Final Engagement

Attack, Defense & Analysis of a Vulnerable Network

Start of Blue Team Presentation

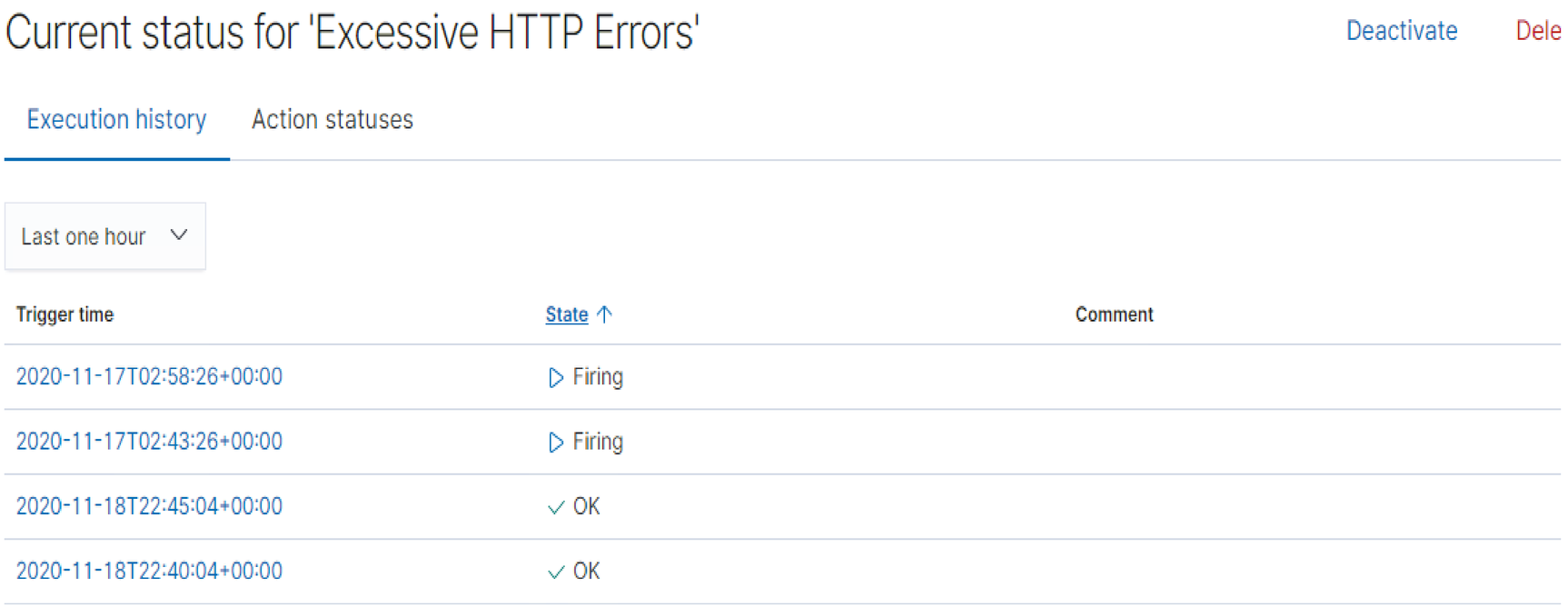
Table of Contents

This document contains the following resources:

Alerts Implemented

[HTTP Errors]

