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
    - **Operating System**: Debian Kali 5.4.0
    - **Purpose**: Attacking Machine
    - **IP Address**: 192.168.1.90
- Capstone
    - **Operating System**: Ubuntu 18.04
    - **Purpose**: Vulnerable Web Server
    - **IP Address**: 192.168.1.105
- ELK
    - **Operating System**: Ubuntu 18.04
    - **Purpose**: ELK Stack
    - **IP Address**: 192.168.1.100
- Target 1
    - **Operating System**: Debian GNU/Linux 8
    - **Purpose**: Expose
    - **IP Address**: 192.168.1.110

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:

Excessive HTTP Errors

Excessive HTTP Errors is implemented as follows:

WHEN count() GROUPED OVER top 5 ‘http.response.status_code’

- **Metric**: Count of http.response.status_code
- **Threshold**: 400 over the last 5 minutes
- **Vulnerability Mitigated**: Brute force attack
- **Reliability**: This alert is highly reliable. Error codes over 400 are requests the server can’t or won’t complete. An excessive amount of these should be flagged.

HTTP Request Size Monitor

HTTP Request Size Monitor is implemented as follows:

WHEN sum() of http.request.bytes OVER all documents IS ABOVE 3500 FOR THE LAST 1 minute [check]

- **Metric**: sum of http.request.bytes
- **Threshold**: above 3500 for the last 60 seconds
- **Vulnerability Mitigated**: Code injection, DDoS
- **Reliability**: This alert has medium reliability. It should always alert when an actual attack is underway, but it may also trigger when the site is just receiving large amounts of http traffic.

CPU Threshold Alert

CPU Threshold Alert is implemented as follows:

WHEN max() of system.process.cpu.total OVER all documents IS ABOVE 0.5 FOR THE LAST 5 minutes

- **Metric**: max of system.process.cpu.total.pct
- **Threshold**: above .5 for the last 5 minutes
- **Vulnerability Mitigated**: Malicious software using up resources.
- **Reliability**: This alert is highly reliable. CPU usage over the threshold could either indicate an attack or that something else is going wrong with the system.