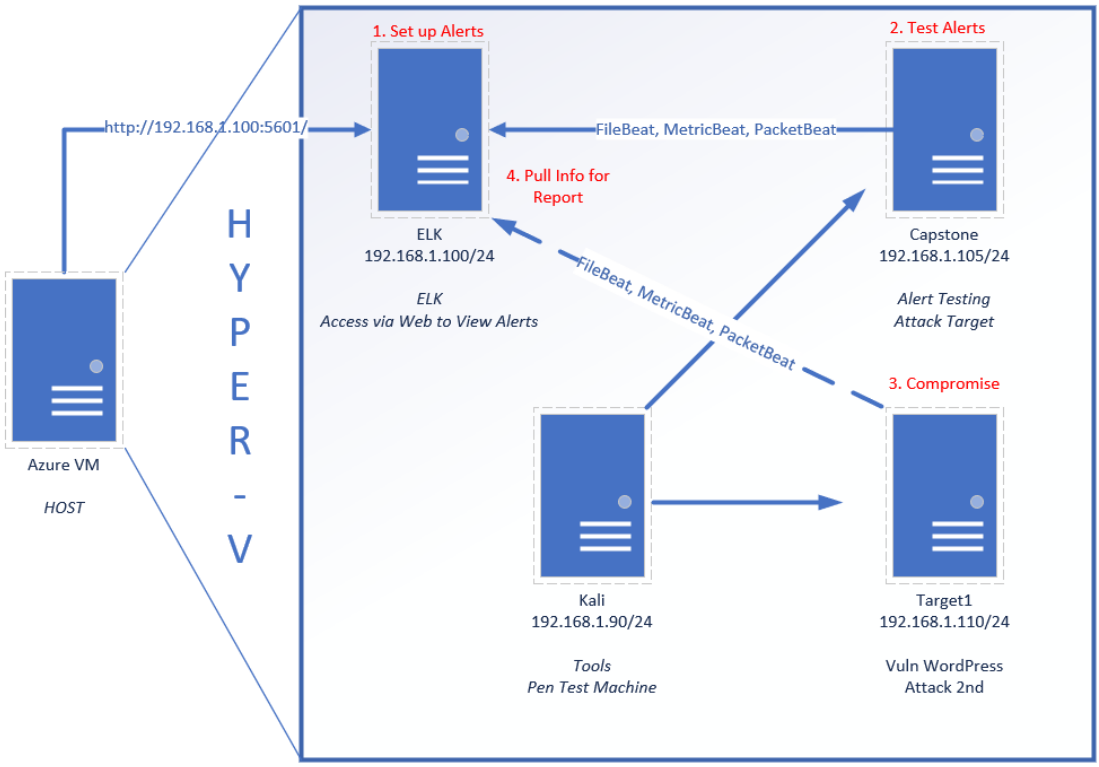
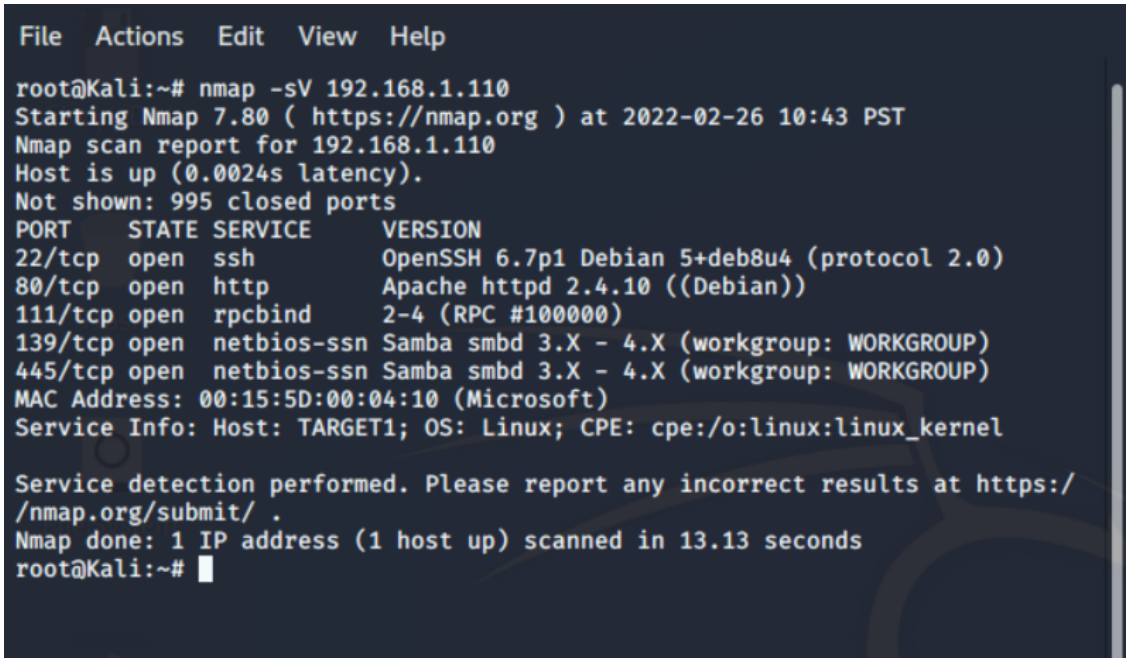
Defensive: Summary of Operations

