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:
- ELK
  - Linux
  - ELK Server setting up alerts
  - 192.168.1.100
- Capstone
  - Linux
  - Monitoring Alerts
  - 192,168.1.105
- Target 1
  - Linux
  - Victim machine designated for compromise
  - 192.168.1.110
- Target 2
  - Linux
  - Victim machine Unknown purpose
  - 192.168.1.115
- Kali
  - Linux
  - Penetration Machine
  - 192.168.1.90

Description of Targets

The target of this attack was: `Target 1` (192.168.1.110).

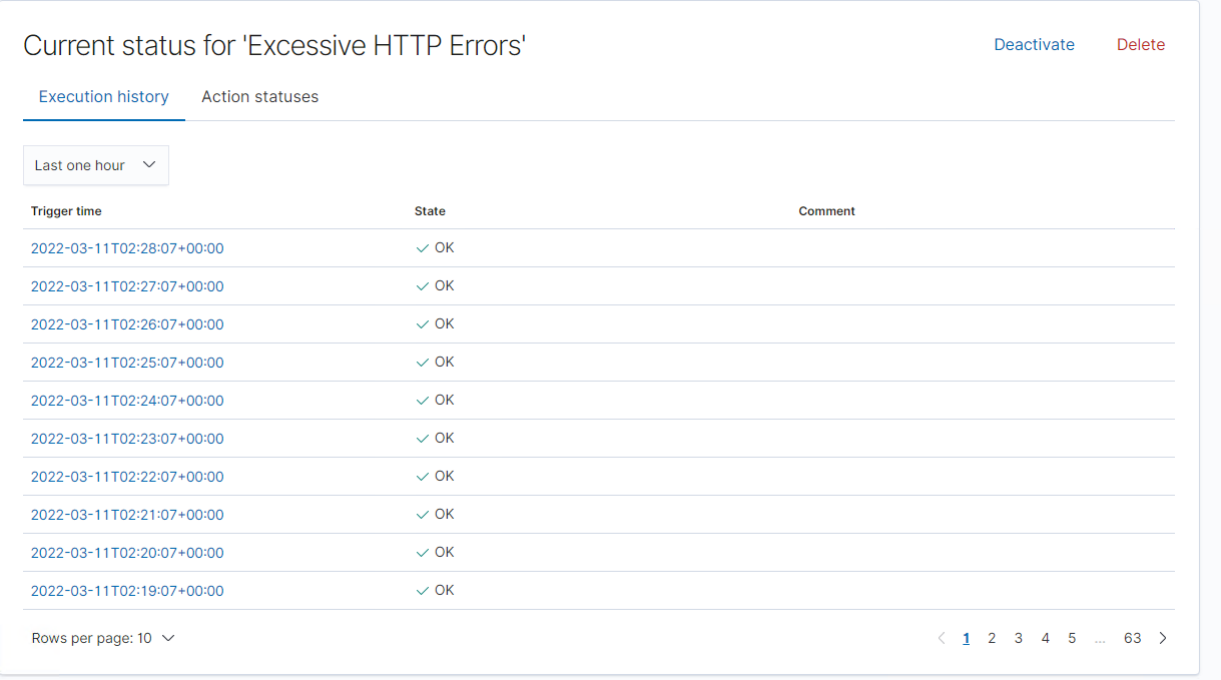
Target 1 is an Apache web server and has SSH enabled, so ports 80 and 22 are possible ports of entry for attackers. As such, the following alerts have been implemented:

Port 80 is HTTP and port 22 is SSH so we have set up alerts monitoring http errors that exceed 400 in 5 minutes, HTTP request size at 3500 bytes over 1 min and cpu usage to see if it spikes above 0.5 over 5 minutes.

