427
  + Operating System: Windows 10
  + Purpose: Hosts the Hyper-V manager which containers the other VMs. Also used to view Kibana
  + IP Address: 192.168.1.1
* Capstone
  + Operating System: Ubuntu 18.04.1 LTS
  + Purpose: No purpose for this project.
  + IP Address: 192.168.1.105
* ELK
  + Operating System: Ubuntu 18.04.1 LTS
  + Purpose: Responsible for logging and unloading data to Elasticsearch for review with Kibana. Hosts the ELK stack.
  + IP Address: 192.168.1.100
* Kali
  + Operating System: Kali GNU/Linux Rolling
  + Purpose: Used to orchestrate attacks on the other VMs (Target 1 and Target 2)
  + IP Address: 192.168.1.90
* Target1
  + Operating System: Debian GNU/Linux 8
  + Purpose: Hosts an Apache web server with WordPress. Main victim of Kali attacks.
  + IP Address: 192.168.1.110
* Target2
  + Operating System: Debian GNU/Linux 8
  + Purpose: Secondary target for Kali attacks (if time permits).
  + 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:

#### **Nmap Watcher**

“Nmap Watcher” is implemented as follows:

* Metric: destination.port
* Threshold: Over 17,000,000 for the last 10 seconds
* Vulnerability Mitigated: Port scans
* Reliability: Medium: Some scans are missed. High traffic could result in false positives

#### **Excessive HTTP Errors**

“Excessive HTTP Errors” is implemented as follows:

* Metric: http.response.status\_code
* Threshold: above 400 in last 5 minutes
* Vulnerability Mitigated: Brute force attack
* Reliability: Medium: Generates a few false positives.

#### **CPU Usage Monitor**

“CPU Usage Monitor” is implemented as follows:

* Metric: system.process.cpu.total.pct
* Threshold: over 0.5 in the last 5 minutes
* Vulnerability Mitigated: DoS attack, malicious/irregular software or scripts are being run on the server.
* Reliability: Medium: Generates few false positives

#### **SSH Alert**

“SSH Alert” is implemented as follows:

* Metric: system.auth.ssh.event
* Threshold: over 0 for the last 1 minute
* Vulnerability Mitigated: Potentially malicious actors accessing systems through ssh
* Reliability: Medium: Also alerts when non-malicious actors use ssh