# Blue Team: Summary of Operations

### Table of Contents

### Network Topology

The following machines were identified on the network:

- Hypervisor / Host Machine (Not a VM)
- Operating System: Microsoft Windows
- Purpose: Hypervisor / Gateway
- IP Address: 192.168.1.1

**ELK**

- Operating System: Linux
- Purpose: Elasticsearch, Logstash, Kibana Server
- IP Address: 192.168.1.100

Capstone

- Operating System: Linux
- Purpose: Basic HTTP Server (this is a red herring)
- IP Address: 192.168.1.105

**Target 1**

- Operating System: Linux
- Purpose: HTTP Server (also wordpress site)
- IP Address: 192.168.1.110

## 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:

### HTTP ERRORS

Alert 1 is implemented as follows:

- Metric: http.response.status_code > 400
- Threshold: 5 in last 5 minutes
- Vulnerability Mitigated: By creating an alert, the security team can identify attacks & block the ip, change the password, & close or filter the port 22
- Reliability: No, this alert does not generate a lot of false positives. This alert is highly reliable in identifying brute force attacks.

### HTTP Request Size Monitor

Alert 2 is implemented as follows:

- Metric: http.request.bytes
- Threshold: 3500 in last 1 minute
- Vulnerability Mitigated: By controlling the number of http request size through a filter it
- protects against DDOS attacks
- Reliability: No, this alert doesn't generate a lot of false positives bc it is reliable.

### CPU Usage Monitor

Alert 3 is implemented as follows:

- Metric: system.process.cpu.total.pct
- Threshold: 0.5 in last 5 minutes
- Vulnerability Mitigated: By controlling the CPU usage percentage at 50%, it will trigger a memory dump of stored information is generated
- Reliability: Yes this alert can generate a lot of false positives bc the cpu can spike even if there is not an attack.

### 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. Update the account password policy in Windows group policy through /etc/security/pwquality.conf & through /etc/security/pwquality.conf in Linux
- Why It Works: By having a strong password it will be almost impossible to guess or brute force

**Vulnerability 2 - HTTP Request Size Monitor**

- Patch: Use advanced intrusion prevention and threat management systems, which combine firewalls, VPN, anti-spam, content filtering, load balancing, and other layers of DDoS defense techniques. Together they enable constant and consistent network protection to prevent a DDoS attack from happening. This includes everything from identifying possible traffic inconsistencies with the highest level of precision in blocking the attack
- Why It Works: Given the complexity of DDoS attacks, there’s hardly a way to defend against them without appropriate systems to identify anomalies in traffic and provide instant response. Backed by secure infrastructure and a battle-plan, such systems can minimize the threat.

**Vulnerability 3 - CPU Usage Monitor**

- Patch: Use Host Instrusion Prevention System to identify DOS attack
- Why It Works: This stops malware by monitoring the behavior of code