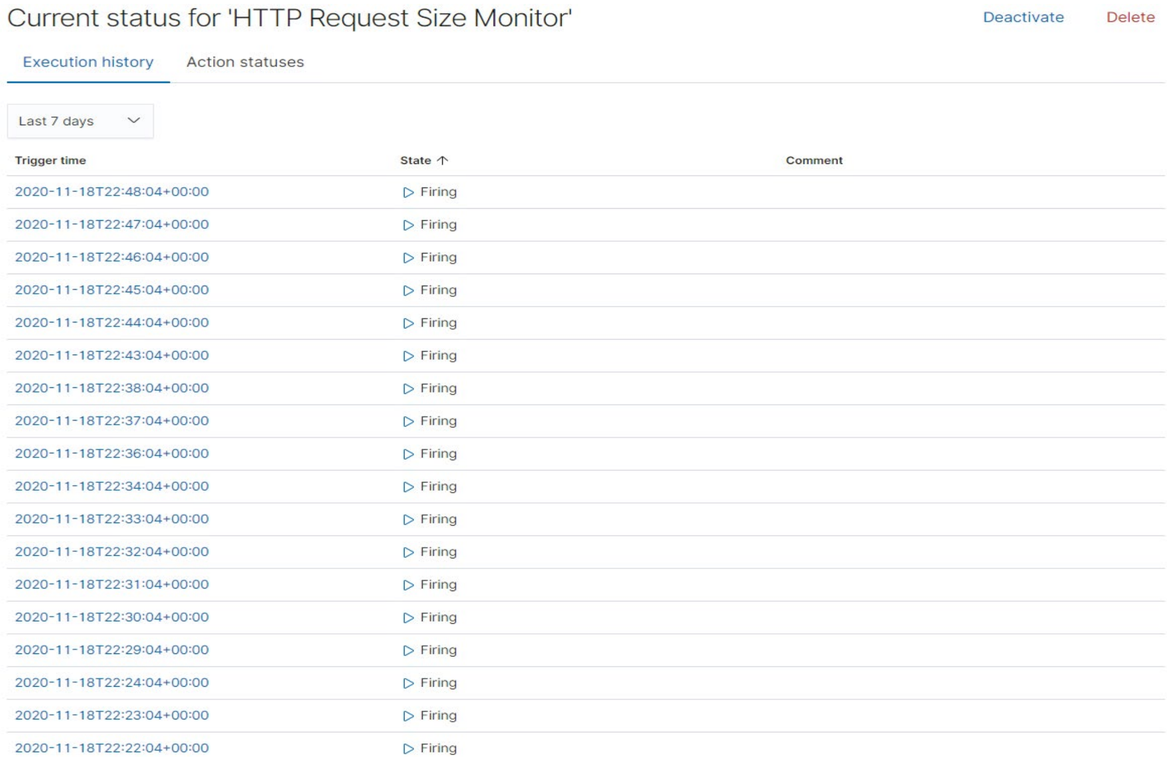
- This metric alert monitors HTTP
- The threshold fires at 400
- Low reliability



[HTTP Request Size Monitor]

