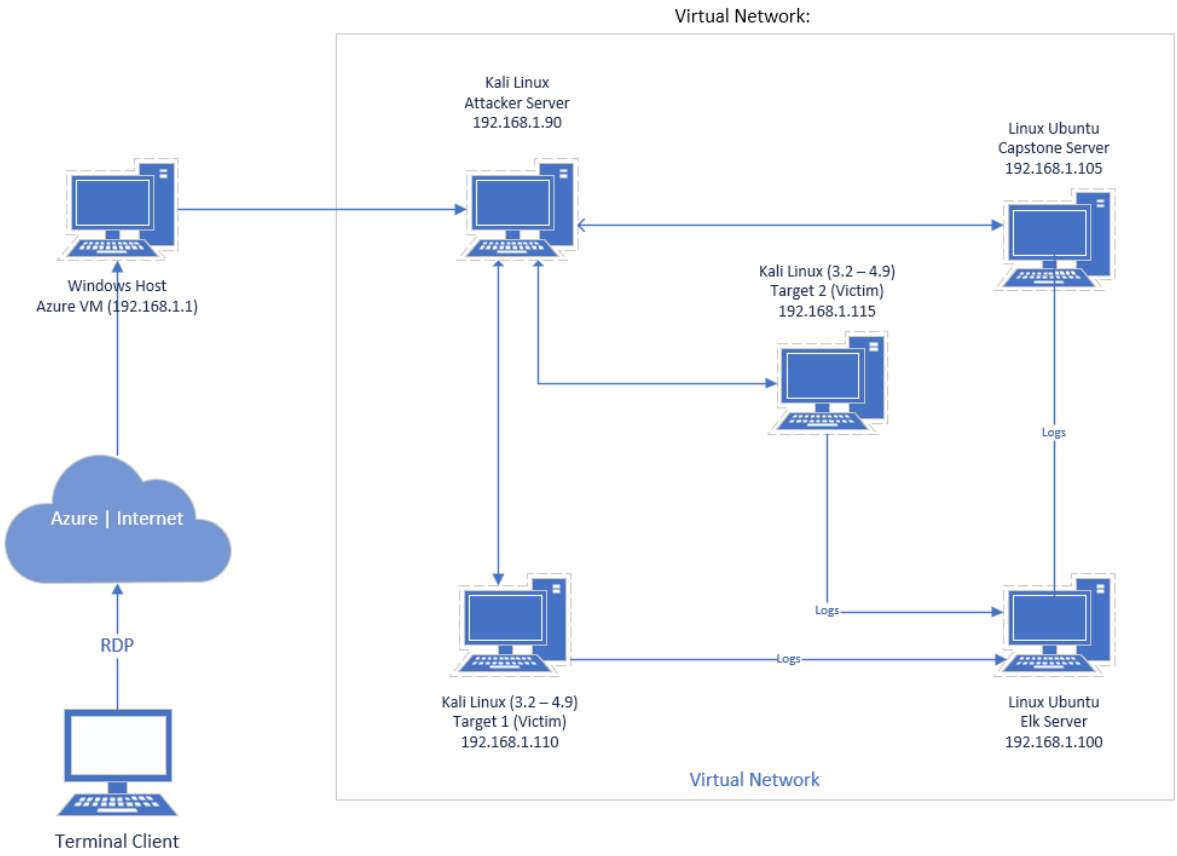
Blue Team: Summary of Operations

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:

- VM : Target 1
    - **Operating System**: Linux 3.2 -4.9

    - **Purpose**: Victim Machine First Target
    - **IP Address**: 192.168.1.110

- VM : Target 2
    - **Operating System**: Linux 3.2 – 4.9
    - **Purpose**: Second Victim Machine to Attack
    - **IP Address**: 192.168.1.115

- VM : Elk
    - **Operating System**: Linux
    - **Purpose**: gathers all info from other servers and prepares it for presentation within Kabana.
    - **IP Address**: 192.168.1.100

- VM : Kali
    - **Operating System**: Linux 2.6.32
    - **Purpose**: Used to attack Target machines
    - **IP Address**: 192.168.1.90

- VM : Capstone
    - **Operating System**: Linux
    - **Purpose**: Test Machine
    - **IP Address**: 192.168.1.105

- VM : Gateway
    - **Operating System**: Microsoft Windows XP|7|2008
    - **Purpose**: Gateway into other machines
    - **IP Address**: 192.168.1.1

Description of Targets

The target of this attack was: Target 1 (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:

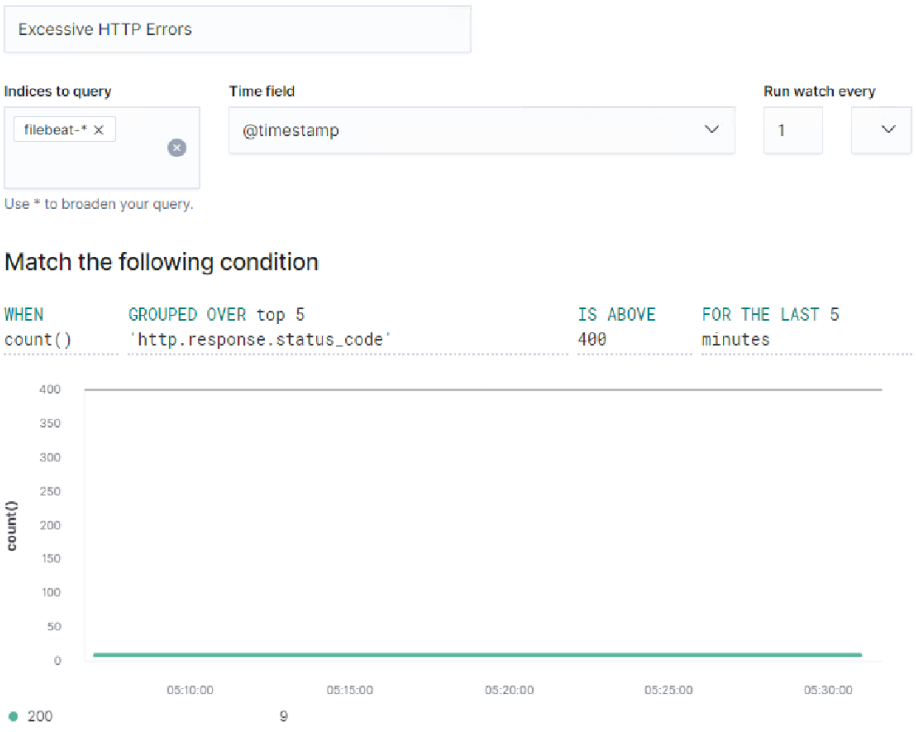
Monitoring the Targets

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:

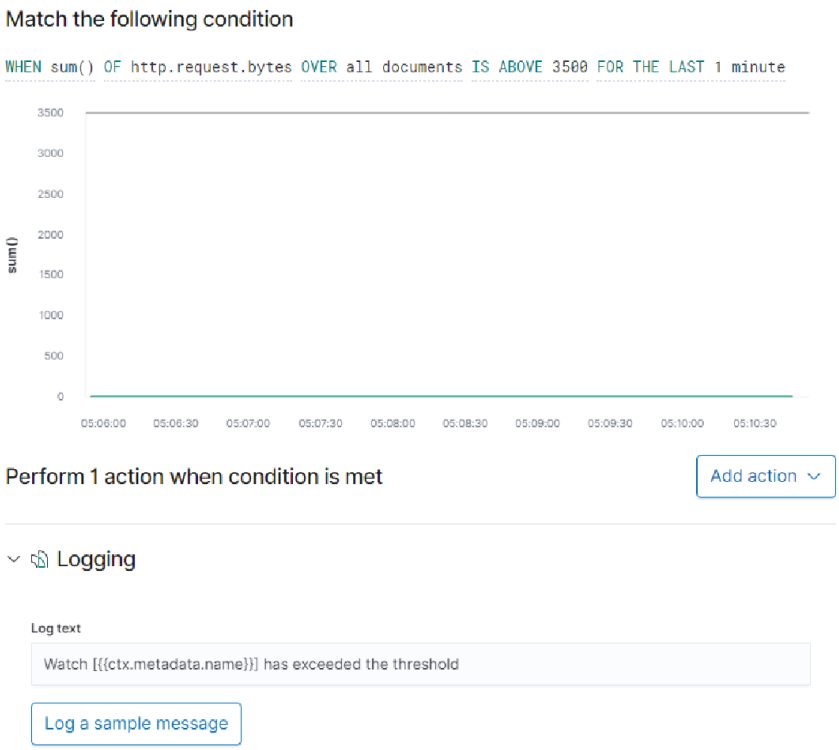
- **Metric**: **http.response.status_code**
- **Threshold**: **400 requests in 5 minutes.**
- **Vulnerability Mitigated**: **Packet Flooding**
- **Reliability**: **Low. False positives generated. Vast majority of requests were 200 OK, which would still trigger the alert.**



Name of Alert 2: HTTP Request Size Monitor

Alert 2 is implemented as follows:

- **Metric**: http.request.bytes
- **Threshold**: 3500+
- **Vulnerability Mitigated**: Log
- **Reliability**: Medium. There can be false positives as it can be common for large legitimate http requests and traffic.



-
-

CPU Usage Monitor

CPU Usage Monitor is implemented as follows:

- **Metric**: MetricBeat
- **Threshold**: all documents above 0.5 in the last 5 minutes
- **Vulnerability Mitigated**: will detect any process that use excessive processing power
- **Reliability**: TODO: Does this alert generate lots of false positives/false negatives? Rate as low, medium, or high reliability.
    - Highly Reliable. Can also be used to improve machine performance.

CPU Usage Monitor

Indices to query

metricbeat-* ×

Time field

@timestamp

Run watch every

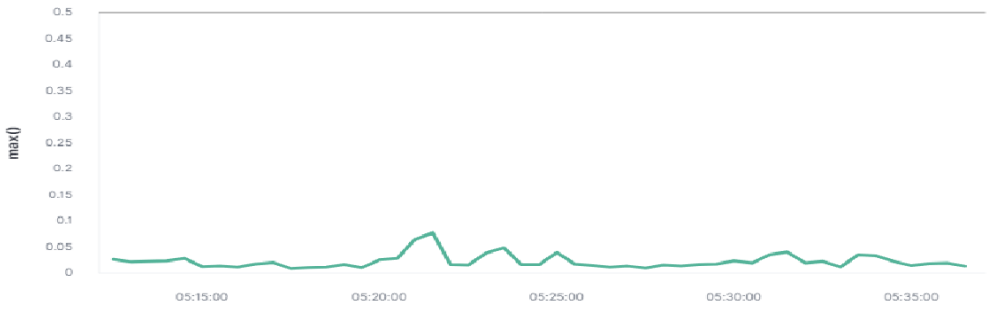
1

mi

Use * to broaden your query.

Match the following condition

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



Perform 1 action when condition is met

Add action

> Logging