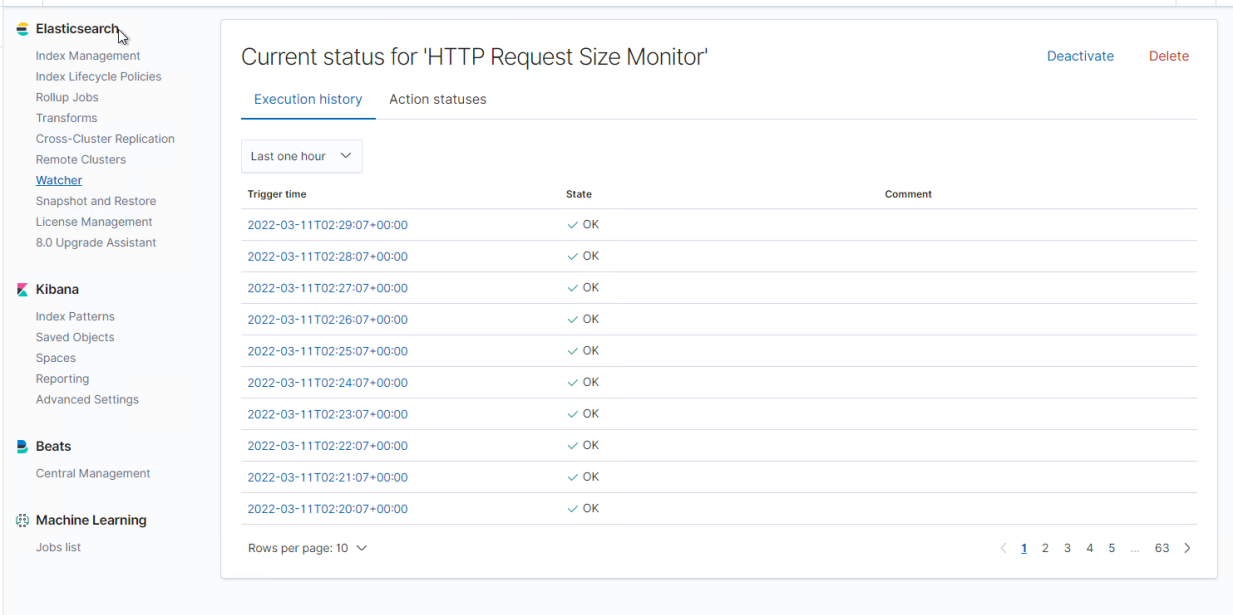
Monitoring the Targets

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

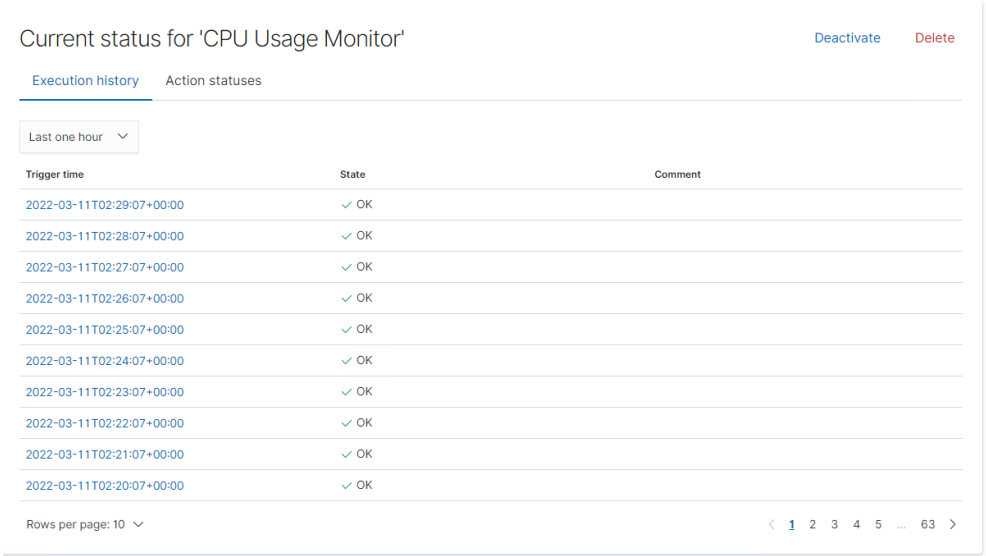
Excessive HTTP Errors
Alert 1 is implemented as follows:
- Metric: http response status codes
- Threshold: above 400
- Vulnerability Mitigated: Brute Force Attacks
- Reliability: TODO: This alert is often high reliability as no normal activity on this website would indicate higher that 400 requests in 5 min



HTTP Request Size Monitor
Alert 2 is implemented as follows:
- Metric: Monitors the sum of bytes over all documents
- Threshold: above 3500 bytes over 1 min
- Vulnerability Mitigated: Can pick up DOS attacks that are flooding the network with information
- Reliability: I would set this at a medium reliability as any alert going off should prob be investigated but may not always be malicious.



CPU Usage Monitor
Alert 3 is implemented as follows:
- Metric: Monitors the total cpu percentage use over the last five minutes
- Threshold: 0.5 processing power
- Vulnerability Mitigated: Alert to indicate high bandwidth and ram usage possibility of malware or virus download
- Reliability: I would say this has a medium reliability that a spike in cpu usage should be investigated but may not always mean malicious activity.



Suggestions for Going Further (Optional)
- 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: Excessive HTTP Errors
    - Patch: Start Maintaining regular updates and use hardening tools.
        - Update the version of wordpress
        - Update the version of php
        - Install security plugins (wordfence Security, Defender, Ithemes Security)
        - Install firewall(Install a Web application firewall plugin: wordfence, siteground security, RSfirewall)
        - Block enumeration of users via wpscan
    - Why It Works:
        - Patches and updates will prevent easy known exploits from being used.
        - The plugins can provide features such as firewalls and virus scans
        - Blocking enumeration by using user nicknames or via plugins such as WP Hardening
- Vulnerability 2: HTTP Request Size Monitor
    - Patch: DDOS protection
        - Limit the size of HTTP requests on the web server
    - Why it works:
        - IF you can limit the size on incoming traffic on a web server any attempts to flood will be met by error messages and will prevent large entries.
- Vulnerability 3 CPU Usage Monitor
    - Patch: Malware and Virus Prevention
        - Ensure you have a good antivirus to protect your webserver against any malware or viruses that would use up or spike cpu usage
        - Implementing a HIDS or NIDs could also help prevent and analyze unwanted traffic coming in.
    - Why it works:
        - Antivirus will protect your server from any unwanted malware or viruses that could cause issues.
        - The HIDs and NIDS will be able to monitor and analyze the packets coming in and out of your system, HIDS focusing on the host itself and the NIDs focusing on traffic.