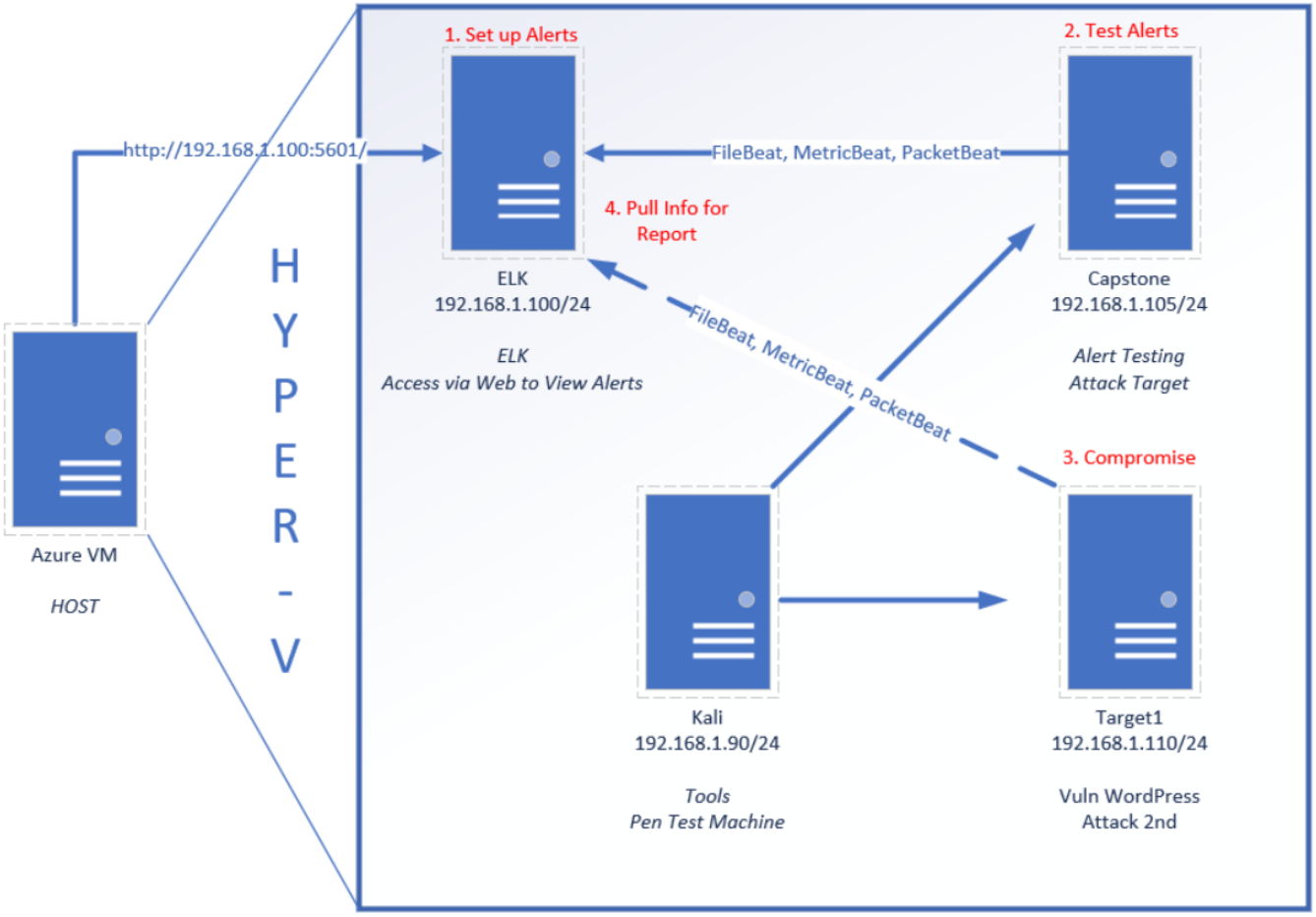
Blue Team: Summary of Operations

Table of Contents

Network Topology



The following machines were identified on the network:

- Name of VM 1

  - **Operating System**: Linux Kali

  - **Purpose**: Pen Testing Machine

  - **IP Address**: 192.168.1.90/24

- Name of VM 2

  - **Operating System**: Ubuntu 18.04.4 LTS

  - **Purpose**: ElK server: collecting logs, holds Kibana dashboard.