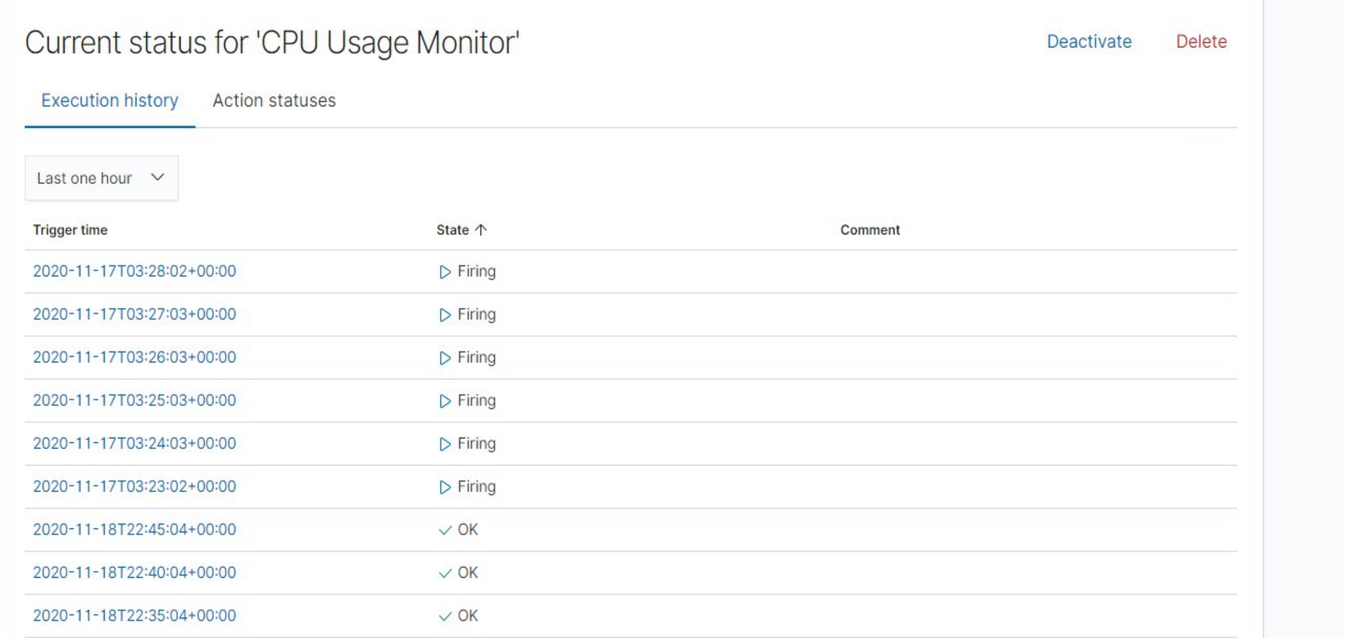
- The metric alert monitors http.request.bytes
- The threshold fires at 3400
- Low Reliability

.



[CPU Usage Monitor]

- The metric alert monitors system.process.cpu.total.pct
- The threshold it fires at 0.5



Hardening

Hardening Against [Open Ports] on Target 1

- Disable Root Logins
- Use Public/Private Keys for Authentication
- Assign Another port (Non standard port) for ssh, http etc
- Disable ICMP to prevent port scans

Hardening Against [Excessive CPU Usage] on Target 1

- Load Balancer should be implemented prevent web-servers from overloading and to add redundancy.
  - Why It Works: Load balancers also add resiliency by rerouting live traffic from one server to another if a server falls prey to DDoS attacks or otherwise becomes unavailable.

- Set an alert that if a user exceeds the expected baseline traffic slow them down or block them temporarily and investigate their actions.
  - If a user was behaving maliciously you may quickly detect it or even prevent it.

Hardening Against [Password Vulnerability] on Target 1

- Make a policy to require secure passwords
  - Guidelines: minimum 16 characters long
  - Must have a capital letter
  - Must have a lowercase letter
  - Must have a number
  - Must have a symbol
  - Lockout users after after multiple failed attempts
  - Maintain geolocation data of where a user logs in from and monitor for anomalies

Implementing Patches

Implementing Patches

```
README
Implementing Patches
Patches for Vulnerablities on Target 1
Hardening against Open Ports [ssh port 22]
    Disable root login
        To do this: Go to /etc/ssh/sshd_config
            set PermitRootLogin to no
    Assign a Non Standard port for ssh to avoid casual scans
        To do this: Open /etc/ssh/sshd_config file and look for line Port 22 and change line to port [Non Standard port]
            Restart sshd server
            Now ssh using ssh -p [non standard port choosen] user@your-ip
    Disable ICMP to prevent results from port scanning
        To do this: no ip icmp echo broadcast-request
Hardening against Password Vulnerablities on Target 1
    Steps to Enforcing password strenght and lenght
        To do this:
            1. Open Command prompt
            2. Enter command net accounts
            3. Enter command net accounts /minpwlen:NumberOfCharacters
    Steps to force local account to change password as needed
        To do this:
            1. Click/tap on Users in the left pane of Local Users and Groups
            2. Right click or press and hold on the name, then click on properties
            3. In the General tab, check the User must change password at [Desired time]


```