Defensive Report

Blue Team: Summary of Operations

Table of Contents

Network Topology

The following machines were identified on the network:

- Elk
  - **Operating System**: Linux, Ubuntu
  - **Purpose**:SIEM
  - **IP Address**: 192.168.1.100
- Capstone
  - **Operating System**: Linux, Ubuntu
  - **Purpose**: Vulnerable machine used to test alerts
  - **IP Address**: 192.168.1.105
- Kali
  - **Operating System**: Linux, Kali
  - **Purpose**: Standard kali install used to attack other machines
  - **IP Address**: 192.168.1.90
- Target1
  - **Operating System**: Linux, Debian
  - **Purpose**: Exposes vulnerable WordPress Server that sends logs to ELK
  - **IP Address**: 192.168.1.110

- Target2
  - **Operating System**: Linux, Debian
  - **Purpose**: A more difficult WordPress target. Server that sends logs to ELK
  - **IP Address**: 192.168.1.115

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:

Monitoring the Targets

Traffic to these services should be carefully monitored. To this end, we have implemented the alerts below:

HTTP Request Size Monitor

Alert 1 is implemented as follows:

- **Metric**: http.request.bytes
- **Threshold**: 3500
- **Vulnerability Mitigated**: Denial of Service
- **Reliability**: This alert generates some false positives because when the site is very busy it will alert, however using this allert will be able to deterime when it is time for an upgrade to allow for more traffic.

Excessive HTTP Errors

Alert 2 is implemented as follows:

- **Metric**: http.response.status_code
- **Threshold**: 400
- **Vulnerability Mitigated**: Denial of Service
- **Reliability**: This alert does not generate as many false positives because it is looking for when the site replys to a user with an error.

CPU Usage Monitor

Alert 3 is implemented as follows:

- **Metric**: system.process.cpu.total.pct
- **Threshold**: 0.5
- **Vulnerability Mitigated**: Denial of Service
- **Reliability**: This alert generates some false positives because on more busy days this alert will pick up that the system is being used more.

Revision #1
Created 2025-12-08 18:17:31 UTC by David Rizzo
Updated 2025-12-08 18:17:31 UTC by David Rizzo