  - **IP Address**: 192.168.1.100/24

-Name of VM 3 (Target Machine)

- **Operating System**: Debian Linux

  - **Purpose**: Vulnerable word Press

  - **IP Address**: 192.168.1.110/24

-Name of VM 3 (Capstone)

- **Operating System**: Ubuntu 18.04

  - **Purpose**: To test alerts

  - **IP Address**: 192.168.1.105/24

Description of Targets

The target of this attack was: `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

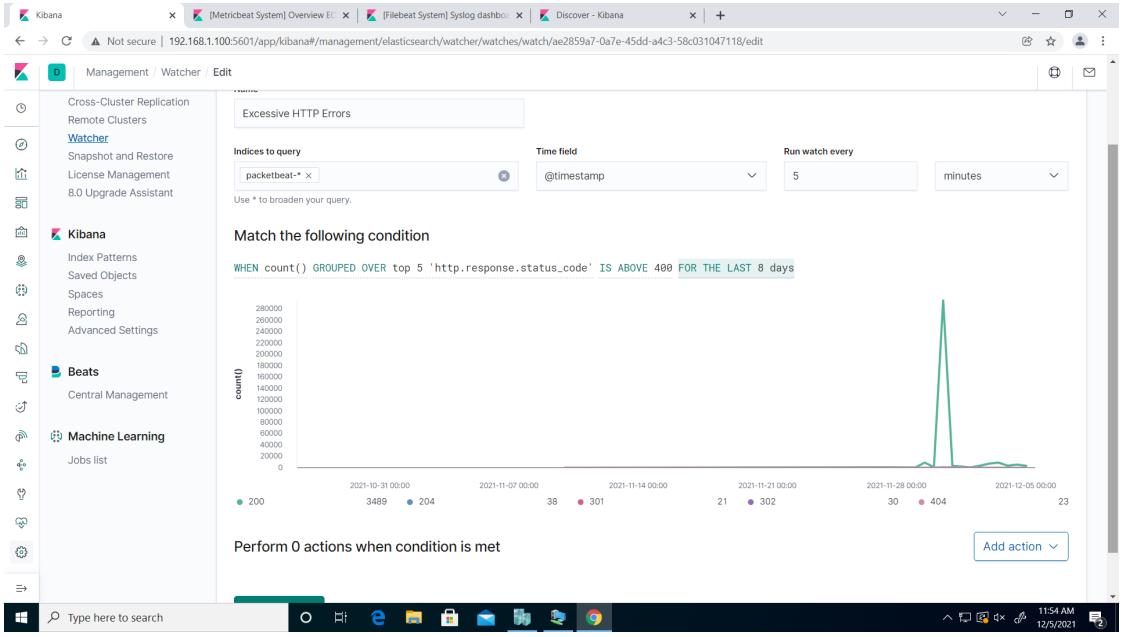
Traffic to these services should be carefully monitored. To this end, we have implemented the alerts below:

Excessive HTTP Errors

Alert 1 is implemented as follows:

WHEN count() GROUPED OVER top 5 'http.response.status_code' IS ABOVE 400 FOR THE LAST 5 minutes

- **Metric**: WHEN count() GROUPED OVER top 5 'http.response.status_code'
- **Threshold**: Above 400
- **Vulnerability Mitigated**: Deploying WAF Web Application Firewall that blocks or sanitizes http requests.
- **Reliability**: It could create a lot of false positives, if not properly configured or not obtained required level of protection of application.



