Blue Team: Summary of Operations

Table of Contents

Network Topology

TODO: Fill out the information below.

The following machines were identified on the network:

- Target 1
    - **Operating System**: Debian GNU/Linux 8.11.0
    - **Purpose**: Vulnerable WordPress host
    - **IP Address**: 192.168.1.110
- Kali
    - **Operating System**: Kali GNU/Linux Loading
    - **Purpose**: Pentesting
    - **IP Address**:192.168.1.90
- ELK
    - **Operating System**: Ubuntu 18.04.4 LTS
    - **Purpose**: VM that holds the Kibana dashboards
    - **IP Address**:192.168.1.100
- Capstone
    - **Operating System**: Ubuntu 18.04
    - **Purpose**: Forwards logs to the ELK machine
    - **IP Address**:192.168.1.105

Description of Targets

TODO: Answer the questions below.

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

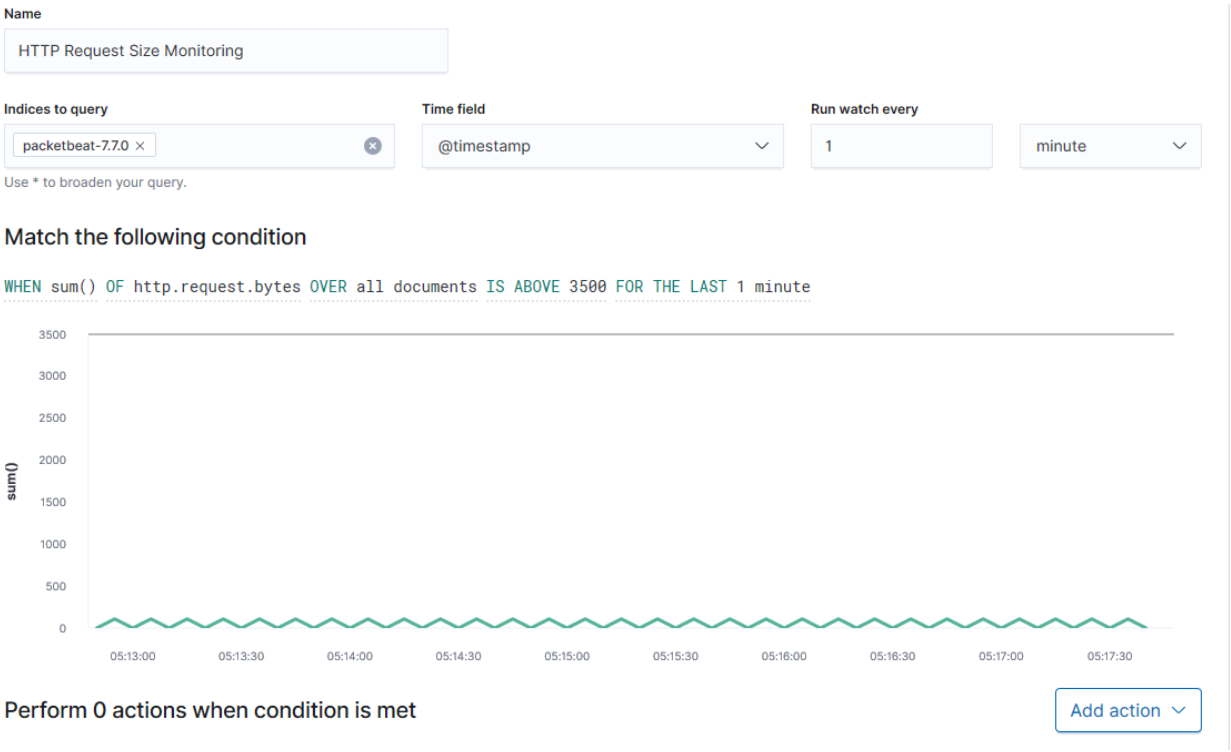
Traffic to these services should be carefully monitored. To this end, we have implemented the alerts below:

