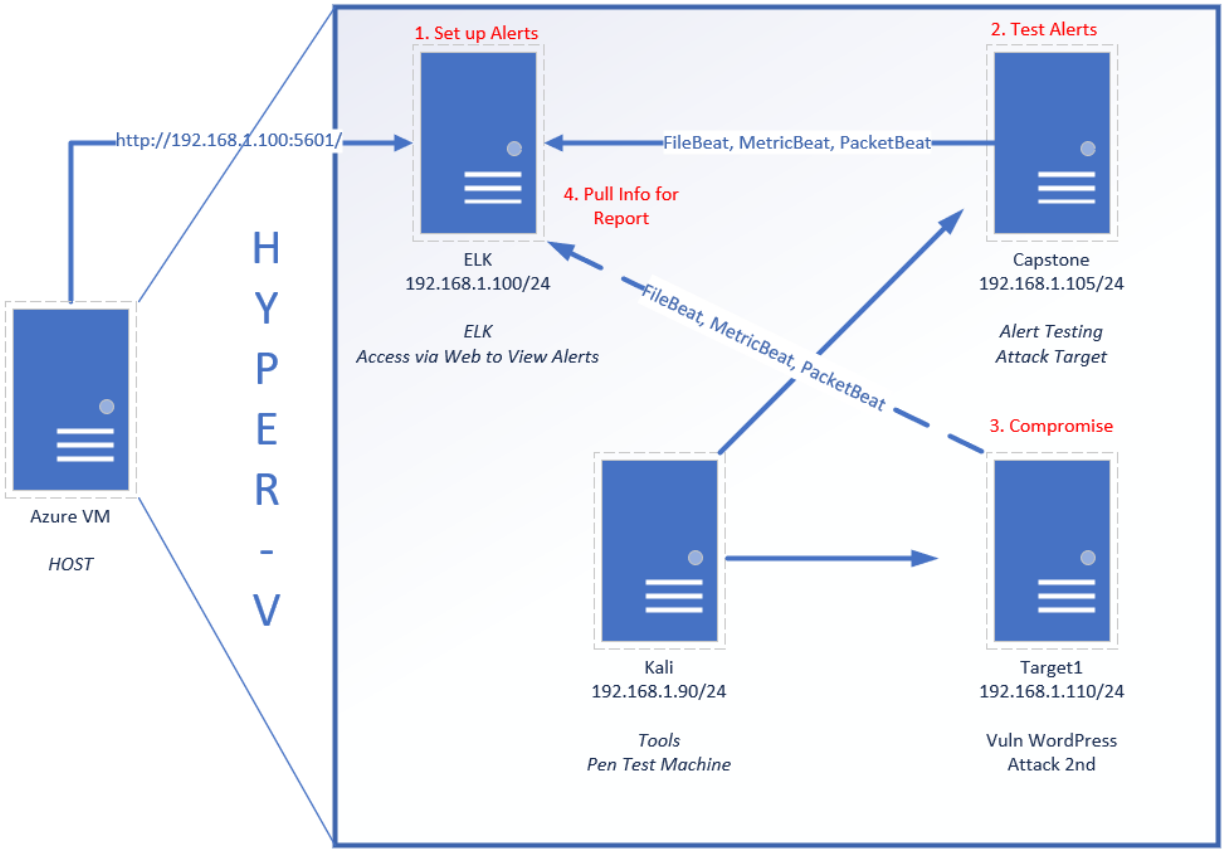
Blue Team: Summary of Operations

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:



- ELK
    - **Operating System**: Linux
    - **Purpose**:Set up Alerts/ability to pull information for reports
    - **IP Address**:192.168.1.100/24
- CAPSTONE
    - **Operating System**: Ubuntu Linux
    - **Purpose**: Test Alerts/Target of Attack
    - **IP Address**:192.168.1.105/24
- Target1
    - **Operating System**: Debian Linux
    - **Purpose**: System being tested by compromising it

        - **IP Address**:192.168.1.110/24
- KALI
        - **Operating System**: Kali Linux
        - **Purpose**: Pentesting Machine
        - **IP Address**:192.168.1.90/24

Description of Targets

The target of this attack was: **Target1@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:

