# Leslie Kahler

Cybersecurity Bootcamp

Final Project

September 8, 2021

# 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:

* Windows 10 Hypervisor
  + Operating System: Windows 10 Pro
  + Purpose: Hypervisor
  + IP Address: 192.168.1.1
* ELK
  + Operating System: Ubuntu Linux
  + Purpose: SIEM/IDS - ELK Stack
  + IP Address: 192.168.1.100
* Target 1
  + Operating System: Debian Linux
  + Purpose: Web Server
  + IP Address: 192.168.1.110
* Target 2
  + Operating System: Debian Linux
  + Purpose: Web Server
  + 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:

#### Excessive HTTP Errors

#### HTTP Request Size Monitor

#### CPU Usage Monitor

### **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: http.response.status\_code > 400
  + Threshold: 5 in the last 5 minutes
  + Vulnerability Mitigated: This alert will notify of a potential attack and act according to the incident response plan. This may include blocking the IP or changing authorization credentials.
  + Reliability: High reliability, very few false positives

#### HTTP Request Size Monitor

* Alert 2 is implemented as follows:
  + Metric: HTTP.request.bytes
  + Threshold: 3500 in the last 1 minute
  + Vulnerability Mitigated: Since this will notify when the HTTP request size is larger than 3500 bytes, it can help alert when a DDoS attack is in progress
  + Reliability: High reliability, very few false positives

CPU Usage Monitor

Alert 3 is implemented as follows:

* Metric: system.process.cpu.total.pct
* Threshold: 0.5 in last 5 minutes
* Vulnerability Mitigated: This will trigger an alert when CPU usage rises above 50%, which could indicate malware.
* Reliability: Low reliability, since CPU usage is not indicative of an attack, it can trigger when any resource-intensive process is running.

### **Suggestions for Going Further (Optional)**

* Each alert above pertains to a specific vulnerability/exploit. Recall that alerts only detect malicious behavior, but do not stop it. For each vulnerability/exploit identified by the alerts above, suggest a patch. E.g., implementing a blocklist is an effective tactic against brute-force attacks. It is not necessary to explain how to implement each patch.
  + The logs and alerts generated during the assessment suggest that this network is susceptible to several active threats, identified by the alerts above. In addition to watching for occurrences of such threats, the network should be hardened against them. The Blue Team suggests that IT implement the fixes below to protect the network:
* Vulnerability 1 - Excessive HTTP Errors
  + Patch: Require a stronger password policy in the user account settings, or require public key authentication in addition. Update the account password policy in Windows group policy through /etc/security/pwquality.conf or /etc/security/pwquality.conf in Linux
  + Why It Works: By having a strong password, the IT team can reduce the likelihood that a password can be easily guessed. With public-key authentication also implemented, we can further reduce the likelihood of a brute force attack.
* Vulnerability 2 - HTTP Request Size Monitor
  + Patch: The IT team could implement an intrusion prevention system or intrusion detection system on the network.
  + Why It Works: Since DDoS attacks are extremely complex and diverse, it is difficult to implement only one tool to automatically respond to such an attack. With proper baselining, it will be possible for the IPS or IDS to alert or notify based on the fact that they perform deep packet analysis to see if the traffic is legitimate or not.
* Vulnerability 3 - CPU Usage Monitor
  + Patch: Implement a host-based intrusion prevention system, a common feature on modern anti-virus programs
  + Why It Works: Similar to a network-based IPS, these will perform deep packet analysis to prevent malware from installing or running on the client's computer, which may steal computer resources causing the CPU usage to spike.