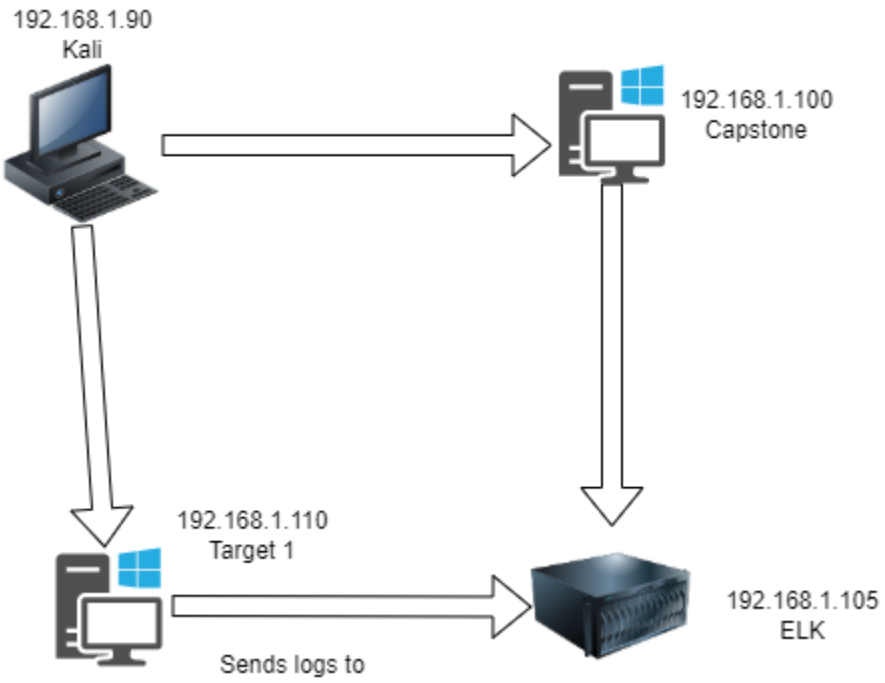
Blue Team: Summary of Operations

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:

1. Kali

Linux
This is the attacker machine.
192.168.1.90

2. Target 1

Linux
The machine that is vulnerable with wordpress.
192.168.1.110

3. ELK

Linux
This machine is used for gathering information with filebeat, metricbeat, and packetbeat.
192.168.1.105

4. Capstone

Linux
This machine was used to test alerts.
192.168.1.100

Description of Targets

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

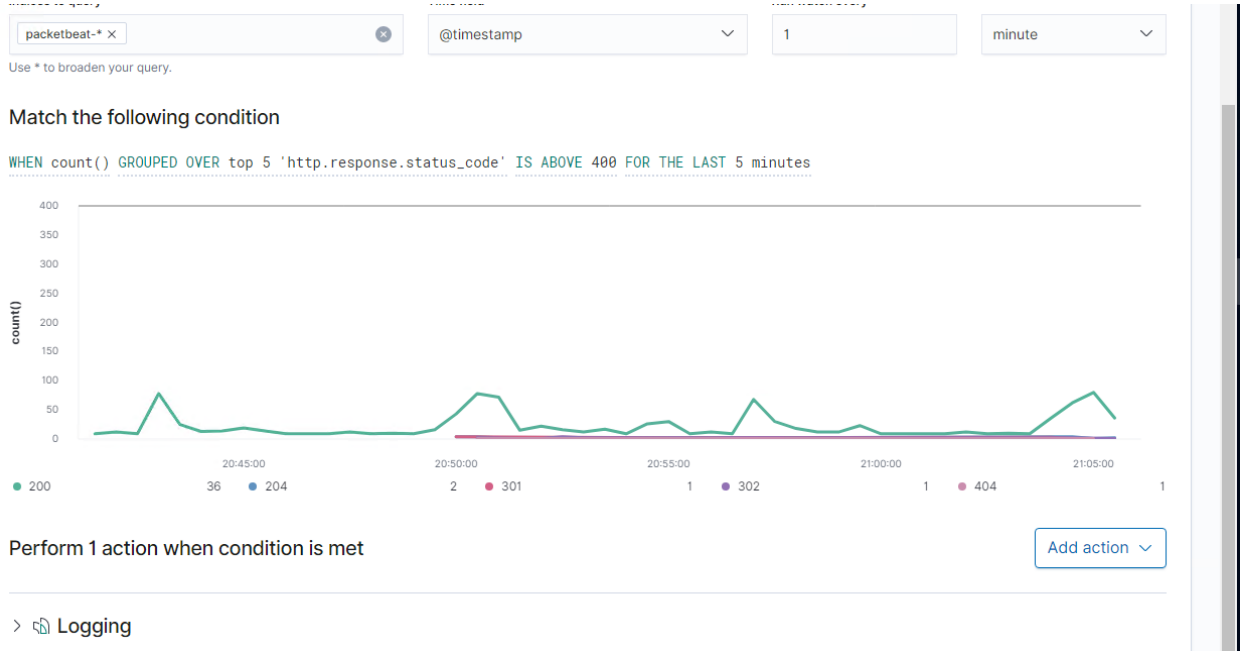
Target 1 is an Apache web server and has SSH enabled, so ports 80 and 22 are possible ports of entry for attackers. As such, the following alerts have been implemented:

Monitoring the Targets

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

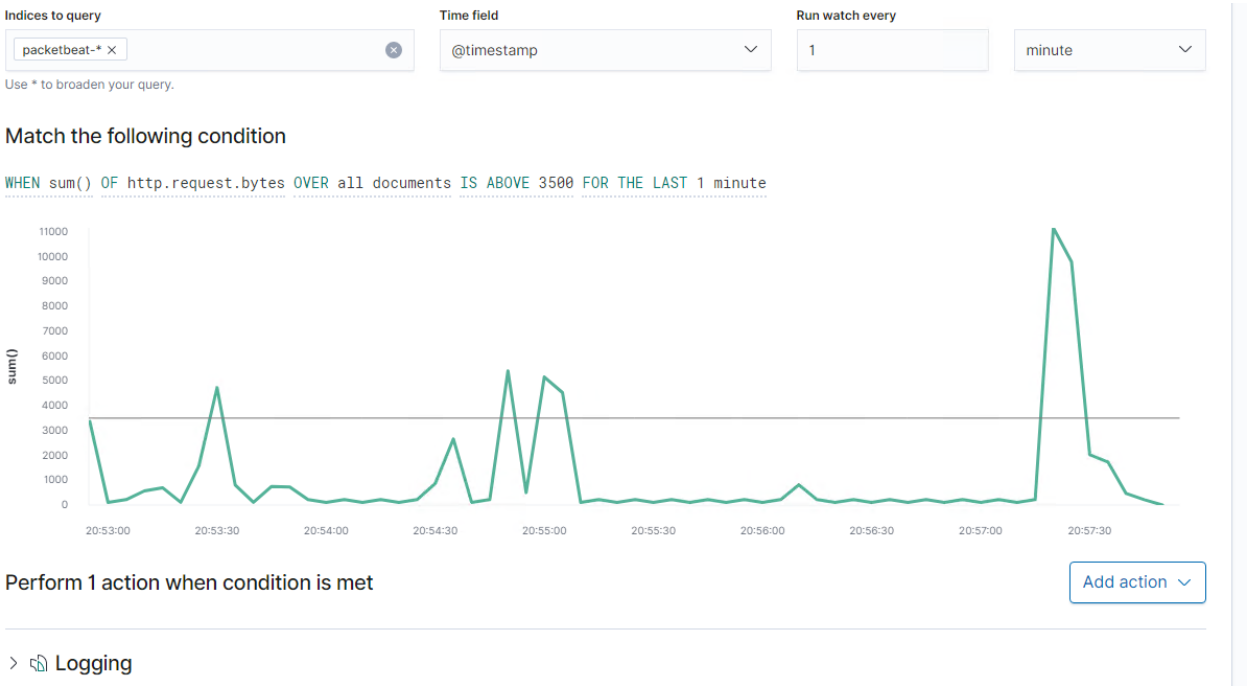
Excessive HTTP Errors

Excessive HTTP Errors is implemented as follows:
- **Metric**: Packetbeat http.response.status.code more than 400
- **Threshold**: When the status code equals more than 400 in the last 5 minutes.
- **Vulnerability Mitigated**: You are able to block ip addresses, change passwords, or close port 22 when the alert goes off.
- **Reliability**: No, this alert doesn't give many false positives. High



