Defensive Analysis

# 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:

- Kali

- Kali Linux

- Attacking machine

- 192.168.1.90

- Target 1

- Linux

- Web server

- 192.168.1.1-255

### Description of Targets

The target of this attack was: `Target 1` (192.168.1.1-255).

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

Excessive HTTP Errors is implemented as follows:

- \*\*Metric\*\*: HTTP Errors

- \*\*Threshold\*\*: 400 over last 5 minutes

- \*\*Vulnerability Mitigated\*\*: Server overload

- \*\*Reliability\*\*: High reliability, unlikely to trigger unless an attack occurs

#### HTTP Request Size Monitor

HTTP Request Size Monitor is implemented as follows:

- \*\*Metric\*\*: HTTP request byte size

- \*\*Threshold\*\*: Over 3500 bytes over one minute

- \*\*Vulnerability Mitigated\*\*: Denial of Service attacks

- \*\*Reliability\*\*: Low reliability, there were many false positives

#### CPU Usage Monitor

CPU Usage Monitor is implemented as follows:

- \*\*Metric\*\*: CPU Usage

- \*\*Threshold\*\*: Usage over 0.5 for the last 5 minutes

- \*\*Vulnerability Mitigated\*\*: Alert for possible virus

- \*\*Reliability\*\*: Medium reliability, high CPU usage could be the result of a virus, but can also be the result of internal processes.

### Suggestions for Going Further (Optional)

\_TODO\_:

- 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

- \*\*Patch\*\*: TODO: E.g., \_install `special-security-package` with `apt-get`\_

- \*\*Why It Works\*\*: TODO: E.g., \_`special-security-package` scans the system for viruses every day\_

- Vulnerability 2

- \*\*Patch\*\*: TODO: E.g., \_install `special-security-package` with `apt-get`\_

- \*\*Why It Works\*\*: TODO: E.g., \_`special-security-package` scans the system for viruses every day\_

- Vulnerability 3

- \*\*Patch\*\*: TODO: E.g., \_install `special-security-package` with `apt-get`\_

- \*\*Why It Works\*\*: TODO: E.g., \_`special-security-package` scans the system for viruses every day\_