Table of Contents

Network Topology





The following machines where identified on the network:

- Name of VM 1:Target 1
    - **Operating System**:Linux
    - **Purpose**:Word press server
    - **IP Address**:192.168.1.110
- Name of VM 2
    - **Operating System**:
    - **Purpose**:
    - **IP Address**:
- Etc.

Description of Targets

The target of this attack was: Target 1 ip. 192.168.1.110

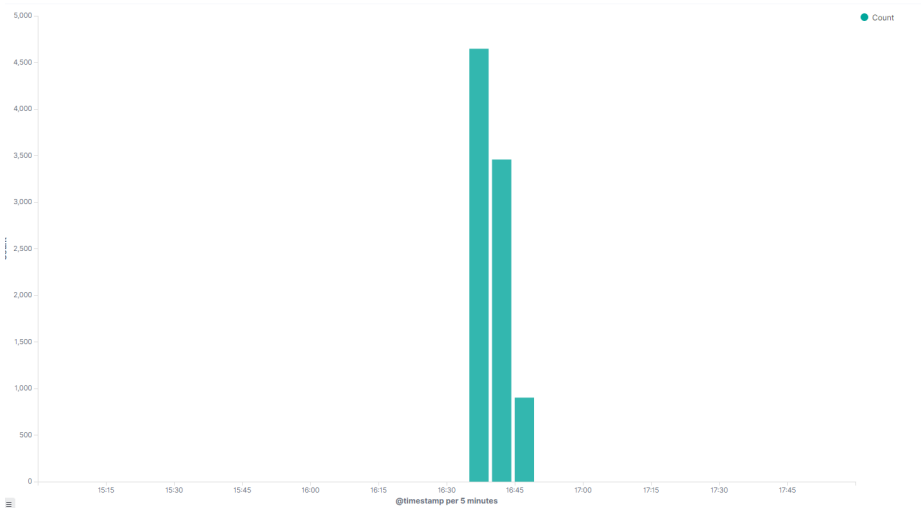
Target 1 is an Apache web server and has SSH enabled, so ports 80 and 22 are possible ports of entry for attackers. As such, the following alerts have been implemented:

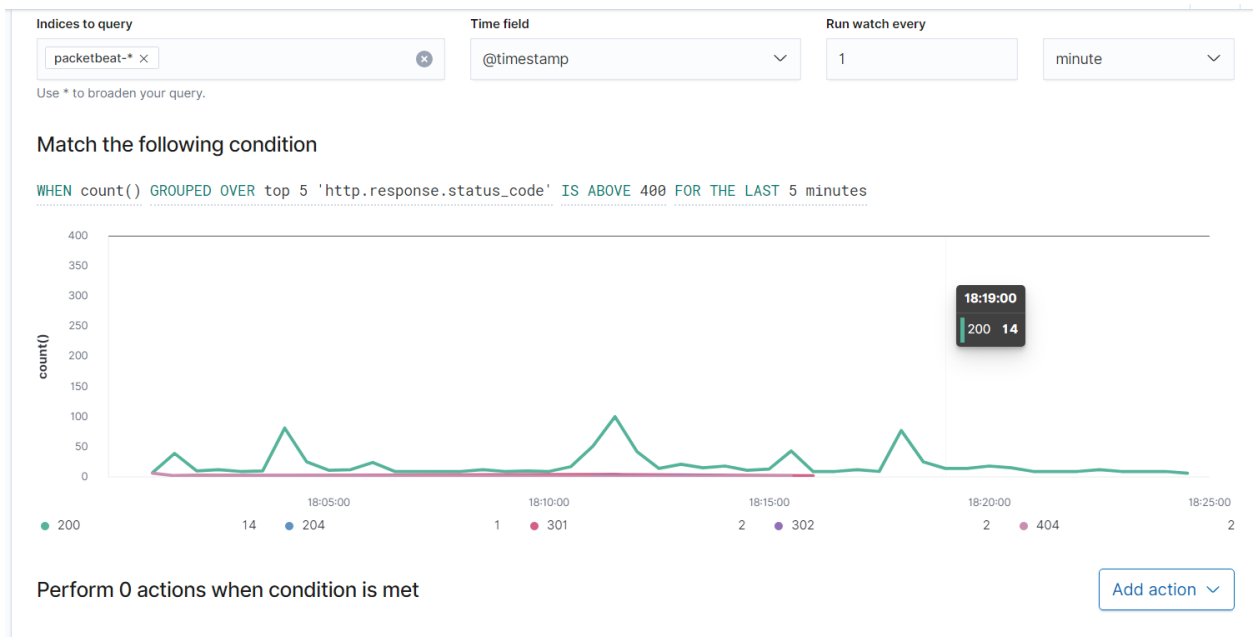
Monitoring the Targets

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

Name of Alert 1

Excessive HTTP Errors is implemented as follows:

- **Metric**: http.respnose.status_code
- **Threshold**:http://response.status_code> 400
- **Vulnerability Mitigated**: Brute Force Attack
- **Reliability**: This alert does not generate false positives. I feel that it is a highly reliable alert for monitoring a brute force attack.
-


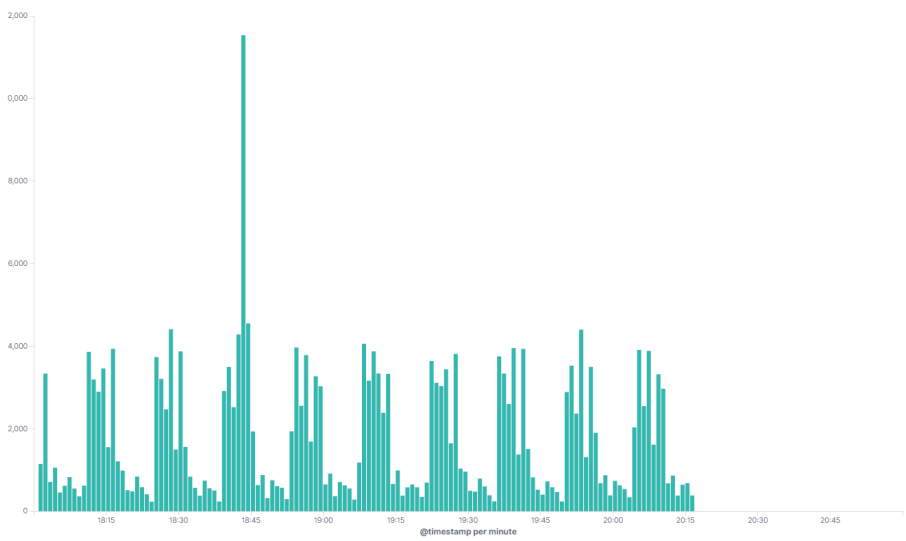
-


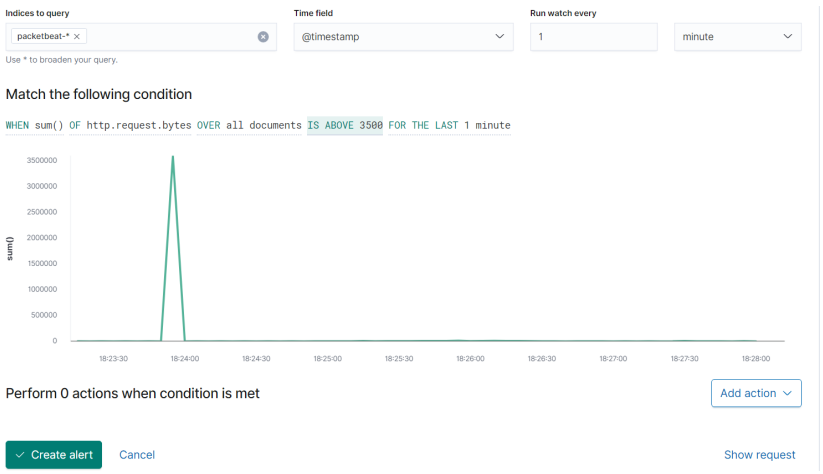
-

Name of Alert 2

HTTP Request Size Monitor is implemented as follows:

- **Metric**:http.request.bytes
- **Threshold**: 3500 hits in 1 min
- **Vulnerability Mitigated**: DDOS
- **Reliability**: No false positives. I feel the reliability is medium due to the number of hits over 3500 but not much higher than 5000.