HTTP Request Size Monitor

Alert 2 is implemented as follows:

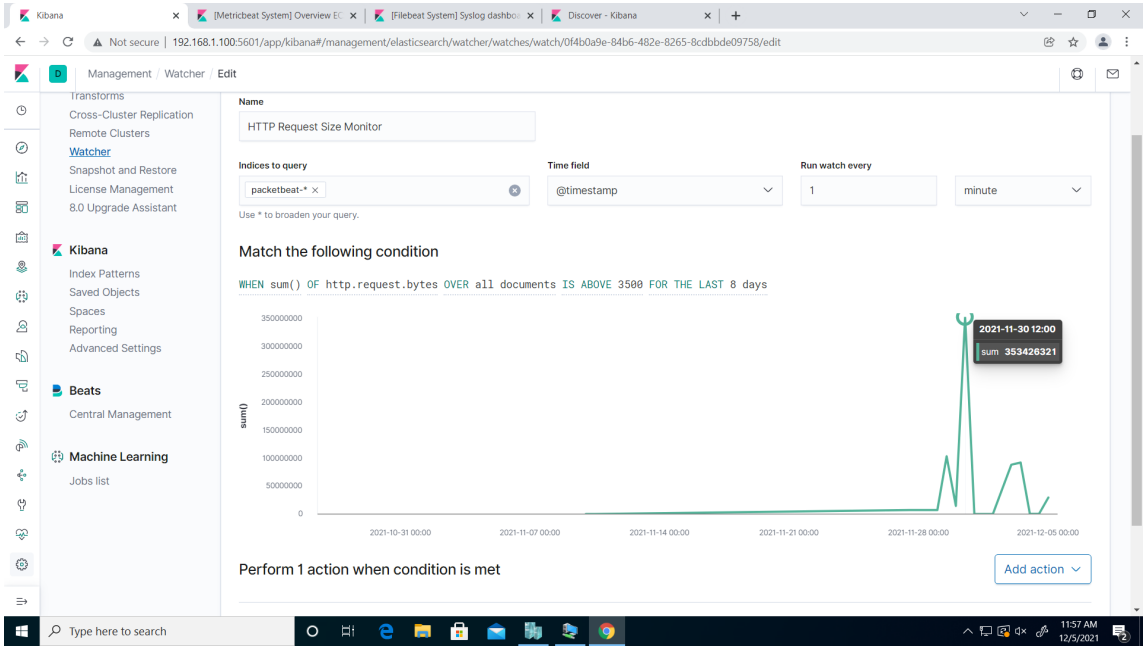
WHEN sum() of http.request.bytes OVER all documents IS ABOVE 3500 FOR THE LAST 1 minute

- **Metric**: WHEN sum() of http.request.bytes

- **Threshold**: Above 3500

- **Vulnerability Mitigated**: Whitelisting of IP addresses, Disabling directory lists.

- **Reliability**: Yes, could create false positives.



CPU Usage Monitor

Alert 3 is implemented as follows:

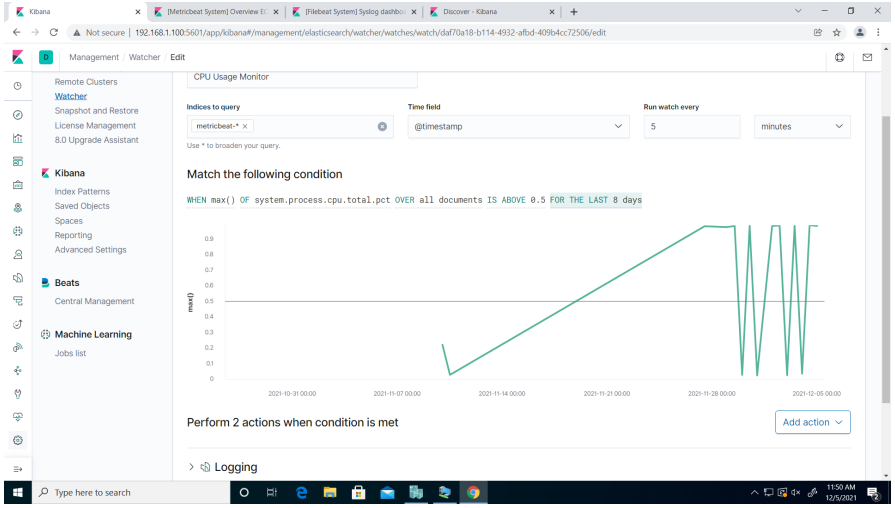
WHEN max() OF system.process.cpu.total.pct OVER all documents IS ABOVE 0.5 FOR THE LAST 5 minutes

