Blue Team: Summary of Operations

Table of Contents

Network Topology

The following machines were identified on the network:

Apache Host Machine 1

- Operating System: Linux
- Purpose: Host an Apache Webserver (Raven Security)
- IP Address: 192.168.1.110

Apache Host Machine 2

- Operating System: Linux
- Purpose: Host an Apache Webserver (Raven Security)
- IP Address: 192.168.1.115

Description of Targets

- Two VMs on the network were vulnerable to attack: Target 1 [192.168.1.110] and Target 2 [192.168.1.115].

- Each VM functions as an Apache web server and has SSH enabled, so ports 80 and 22 are possible ports of entry for attackers.

- This report is directed at the first machine, Target 1.

Monitoring the Targets

This scan identifies the services below as potential points of entry:

- **Target Machine**
  - Apache version 2.4.10
  - WordPress version 4.8.14
  - SSH port 22

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.response.status_code must be less than 400
- Threshold: 400+ will set the alarm off
- Vulnerability Mitigated: Server and Client Errors
- Reliability: This alarm can set off false positives if a client is running a misconfigured browser.

HTTP Request Size Monitor

HTTP Request Size Monitor is implemented as follows:

- Metric: http.request.bytes over all documents
- Threshold: If the size of the bytes reaches a value greater than 3500
- Vulnerability Mitigated: Alerts SOC when a large file is being transferred. Because there are no large files on the webserver, the only time it should go off is if somebody is trying to exfiltrate data
- Reliability: This alert will set off false positives if there are any downloadables that will be added to the website

CPU Usage Monitor

CPU Usage Monitor is implemented as follows:

- Metric: system.process.cpu.total.pct over all documents
- Threshold: 0.5 (50%) of CPU is used over the course of 5 minutes
- Vulnerability Mitigated: Will alert SOC if there is a lot of traffic going through the webservers
- Reliability: This alert may develop a lot of false positives depending on how much traffic the webservers see in a day

Suggestions for Going Further

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

- Patch: Update Apache to newest version with *sudo apt update*

- Why It Works: This will prevent any attackers from using known vulnerabilities on the web server

Vulnerability 2

- Patch: Update WordPress to the newest version. Back up the old wordpress blog first, and then go to the blog site as an administrator to update the site from the browser.
- Why It Works: This will prevent attackers from using the WordPress blog as an access point in future attacks.

Vulnerability 3

- Patch: Set up new User and Client password policies through the command line to enforce new passwords with a minimum length and complexity.
- Why It Works: This will prevent attackers from guessing passwords and prevent brute force attacks from being successful too quickly.