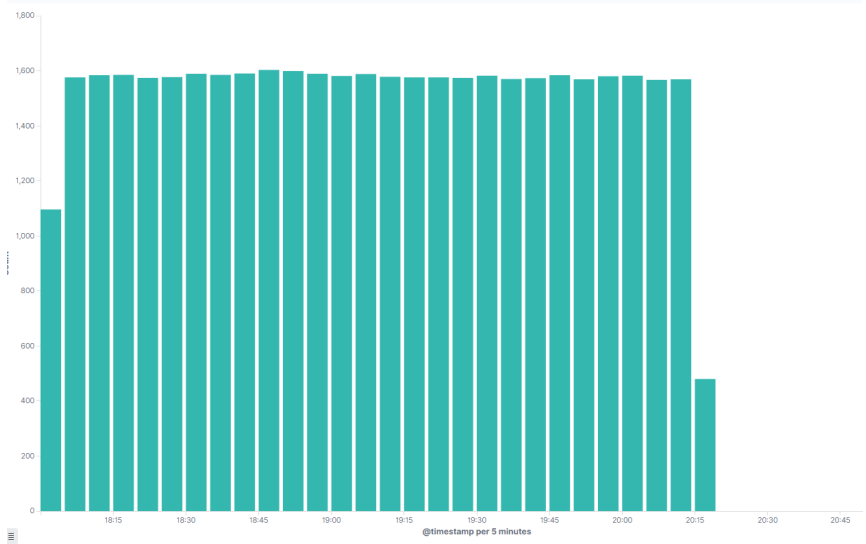


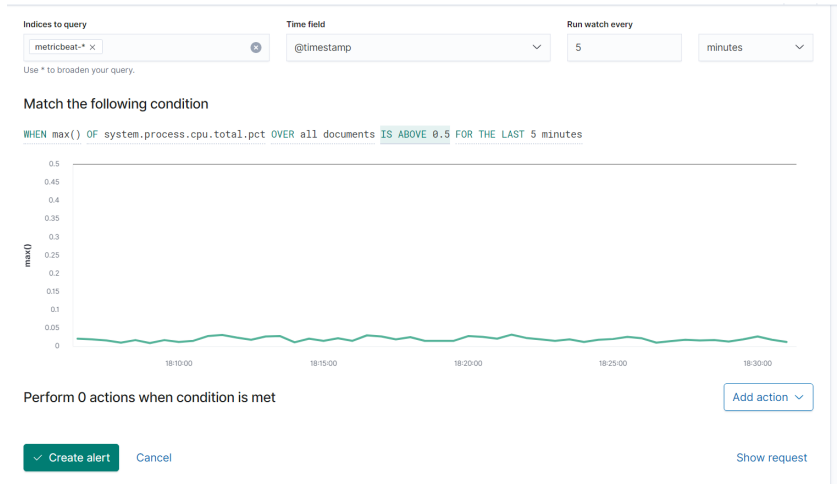
- 

Name of Alert 3:

CPU Usage Monitor is implemented as follows:

- **Metric**: system.process.cpu.total.pct
- **Threshold**: 0.5 usage every 5 minutes
- **Vulnerability Mitigated**: Malware
- **Reliability**: TODO: This alert will generate a lot of false positives. I would rate this alert low.

- 
1,800
1,600
1,400
1,200
1,000
800
600
400
200
0
18:15
18:30
18:45
19:00
19:15
19:30
19:45
20:00
20:15
20:30
20:45
@timestamp per 5 minutes

- 
Indices to query
metricbeat-* ×
Use * to broaden your query.
Time field
@timestamp
Run watch every
5
minutes
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
18:10:00
18:15:00
18:20:00
18:25:00
18:30:00
Perform 0 actions when condition is met
Add action
Create alert
Cancel
Show request