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:

- Name of VM 1: Hyper V Manager.
    - **Operating System**: Windows.
    - **Purpose**: Hosting five machines.
    - **IP Address**: 192.168.1.1
- Name of VM 2: Kali
    - **Operating System**: Linux
    - **Purpose**: Attacking machine
    - **IP Address**: 192.168.1.90
- Name of VM 3: ELK.
    - **Operating System**: Linux.
    - **Purpose**: It holds the Kibana dashboard.
    - **IP Address**: 192.168.1.100
- Name of VM 4: Capstone.
    - **Operating System**: Linux.
    - **Purpose**: Filebeat and Metricbeat are installed and will forward logs to the ELK machine. (this VM is in the network only for the purpose of testing alerts).
    - **IP Address**: 192.168.1.105
- Name of VM 5: Target 1
    - **Operating System**: Linux
    - **Purpose**: Vulnerable WordPress server.
    - **IP Address**: 192.168.1.110
- Name of VM 6: Target 2
    - **Operating System**: Linux
    - **Purpose**: Vulnerable WordPress server
    - **IP Address**: 192.168.1.115

Description of Targets

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

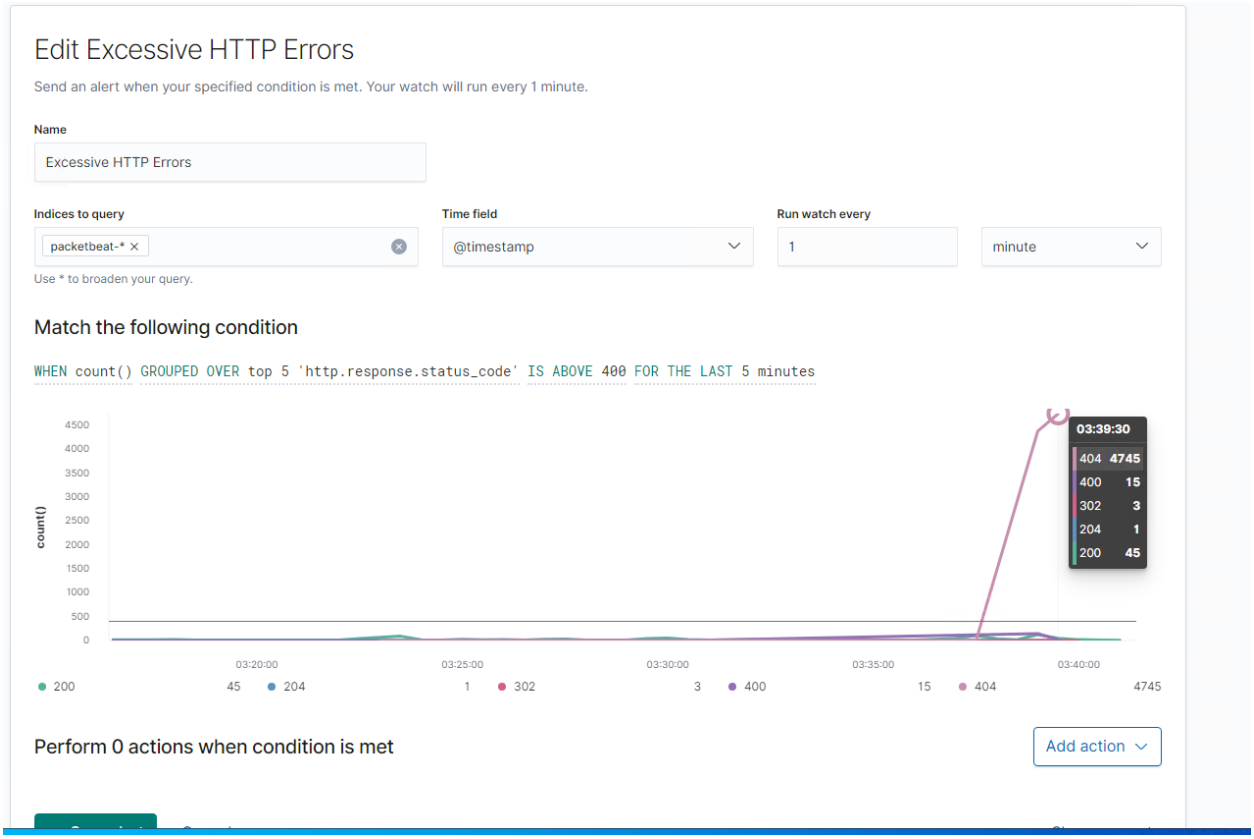
Target 1 is an Apache web server and has SSH enabled, so ports 80 and 22 are possible ports of entry for attackers. As such, the following alerts have been implemented:

Monitoring the Targets

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

Excessive HTTP Errors (Alert 1)