- **Metric**: WHEN max() OF system.process.cpu.total.pct OVER all documents

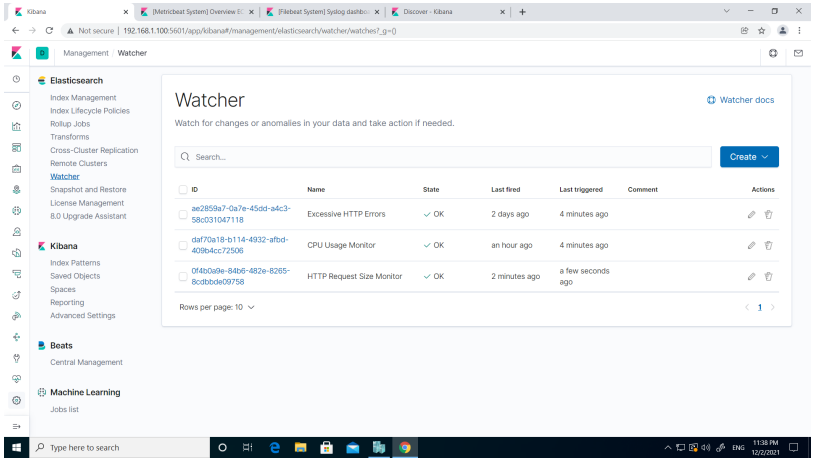
- **Threshold**: Above 0.5

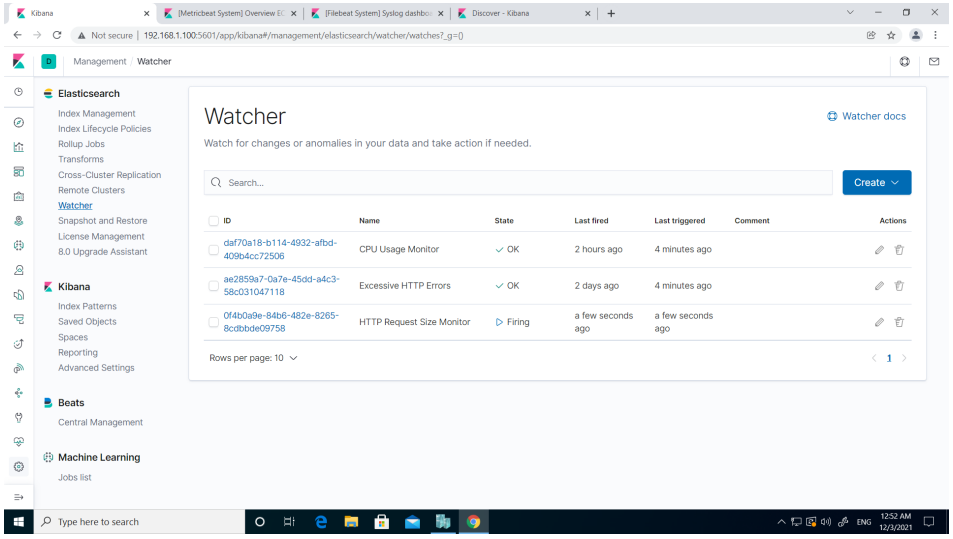
- **Vulnerability Mitigated**: Avoid installing too many softwares on web server and keep the software up-to-date.

- **Reliability**: Yes, if the software is not regularly updated, the probability of many false positives does exist.



Watcher Screenshots





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_