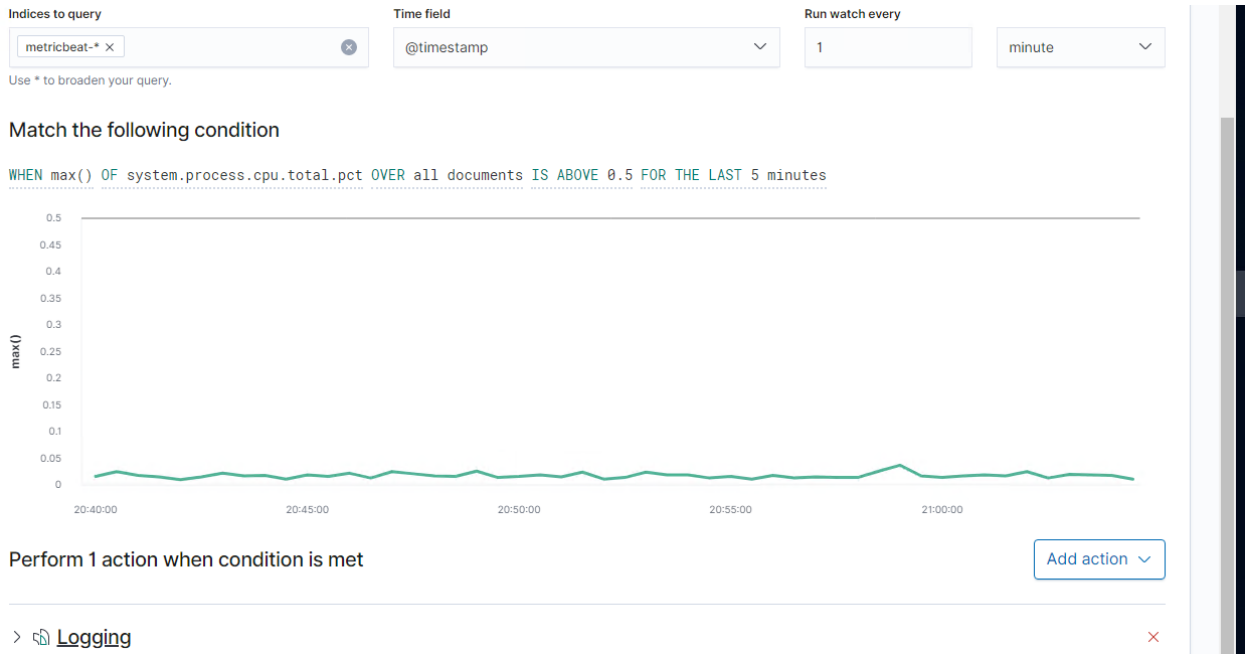
HTTP Request Size Monitor

HTTP Request Size Monitor is implemented as follows:
 - **Metric**: Packetbeat request http bytes
 - **Threshold**: The sum of all HTTP requests must exceed 3500 bytes in a single minute
 - **Vulnerability Mitigated**: With this alert you can prevent a DDOS.
 - **Reliability**: This doesn't create very many false positives. Medium



CPU Usage Monitor

CPU Usage Monitor is implemented as follows:
 - **Metric**: System cpu processes.
 - **Threshold**: If system processes goes over 0.5 per every 5 minutes.
 - **Vulnerability Mitigated**: By keeping the CPU usage under 50% you can prevent a virus or malware.
 - **Reliability**: TODO: This can make a few false positives because everytime you start processes there can be a spike. Low



Suggestions for Going Further (Optional)
TODO:
- 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
  - **Patch**: TODO: E.g., _install `special-security-package` with `apt-get`_
  - **Why It Works**: TODO: E.g., _`special-security-package` scans the system for viruses every day_
- Vulnerability 2
  - **Patch**: TODO: E.g., _install `special-security-package` with `apt-get`_
  - **Why It Works**: TODO: E.g., _`special-security-package` scans the system for viruses every day_
- Vulnerability 3
  - **Patch**: TODO: E.g., _install `special-security-package` with `apt-get`_
  - **Why It Works**: TODO: E.g., _`special-security-package` scans the system for viruses every day_