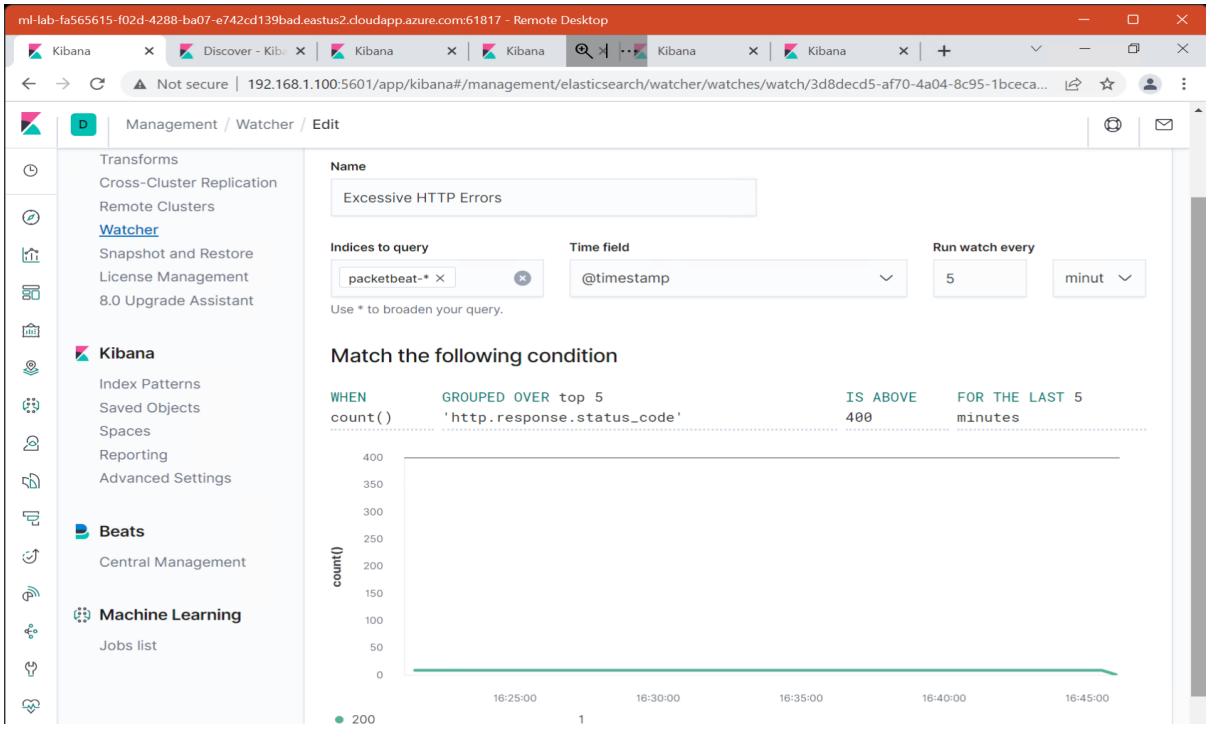
Monitoring the Targets

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

Excessive HTTP Errors

Alert 1 is implemented as follows:

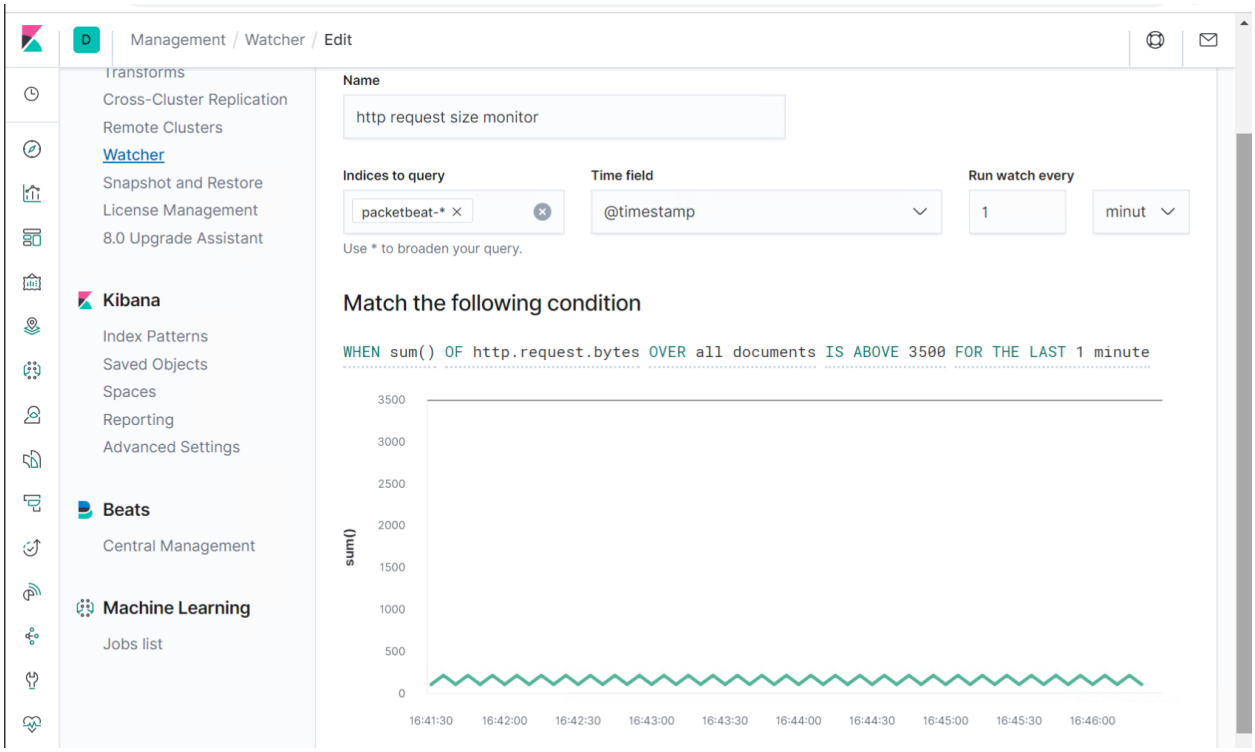
- **Metric**: Packetbeat
- **Threshold**: If the top 5 HTTP response code is above 400 for the last 5 minutes
- **Vulnerability Mitigated**: Alerts on potential brute force attacks on the web server.
- **Reliability**: This alert is rated as **HIGH** and **RELIABLE** as all of the alerts were triggered due to the threshold being above 5 HTTP error codes (400), signaling suspicious activity.



HTTP Request Size Monitor

Alert 2 is implemented as follows:

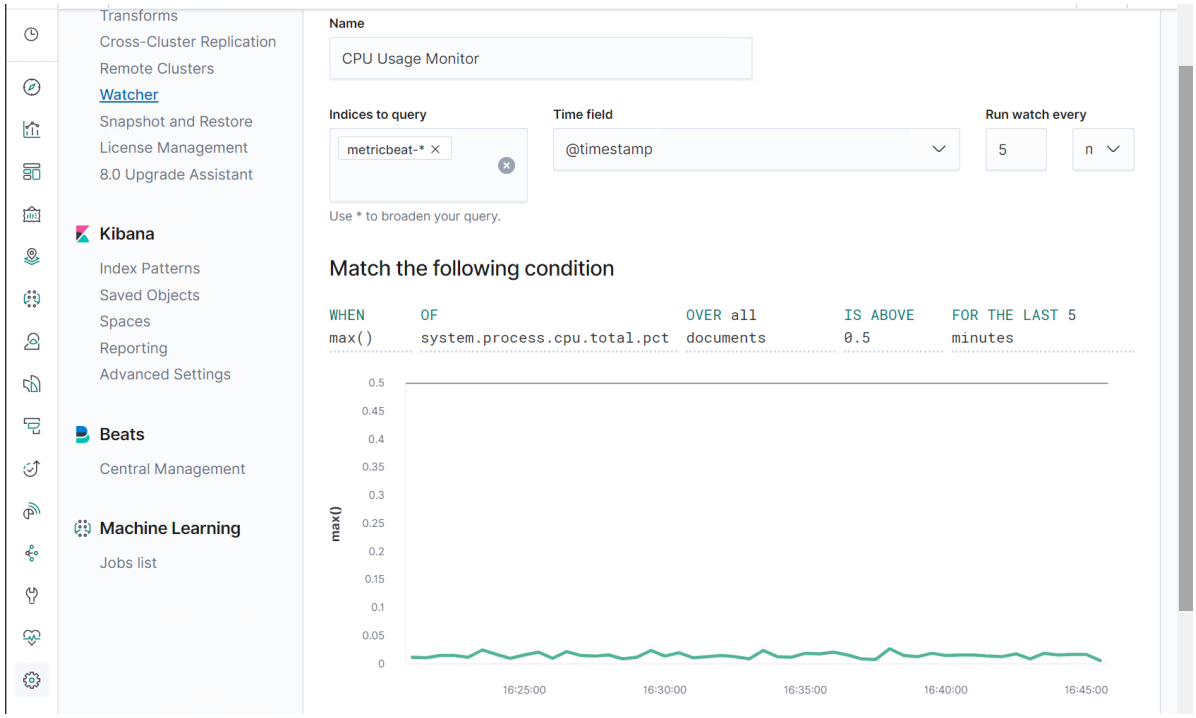
- **Metric**: Packetbeat
- **Threshold**: If the number of HTTP requests per minute exceeds 3500
- **Vulnerability Mitigated**: Measures the amount of HTTP requests which could indicate an attack if there is an overwhelming amount of requests, potentially DDoS attacks.
- **Reliability**: This alert is rated as **HIGH** and **RELIABLE** due to the accuracy of the alerts measuring true attacks rather than false negatives or positives.