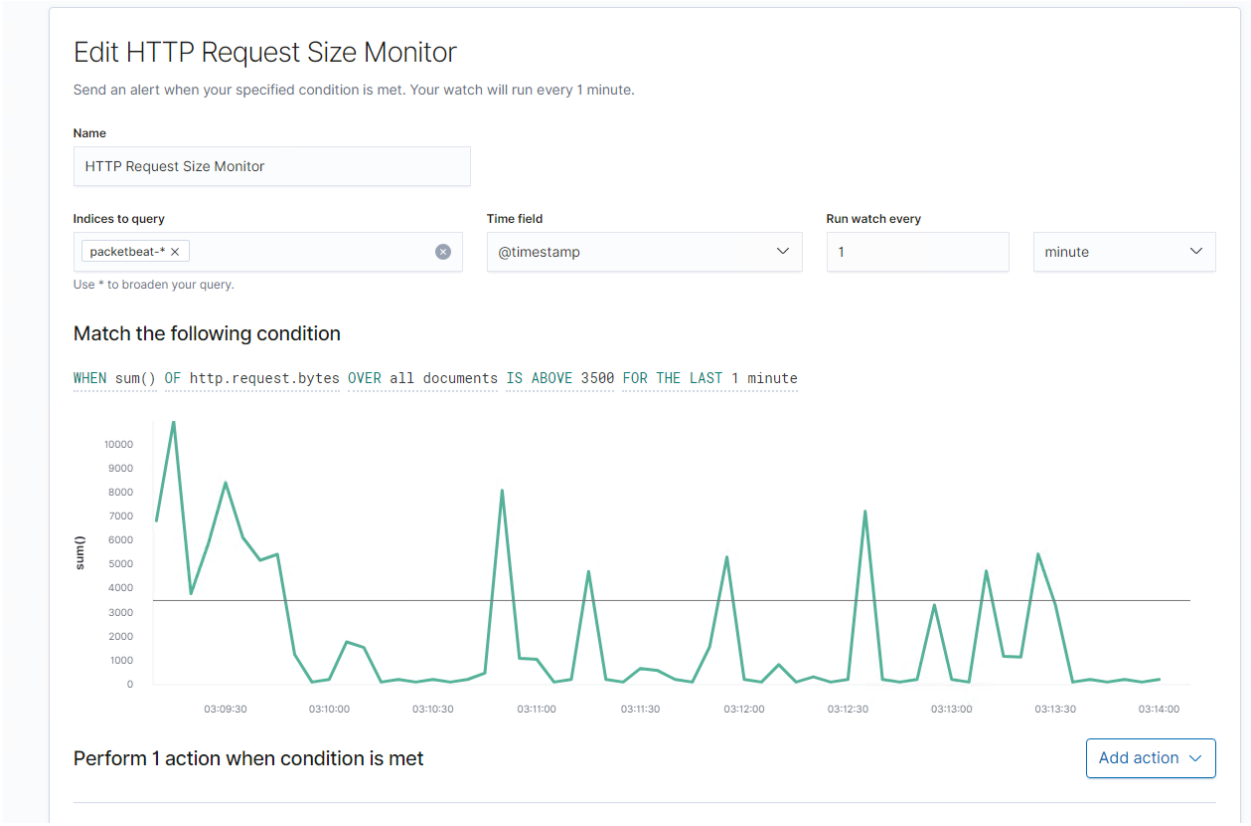
Excessive HTTP Errors is implemented as follows:



- **Metric**: Packetbeat
- **Threshold**: WHEN count() GROUPED OVER top 5 'http.response.status_code' IS ABOVE 400 FOR THE LAST 5 minutes
- **Vulnerability Mitigated**: This alert will successfully identify a brute force attack and enumeration, so we can block any IP addresses associated with the attack.
- **Reliability**: This alert doesn't generate lots of false positives/false negatives. I would rate this alert as **High reliability**.

HTTP Request Size Monitor (Alert 2)

