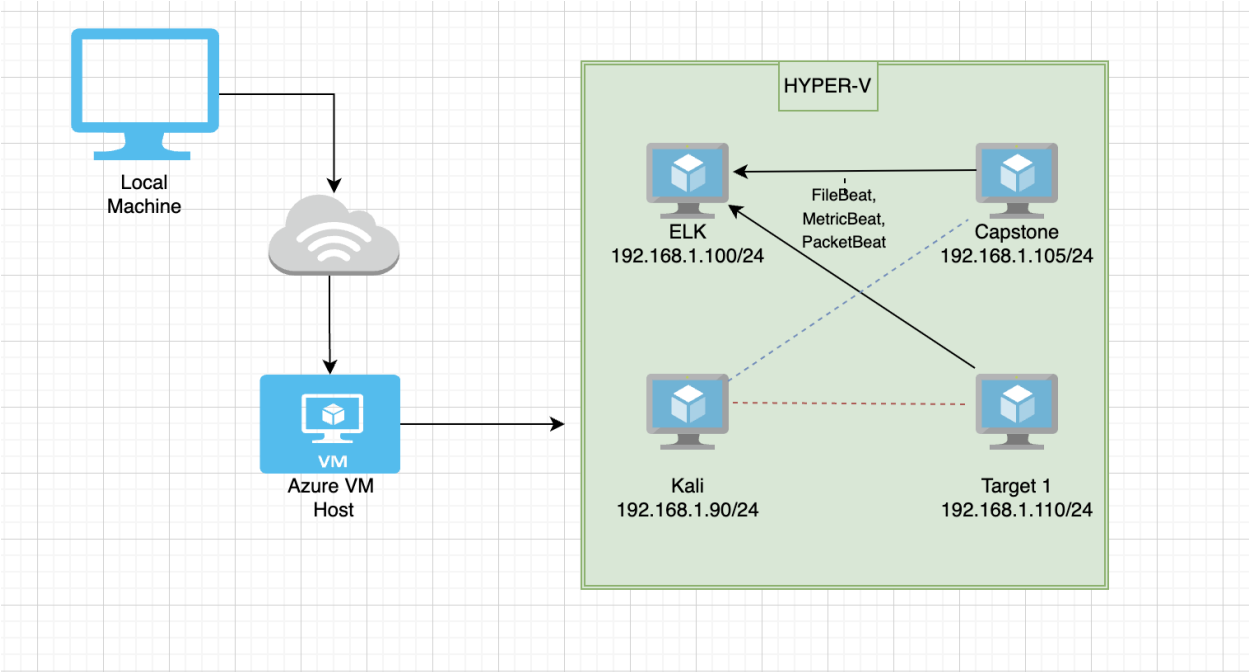
Network Topology



The following machines were identified on the network:

- Kali
  - **Operating System**: Linux
  - **Purpose**: Attacking Machine
  - **IP Address**: 192.168.1.90/24
- Target 1
  - **Operating System**: Linux
  - **Purpose**: wordpress host / machine being attacked
  - **IP Address**: 192.168.1.110
- Capstone
  - **Operating System**: Ubuntu
  - **Purpose**: wordpress host / machine being attacked
  - **IP Address**:192.668.1.105
- ELK

    - **Operating System**: Ubuntu
    - **Purpose**: Observation ELK stack with Kibana
    - **IP Address**: 192.168.1.100

