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:

- Hypervisor / Host Machine
    - Operating System: Microsoft Windows
    - Purpose: Hypervisor / Gateway
    - IP Address: 192.168.1.1
- ELK
    - Operating System: Linux
    - Purpose: SIEM
    - IP Address: 192.168.1.100
- Capstone
    - Operating System: Linux
    - Purpose: HTTP Server (Red Herring)
    - IP Address: 192.168.1.105
- Target 1
    - Operating System: Linux
    - Purpose: HTTP Server and Wordpress Site
    - IP Address: 192.168.1.110
- Target 2
    - Operating System: Linux
    - Purpose: HTTP Server
    - 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:

Excessive HTTP Errors

HTTP Request Size 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: http.response.status_code > 400
- Threshold: 5 in last 5 minutes
- Vulnerability Mitigated: Able to identify brute force attacks
- Reliability: Highly reliable, does not generate frequent false positives

HTTP Request Size Monitor

Alert 2 is implemented as follows:

- Metric: http.request.bytes
- Threshold: 3500 in last 1 minute
- Vulnerability Mitigated: Protects against DDOS attacks
- Reliability: Highly reliable, does not generate frequent false positives

CPU Usage Monitor

Alert 3 is implemented as follows:

- Metric: system.process.cpu.total.pct
- Threshold: 0.5 in last 5 minutes
- Vulnerability Mitigated: Triggers a memory dump if stored information is generated
- Reliability: Not very reliable, can generate frequent false positives