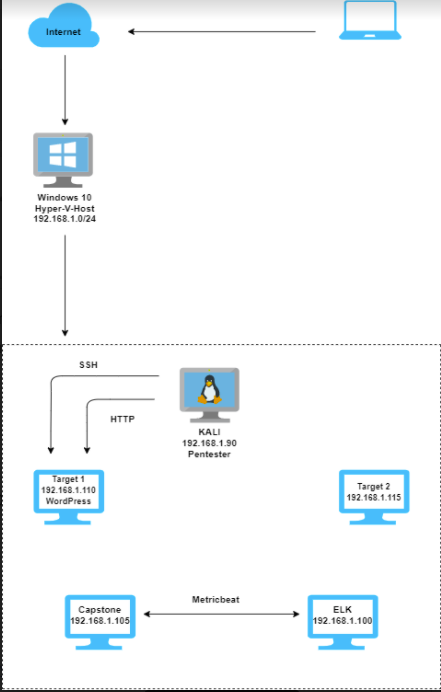
# **Blue Team: Summary of Operations**

## **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:

* KALI
  + **Operating System**: Linux
  + **Purpose**: Pentest Machine
  + **IP Address**: 192.168.1.90
* Target 1
  + **Operating System**: Linux
  + **Purpose**: Wordpress Host
  + **IP Address**: 192.168.1.110
* Target 2
  + **Operating System**: Linux
  + **Purpose**: Not targeted but included in the network
  + **IP Address**: 192.68.1.115
* Capstone
  + **Operating System**: Linux
  + **Purpose**: Vulnerable web server
  + **IP Address**: 192.168.1.105
* ELK
  + **Operating System**: Linux
  + **Purpose**: The ELK stack
  + **IP Address**: 192.168.1.100