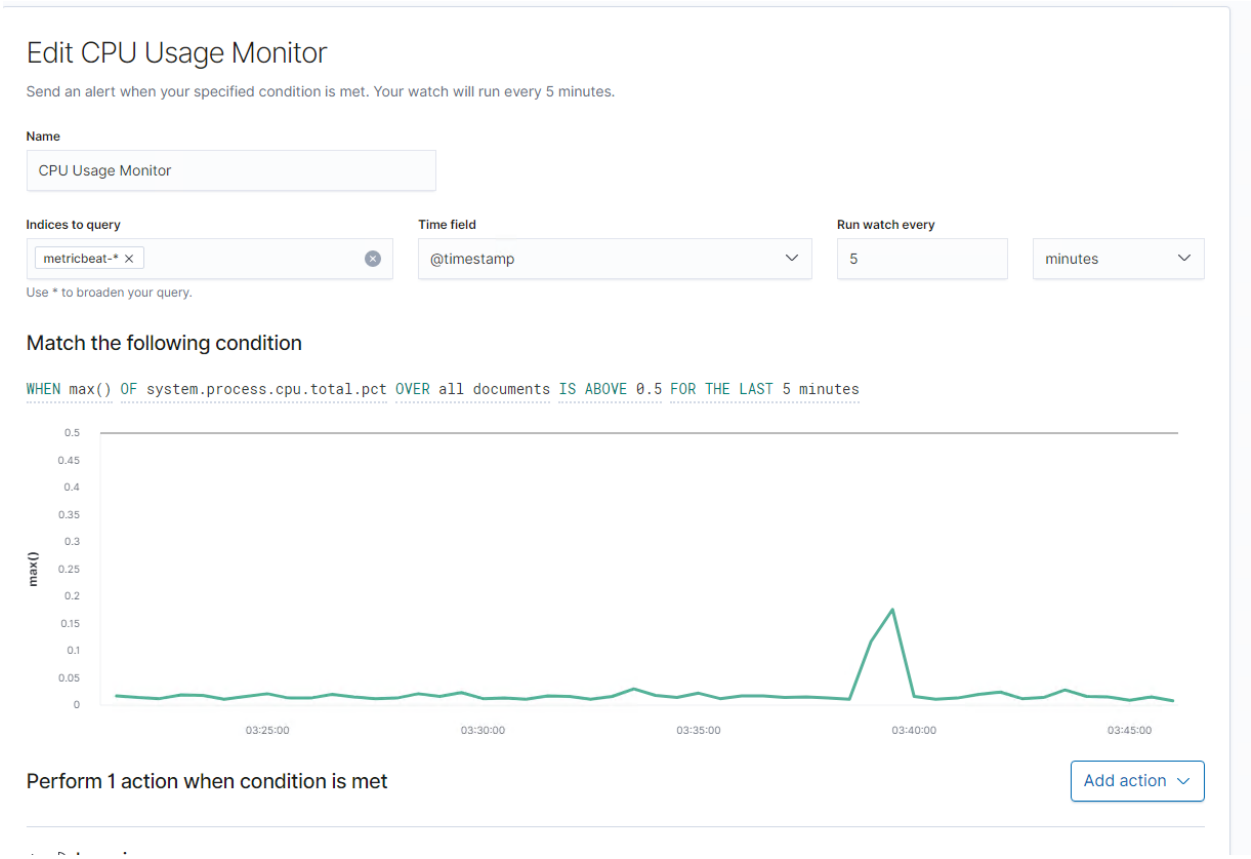
HTTP Request Size Monitor is implemented as follows:



- **Metric**: Packetbeat
- **Threshold**: WHEN sum() of http.request.bytes OVER all documents IS ABOVE 3500 FOR THE LAST 1 minute
- **Vulnerability Mitigated**: This alert can detect a potential DDoS attack and code injection in HTTP requests, by monitoring the HTTP request size.
- **Reliability**: This alert has the potential to generate false positives, because sometimes normal HTTP requests can be larger. I would rate this alert as **Medium reliability.**

CPU Usage Monitor (Alert 3)

CPU Usage Monitor is implemented as follows:



- **Metric**: Metricbeat
- **Threshold**: WHEN max() OF system.process.cpu.total.pct OVER all documents IS ABOVE 0.5 FOR THE LAST 5 minutes
- **Vulnerability Mitigated**: This alert will be triggered if the CPU usage is above 50% for the last five minutes. This sometimes indicates that some Malware is in the system and is using the memory.
- **Reliability**: This alert has the potential to trigger false positives because oftentimes CPU usage goes above 50% because some programs are running in the background such as antivirus scan and streaming applications. I would rate this alert as **Medium**.

Suggestions for Going Further

Each alert above pertains to a specific vulnerability/exploit. Recall that alerts only detect malicious behavior, but do not stop it.

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:

- **Brute-Force Attack and Enumeration**

    - **Patch**: Implementation of multi-factor authentication and WordPress Hardening.
    - **Why It Works**: The use of multi-factor authentication can prevent brute-force attacks because in addition to password the user is required to use another credential. Implementing regular updates to WordPress provide patches to known vulnerabilities.

- **DDoS and Code Injection in HTTP Requests**

    - **Patch**: Implementation of input validation. Implementation of HTTP Request Limit on the web server (limit on size of the request, limit onURL length), and use of Load Balancer.
    - **Why It Works**: According to OWASP, input validation can prevent malformed data from persisting in the database and triggering malfunction of various downstream components. Implementation of HTTP Request Limit will reject the potentially malicious requests that are too large. And the use of Load Balancer can block many known DDoS attacks.

- **Malware and Viruses**

    - **Patch**: Use of Antivirus software and/or Host Based Intrusion Detection System
    - **Why It Works**: The use of antivirus software can detect and remove malicious softwares that are trying to penetrate the system, or are already inside. The Host Based Intrusion Detection System also conducts monitoring and analyzing of the internals of a computing system as well as the network packets on its network interfaces.

Prepared by Ognen Nastoski

March 7, 2022