Symantha Meyers - Project 3

Blue Team - Summary of Operations
January 19, 2021

Table of Contents

Network Topology

The following machines were identified on the network:

- Capstone
    - **Operating System**: Ubuntu
    - **Purpose**: Testing of Filebeat and Metricbeat setup
    - **IP Address**: 192.168.1.105
- ELK
    - **Operating System**: Ubuntu
    - **Purpose**: Server hosting ELK Stack
    - **IP Address**: 192.168.1.100
- Kali
    - **Operating System**: Kali Linux
    - **Purpose**: Attack server
    - **IP Address**: 192.168.1.90
- Target 1
    - **Operating System**: Ubuntu
    - **Purpose**: Vulnerable Apache WordPress Server - Target of attack
    - **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:

Name of Alert 1 - HTTP Request Size Monitor

Alert 1 is implemented as follows:

- **Metric**: WHEN sum OF http.request.bytes
- **Threshold**: 3500
- **Vulnerability Mitigated**: Any excessive amounts of http requests will trigger this alert
- **Reliability**: This alert seems to be reliable and will report if any excessive amounts of HTTP requests are logged.

Name of Alert 2 - CPU Usage Monitor

Alert 2 is implemented as follows:

- **Metric**: WHEN max OF system.process.cpu.total.pct
- **Threshold**: 0.5
- **Vulnerability Mitigated**: This alert will trigger when the CPU is being taxed irregularly
- **Reliability**: This alert seems reliable. It runs every minute and will alert if the threshold is reached or exceeded.

Name of Alert 3 - Excessive HTTP Errors

Alert 3 is implemented as follows:

- **Metric**: WHEN count GROUPED OVER top 5 'http.response.status_code'
- **Threshold**: 400
- **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*