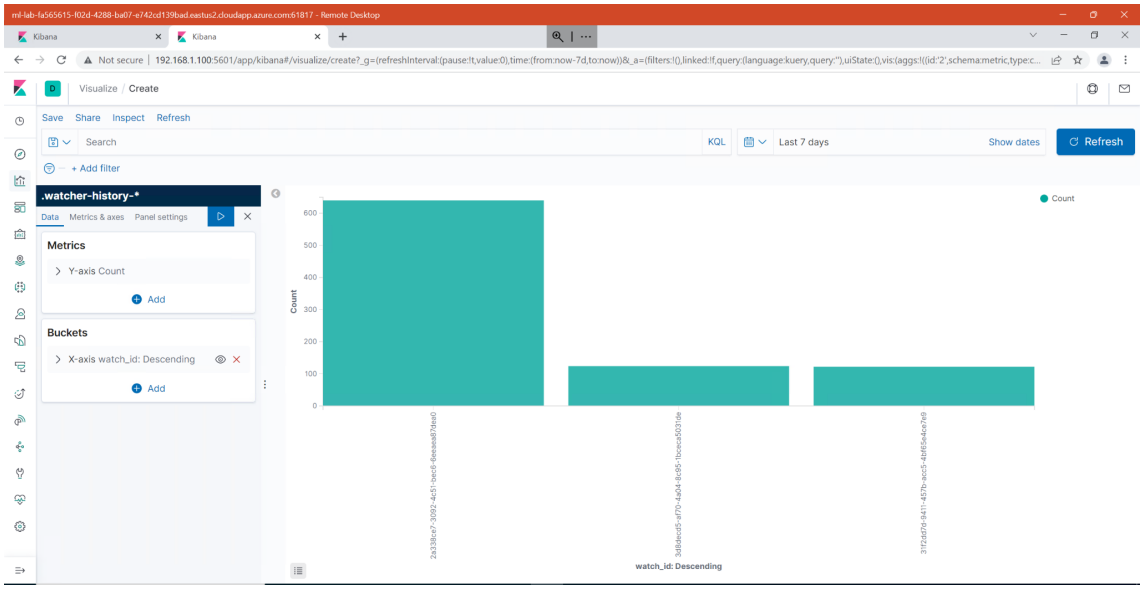


CPU Usage Monitor

Alert 3 is implemented as follows:

- **Metric**: Metricbeat/ WHEN max() OF system.process.cpu.total.pct OVER all documents
- **Threshold**: If the CPU total exceeds 0.5 usage over the past 5 minutes
- **Vulnerability Mitigated**: This monitors the CPU usage in order to determine if there is any malware software that uses an extreme amount of processing power.
- **Reliability**: The alert is rated as **LOW** and **UNRELIABLE** as it generated many false positives, even when the CPU was not targeted.


Transforms
Cross-Cluster Replication
Remote Clusters
Watcher
Snapshot and Restore
License Management
8.0 Upgrade Assistant
Kibana
Index Patterns
Saved Objects
Spaces
Reporting
Advanced Settings
Beats
Central Management
Machine Learning
Jobs list
Name
CPU Usage Monitor
Indices to query
metricbeat-* ×
Time field
@timestamp
Run watch every
5
n
Use * to broaden your query.
Match the following condition
WHEN
max()
OF
system.process.cpu.total.pct
OVER all
documents
IS ABOVE
0.5
FOR THE LAST 5
minutes
max()
0.5
0.45
0.4
0.35
0.3
0.25
0.2
0.15
0.1
0.05
0
16:25:00
16:30:00
16:35:00
16:40:00
16:45:00


Visualize / Create
Save
Share
Inspect
Refresh
Search
KQL
Last 7 days
Show dates
Refresh
+ Add filter
.watcher-history-*
Data
Metrics & axes
Panel settings
Metrics
Y-axis Count
Add
Buckets
X-axis watch_id: Descending
Add
Count
watch_id: Descending