Excessive HTTP Errors

- **Metric**: WHEN count() GROUPED OVER top 5 ‘http.response.status_code
- **Threshold**: 400
- **Vulnerability Mitigated**: Brute Force
- **Reliability**: High

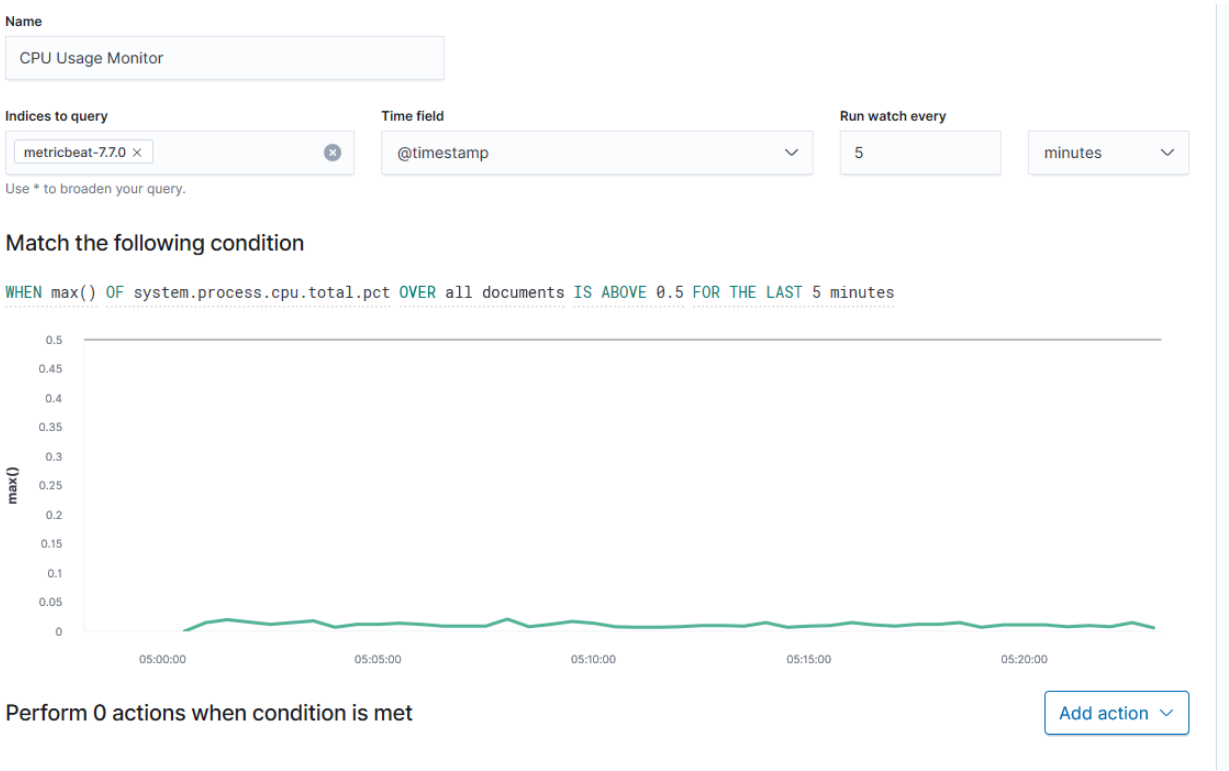
HTTP Request Size Monitor

- **Metric**: WHEN sum() of http.request.bytes OVER all documents
- **Threshold**: IS ABOVE 3500
- **Vulnerability Mitigated**: Code Injection
- **Reliability**: Medium



CPU Usage Monitor

- **Metric**: WHEN max() OF system.process.cpu.total.pct OVER all documents
- **Threshold**: IS ABOVE 0.5
- **Vulnerability Mitigated**: Malware/Viruses
- **Reliability**: High



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*