**DEFENSIVE**

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:

1. **Kali Machine**

- \*\*Operating System\*\*: Linux

- \*\*Purpose\*\*: to exploit the machine

- \*\*IP Address\*\*: 198.168.1.90

**2. Capstone**

Operating System: Ubuntu 18.04

Purpose: The Vulnerable Web Server

IP Address: 192.168.1.105

**3. Target 1**

Operating System: Linux

Purpose: the target machine

IP Address: 192.168.1.110

**4. Target 2**

Operating System: Linux Operating system

Purpose: the attacker

IP Address: 192.168.1.115

**5. ELK**

Operating System: Ubuntu

Purpose: The scanner

IP Address: 192.168.1.100

**Description of Targets**

The target of this attack was: `Target 1` 192.168.1.100

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
* CPU Usage 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\*\*: this alert keeps track of any incoming HTTP errors codes

- \*\*Threshold\*\*: It is set to fire if more than 400 error codes are detected in the span of 5 minutes.

- \*\*Vulnerability Mitigated\*\*: yes

- \*\*Reliability\*\*: TODO: Does this alert generate lots of false positives/false negatives? Rate as low, medium, or high reliability.

**HTTP Request Size Monitor**

Alert 2 is implemented as follows:

- \*\*Metric\*\*: This alert monitors the size of all incoming HTTP requests

- \*\*Threshold\*\*: It is set to fire upon receiving any HTTP request that is over 3500 bytes in size.

- \*\*Vulnerability Mitigated\*\*: Yes

- \*\*Reliability\*\*: TODO: It is reliable because it is executing and showing that the alert has been fired up.

**CPU Usage Monitor**

Alert 3 is implemented as follows:

- \*\*Metric\*\*: Monitors percentage of total CPU usage since the last event

- \*\*Threshold\*\*: It will fire if 50% is used within the last 5 minutes.

- \*\*Vulnerability Mitigated\*\*: TODO

- \*\*Reliability\*\*: TODO: Does this alert generate lots of false positives/false negatives? Rate as low, medium, or high reliability.

**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\_