Description of Targets

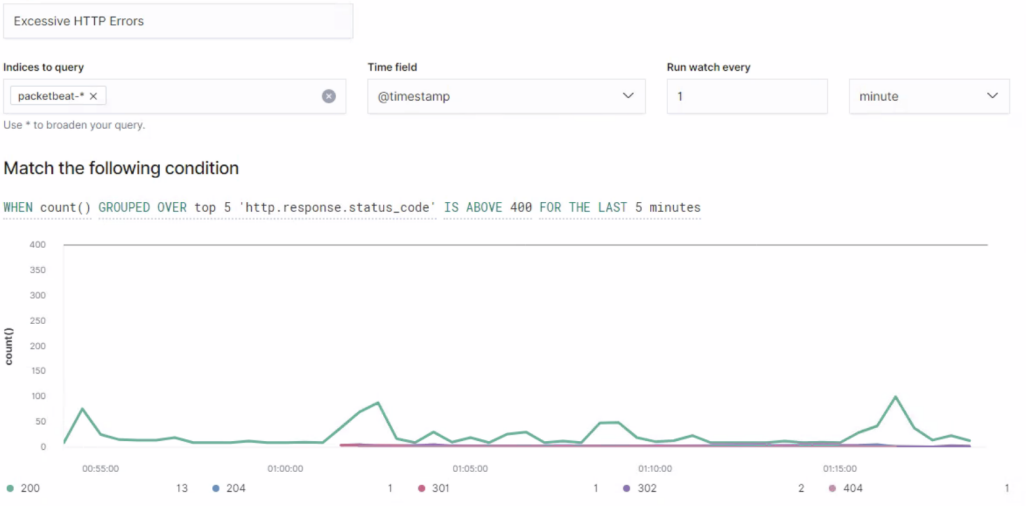
Target 1 - 192.168.1.110/24

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

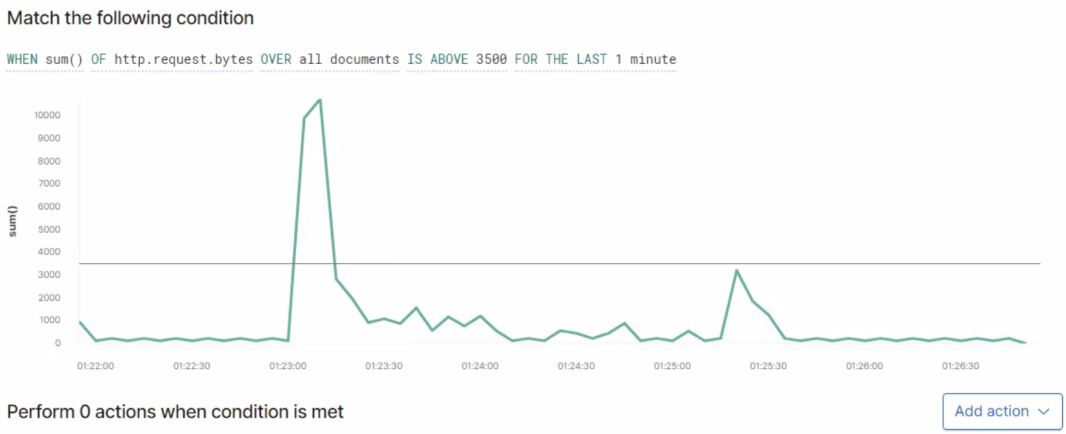
Traffic to these services should be carefully monitored. To this end, we have implemented the alerts below:

HTTP ERRORS

- **Metric**: WHEN count() GROUPED OVER top 5 'http.response.status_code' IS ABOVE 400 FOR THE LAST 5 minutes
- **Threshold**: >400
- **Vulnerability Mitigated**: Brute Force
- **Reliability**: Monitoring error codes in the 400s is a reliable method of mitigation
- 

HTTP byte request

- **Metric**: WHEN sum() of http.request.bytes OVER all documents IS ABOVE 3500 FOR THE LAST 1 minute
- **Threshold**: >3500

- **Vulnerability Mitigated**: HTTP requests
- **Reliability**: legitimate files with large sizes could trigger a false positive
- 

PCU Usage

- **Metric**: WHEN max() OF system.process.cpu.total.pct OVER all documents IS ABOVE 0.5 FOR THE LAST 5 minutes
- **Threshold**: >0.5
- **Vulnerability Mitigated**: Drain on network bandwidth and resources
- **Reliability**: Malware running can reliably be determined by CPU usage
-