# Blue Team: Summary of Operations

## Table of Contents

* Network Topology
* Description of Targets
* Monitoring the Targets
* Patterns of Traffic and Behavior
* Suggestions for Going Further

## Network Topology

The following machines were identified on the network:

**[Target 1]**

* Operating System: Linux
* Purpose: Victim Machine
* IP Address: 192.168.1.110

**[ELK]**

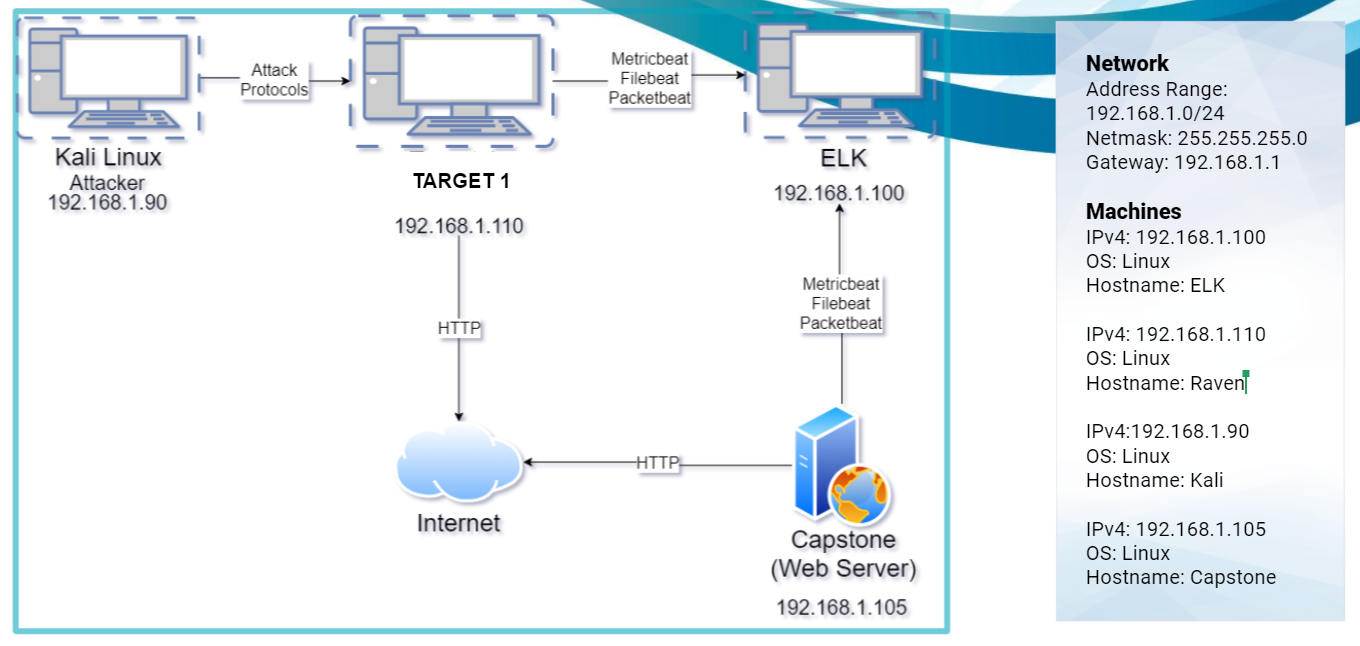
* Operating System: Linux
* Purpose: Setup alerts
* IP Address: 192.168.1.100

**[Kali]**

* Operating System: Linux
* Purpose: Attacking machine
* IP Address: 192.168.1.90

**[Capstone]**

* Operating System: Linux
* Purpose: Test alerts
* IP Address: 192.168.1.105



## Description of Targets

Fill in the following:

* Target 1: [192.168.1.110]
* Each VM functions as an Apache web server and has SSH enabled, so ports 80 and 22 are possible ports of entry for attackers.

## Monitoring the Targets

Traffic to these services should be carefully monitored. To this end, we have implemented the alerts below: (Note: Add at least three alets. You can add more if time allows.)

**Name of Alert 1**

[Excessive HTTP Errors] is implemented as follows:

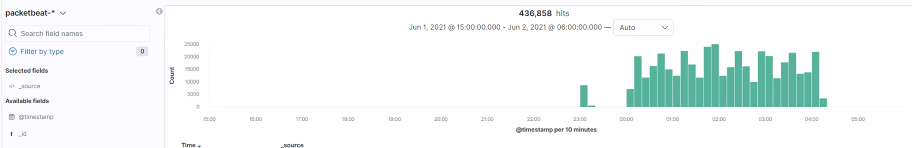
* Metric: WHEN count() GROUPED OVER top 5 'http.response.status\_code' IS ABOVE 400 FOR THE LAST 5 minutes.
* Threshold: Above 400 for last 5 minutes
* Vulnerability Mitigated: This would warn us if an attacker was trying to access parts of the server they did not have permissions for.
* Reliability: Failed to trip - Set threshold too high - suggested threshold of 25 HTTP errors in 1 Minute



**Name of Alert 2**

[HTTP Request Size Monitor] is implemented as follows:

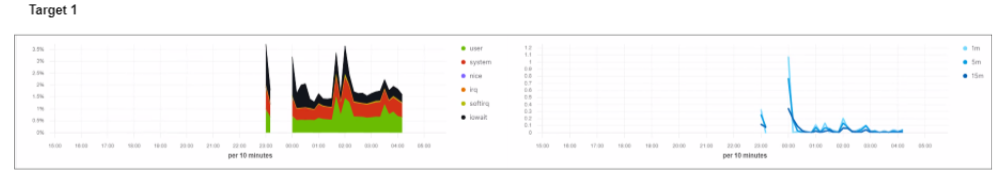
* Metric: WHEN sum() of http.request.bytes OVER all documents IS ABOVE 3500 FOR THE LAST 1 minute. (Packetbeat)
* Threshold: Above 3500 for last 60 seconds
* Vulnerability Mitigated: This will monitor against excessive requests to a website possibly warning agains a brute force attack.
* Reliability: Failed to trip - recommended threshold of 1,000 HTTP requests in last minute.



**Name of Alert 3**

[CPU Usage Monitor] is implemented as follows:

* Metric: Monitor usage spikes to alert for abnormal use.
* Threshold: Above .5 for last 5 minutes
* Vulnerability Mitigated: This will alert for scans like the WP scan but nothing else
* Reliability: This alert did hit on a scan, bud did not hit for anything else we did. We recommend lowering the threshold to 1,000.



## Suggestions for Going Further

**Suggest a patch for each vulnerability identified by the alerts above.** Remember: alerts only detect malicious behavior. They do not prevent it.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. 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 - Social Engineering:**

* Patch: User Education
* Why It Works: User Education works by requiring users to have stronger passwords, and not use the same one on sites that are considered to have weak security.

**Vulnerability 2 - MySQL**

* Patch: Controlling and vetting user input.
* Why It Works: Blocking out unknown users from gaining access will stop the majority of attacks. If you don’t need access you don’t get access.

**Vulnerability 3 - WordPress scan**

* Patch: Use the most up to date plug-ins and Themes
* Why It Works: Having the most up to date security will keep out the known attacks as well as ensuring your passwords are strong and secure from brute force attacks.