Blue Team: Summary of Operations

Table of Contents

Network Topology

The following machines were identified on the network:

- Kali
  - Operating System: Kali
  - Purpose: Attacking Machine
  - IP Address: 192.168.1.90
- Capstone
  - Operating System: Ubuntu
  - Purpose: vulnerable target VM
  - IP Address: 192.168.1.105
- ELK
  - Operating System:Ubuntu
  - Purpose: Collects logs from Target 1 and Capstone VMs
  - IP Address: 192.168.1.100
- Target 1
  - Operating System : Wordpress
  - Purpose: Exposes a vulnerable web server; sends logs to ELK
  - 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:

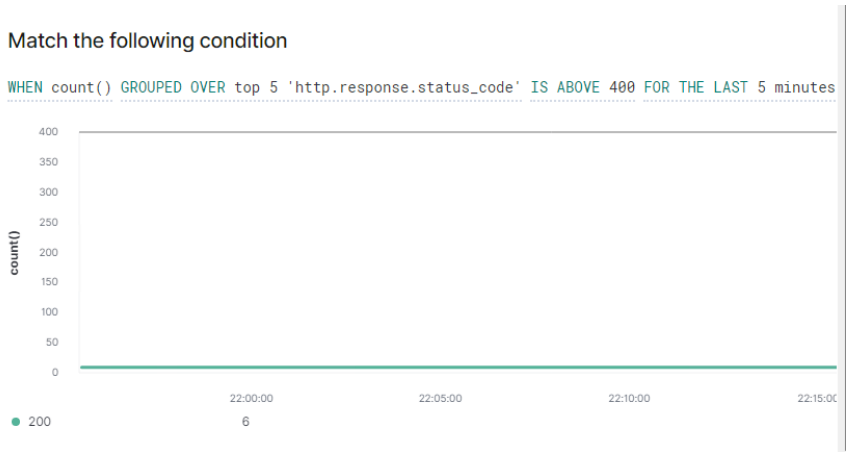
Monitoring the Targets

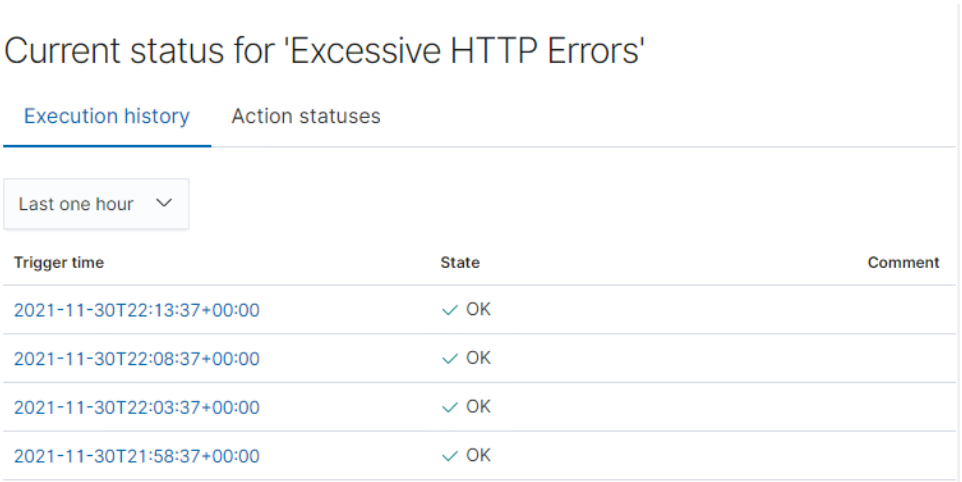
Traffic to these services should be carefully monitored. To this end, we have implemented the alerts below:

Excessive HTTP Errors alert

Alert 1 is implemented as follows:

- Metric: http.response.status_code
- Threshold: 400
- Vulnerability Mitigated: Brute Force / Enumeration
- Reliability: high
- Screenshots of alert:

