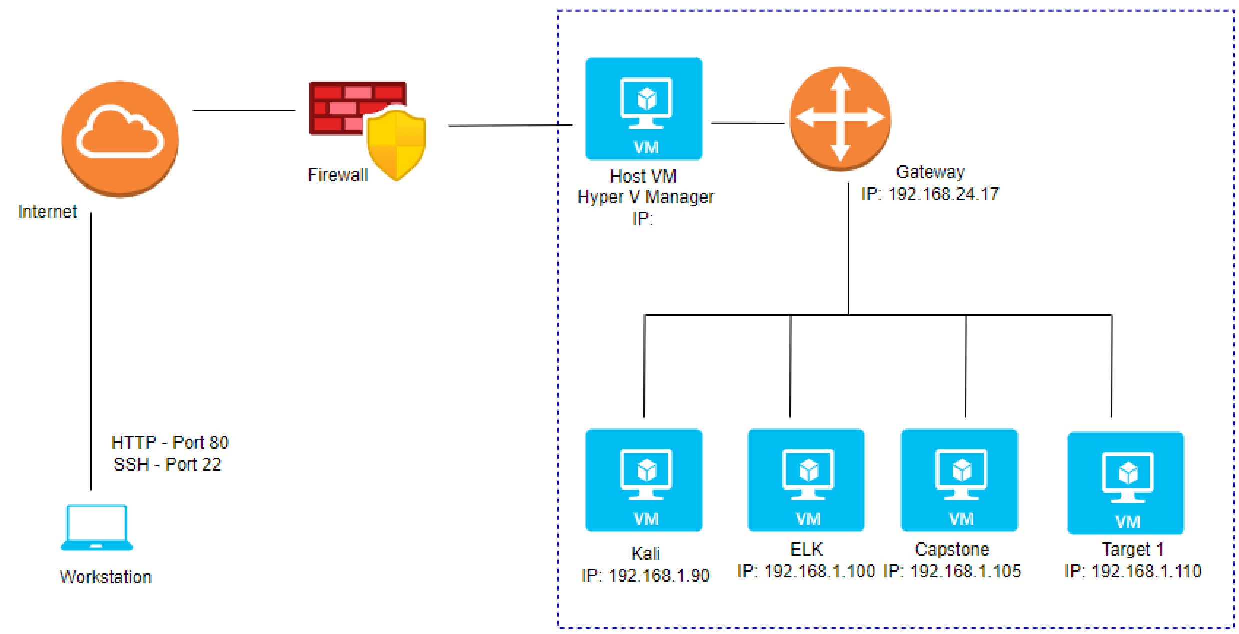
Blue Team: Summary of Operations

Table of Contents

Network Topology



The following machines were identified on the network:

- Name of VM 1: Hyper V Host Manager
  - Operating System: Windows 10
  - Purpose: Contains the target, attack, and data logging virtual machines
  - IP Address: 192.168.1.1

- Name of VM 2: Kali
  - Operating System: Linux
  - Purpose: Utilized as attacking virtual machine
  - IP Address: 192.168.1.90

- Name of VM 3: Capstone
  - Operating System: Linux (Ubuntu)

    - Purpose: Utilized as a testing system for alerts
    - IP Address: 192.168.1.105

- Name of VM 4: ELK
    - Operating System: Linux (Ubuntu)
    - Purpose: Utilized for gathering information from the target machine using Metricbeat, Filebeat, and Packetbeat
    - IP Address: 192.168.1.100

- Name of VM 5: Target 1
    - Operating System: Linux
    - Purpose: Utilized as target virtual machine and contains a WordPress server
    - IP Address: 192.168.1.110

Description of Targets

The target of this attack was: Target 1 (IP: 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:

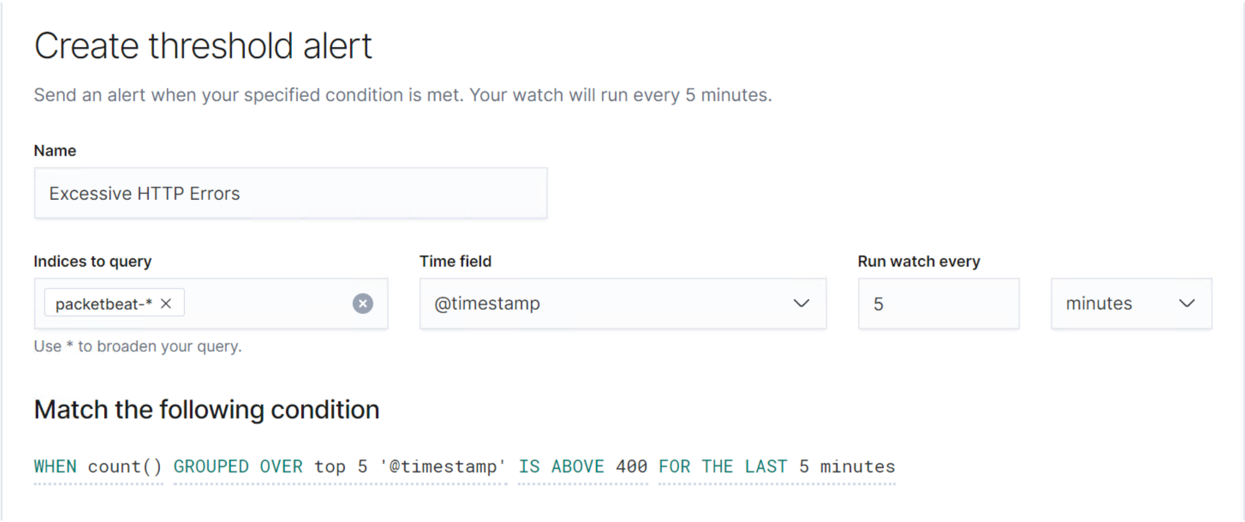
Monitoring the Targets

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

1. Excessive HTTP Errors

Excessive HTTP Errors alert is implemented as follows:

- Metric: Packetbeat
- Threshold: When count() grouped over top5 ‘http.response.status_code’ is above 400 for the last 5 minutes
- Vulnerability Mitigated:
    - Unauthorized IP addresses
    - Open Port 22
- Reliability: Medium
    - The alert will not flag excessive false positives to confuse with potential brute-force attacks



Create threshold alert

Send an alert when your specified condition is met. Your watch will run every 5 minutes.

Name: Excessive HTTP Errors

Indices to query: packetbeat-*

Use * to broaden your query.

Time field: @timestamp

Run watch every: 5 minutes

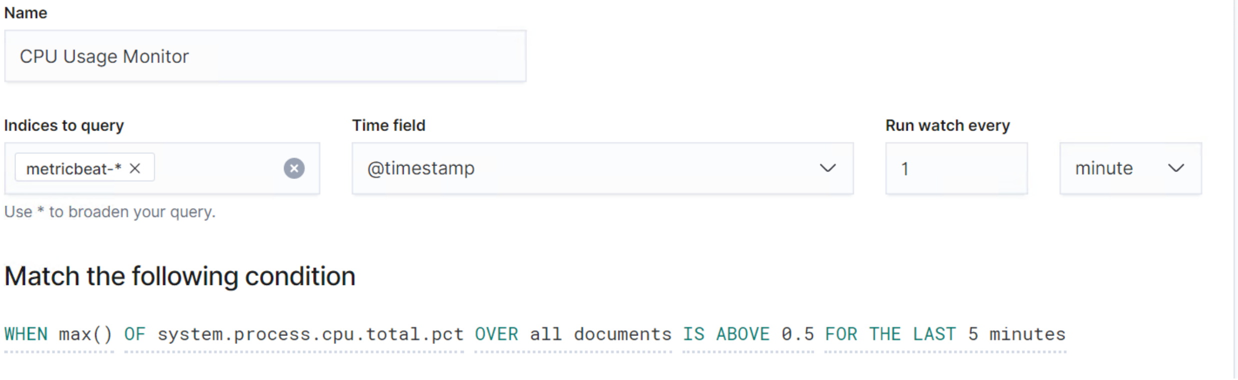
Match the following condition

```
WHEN count() GROUPED OVER top 5 '@timestamp' IS ABOVE 400 FOR THE LAST 5 minutes
```

2. CPU Usage Monitor

CPU Usage Monitor alert 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: Malware that uses high amounts of CPU
- Reliability: Medium. The alert can flag false positives if normal programs or new softwares are being installed and run



Name: CPU Usage Monitor

Indices to query: metricbeat-*

Use * to broaden your query.

Time field: @timestamp

Run watch every: 1 minute

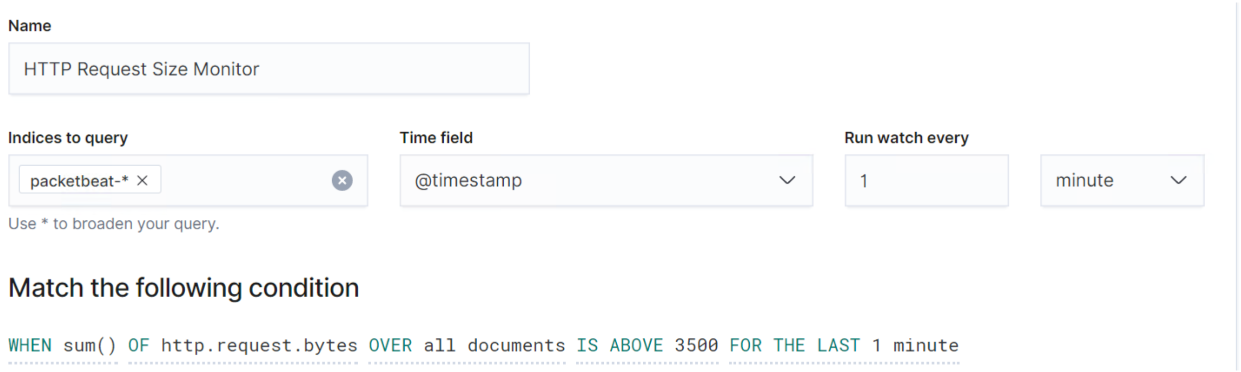
Match the following condition

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

3. HTTP Request Size Monitor

HTTP Request Size alert 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: DDOS attacks
- Reliability: Medium. The alert is likely to not flag excessive false positives



Name

HTTP Request Size Monitor

Indices to query

packetbeat-* ×

Use * to broaden your query.

Time field

@timestamp

Run watch every

1

minute

Match the following condition

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