Blue Team: Summary of Operations

Table of Contents

Network Topology

Network Diagram:

- **Kali**
  - **Operating System**: Kali linux
  - **Purpose**: The penetration tester
  - **IP Address**: 192.168.1.90
- **ELK**
  - **Operating System**: Ubuntu linux
  - **Purpose**: The ELK (elasticsearch and Kibana) Stack
  - **IP Address**: 192.168.1.100
- **Target 1**
  - **Operation System:** Linux
  - **Purpose:** The WordPress Host
  - **IP address:** 192.168.1.110
- **Capstone**
  - **Operation System:** Linux
  - **Purpose:** The Vulnerable Web Server
  - **IP address:** 192.168.1.105

Description of Targets

The target of this attack was: Target 1 (IP Address: 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

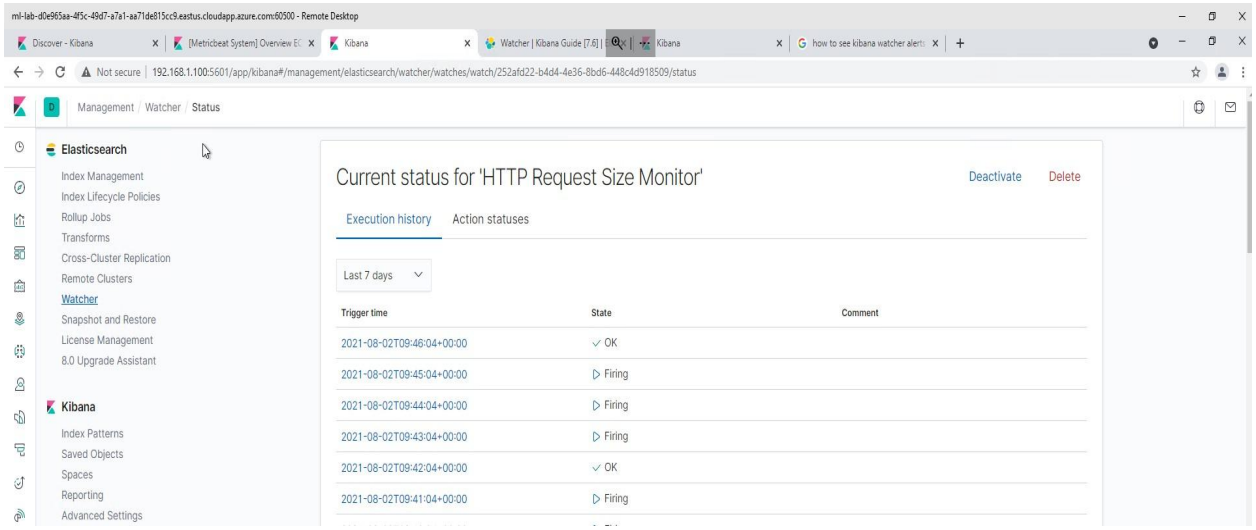
Traffic to these services should be carefully monitored. To this end, we have implemented the alerts below:

Excessive HTTP Errors

Excessive HTTP Errors is implemented as follows:

```
WHEN count() GROUPED OVER top 5 'http.response.status_code' IS ABOVE 400
FOR THE LAST 5 minutes
```

- **Metric**:
  - `WHEN count() GROUPED OVER top 5 'http.response.status_code'`
- **Threshold**:
  - `IS ABOVE 400 FOR THE LAST 5 minutes`
- **Vulnerability Mitigated**:
  - Enumeration/Brute Force
- **Reliability**:
  - Highly reliable that able to be measured by error codes 400 and above will filter out any normal or successful responses.

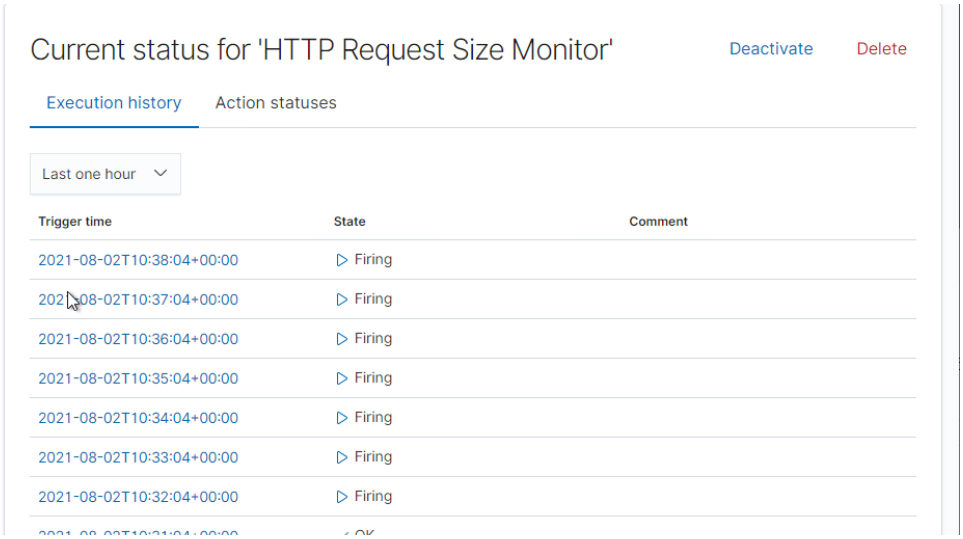


HTTP Request Size Monitor

HTTP Request Size Monitor is implemented as follows:

- **Metric**:
  - WHEN sum() of http.request.bytes OVER all documents
- **Threshold**:
  - IS ABOVE 3500

- **Vulnerability Mitigated**:
    - Code injection in HTTP requests (XSS and CRLF) or DDOS
- **Reliability**:
    - Medium reliability because there is a possibility for legitimate traffic on HTTP requests.



CPU Usage Monitor

CPU Usage Monitor is implemented as follows:

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

- **Metric**:
  - `WHEN max() OF system.process.cpu.total.pct OVER all documents`
- **Threshold**:
  - `IS ABOVE 0.5 FOR THE LAST 5 minutes`
- **Vulnerability Mitigated**:
  - Malicious software running taking up resources.
- **Reliability**:
  - Highly reliable that can help identify where to improve on CPU usage and mitigate a malicious software risk.