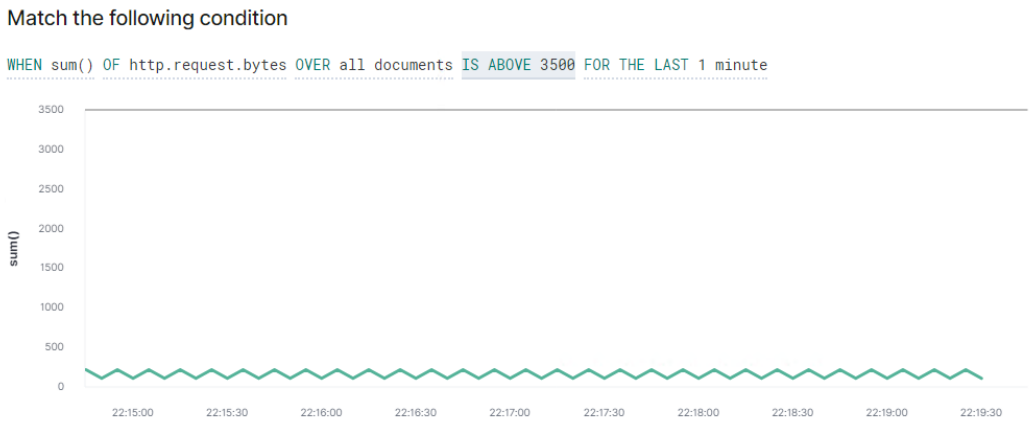


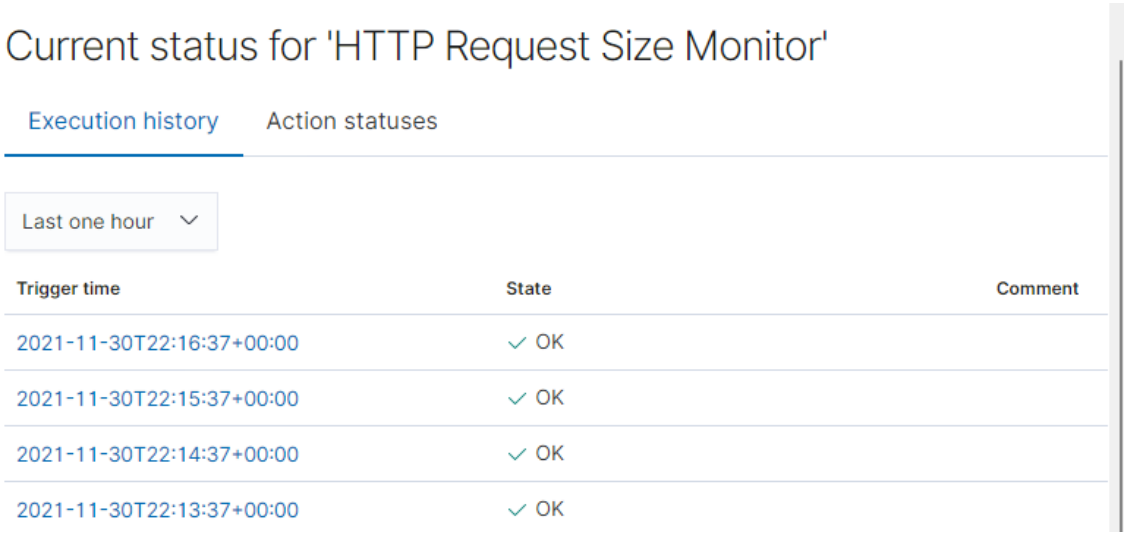


HTTP Request Size Monitor

Alert 2 is implemented as follows:

- Metric: http.request.bytes
- Threshold: 3500 in 1 minute
- Vulnerability Mitigated: DDoS / Code Injection
- Reliability: medium; this alert has generated a few false positives
- Screenshots of alert:

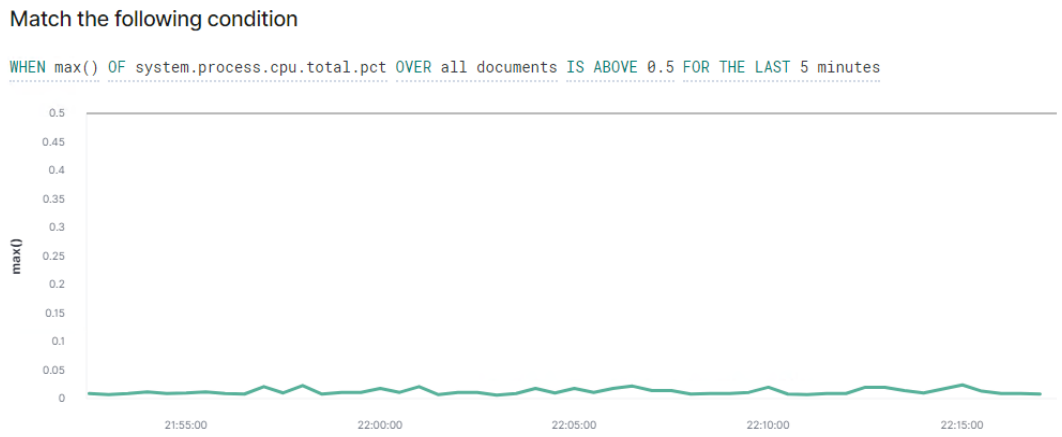


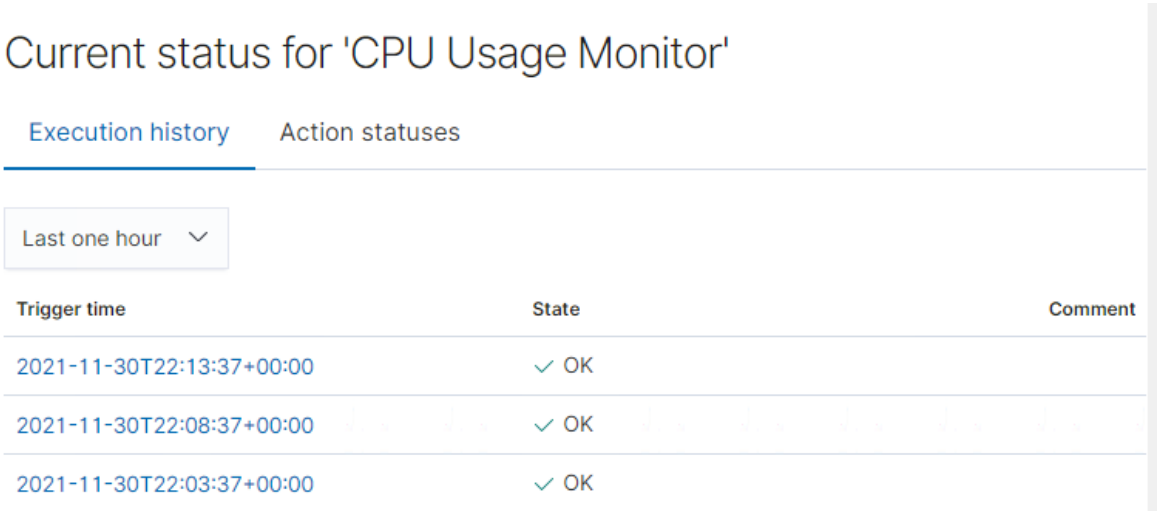


CPU Usage Monitor

Alert 3 is implemented as follows:

- Metric: system.process.cpu.total.pct
- Threshold: over .5 in last five minutes
- Vulnerability Mitigated: Malware / Viruses
- Reliability: high
- Screenshots of alert:





Suggestions for Going Further (Optional)

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: Brute Force
    - Patch: Implement Two-Factor Authentication on employee accounts
    - Why It Works: 2FA adds an additional layer of security to accounts. Even if a malicious user were able to obtain a username and password, the additional login authentication requirement would prevent them from gaining access
- Vulnerability 2: DDos
    - Patch: Implement a Scrubbing server on the network
    - Why It Works: The scrubbing server would be a dedicated machine to receive all of the network traffic destined for the target machine. This scrubbing server would be used to filter traffic, and only send non-DDoS packets. While not entirely foolproof, it would be a good addition to the overall security framework
- Vulnerability 3: Malware / Viruses
    - Patch: Install Anti-Virus / Anti-Malware software on all employee devices
    - Why It Works: Anti-Virus software scans files or code being passed through network traffic and compares them to a database of known threats. If there is a match, it will block the malicious files