### **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:

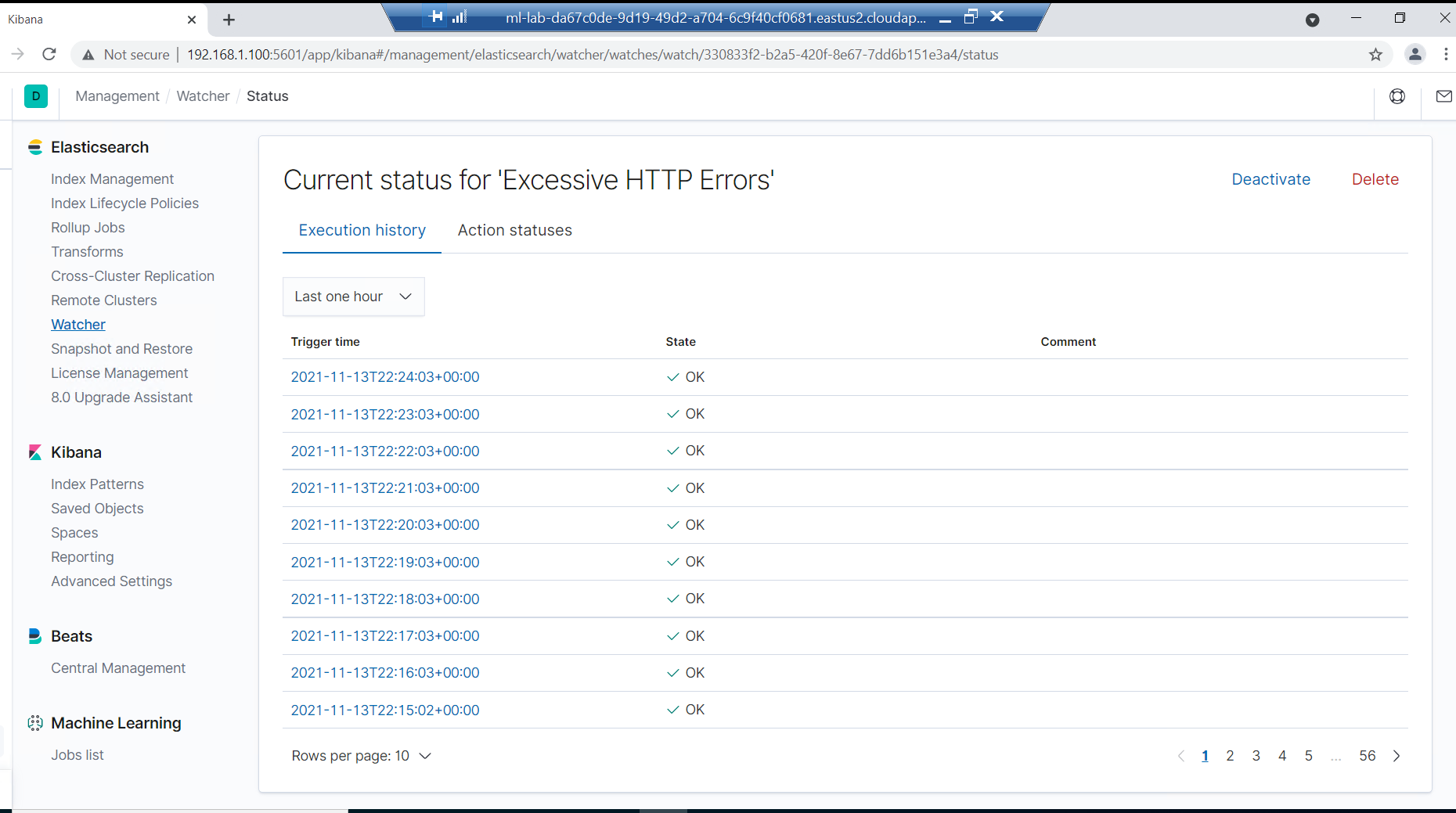
#### 

#### 

#### **Excessive HTTP Errors**

WHEN count() GROUPED OVER top 5 ‘http.response.status\_code’ IS ABOVE 400 FOR THE LAST 5 minutes

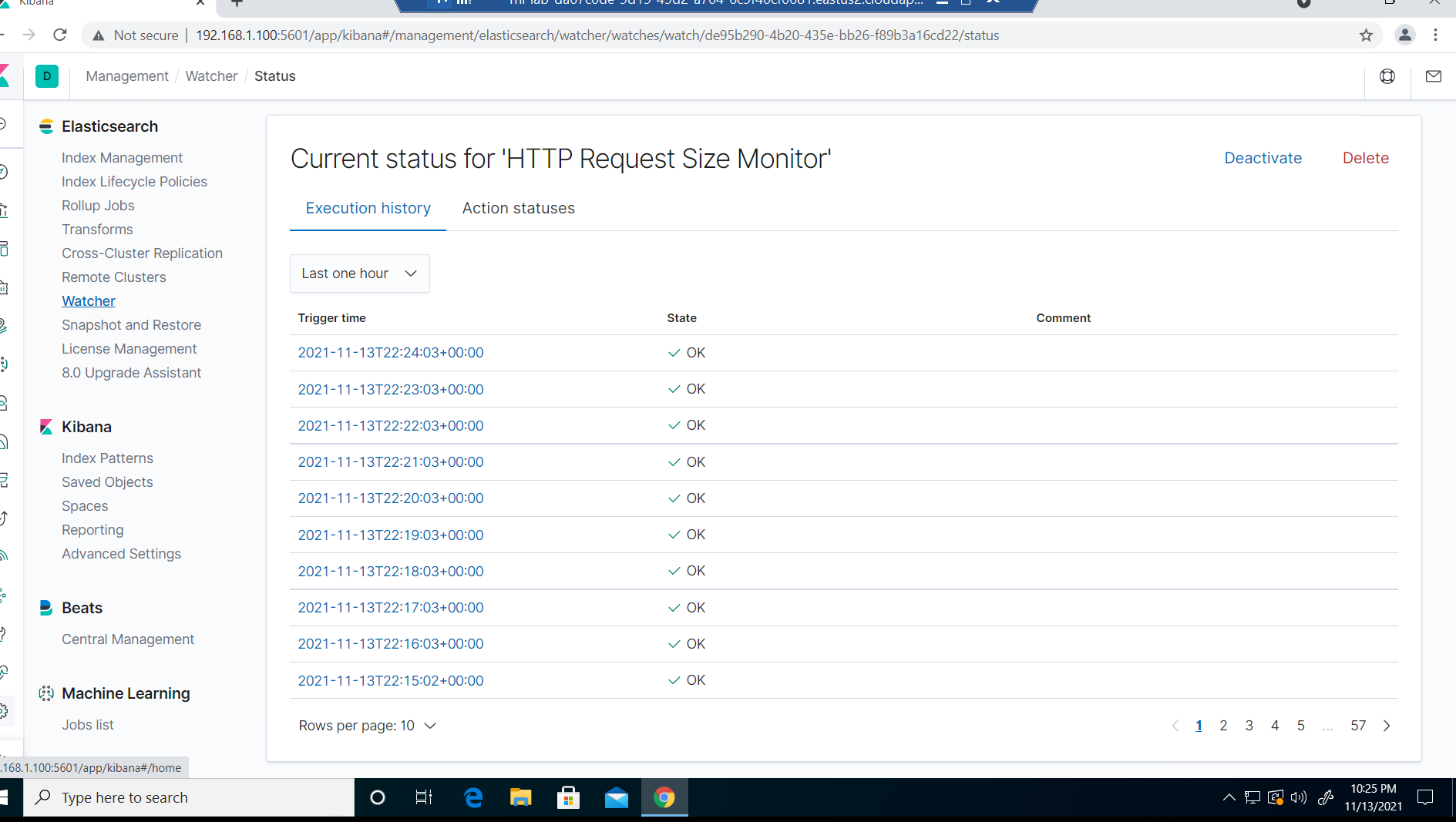
* **Metric**: WHEN count() GROUPED OVER top 5 ‘http.response.status\_code’
* **Threshold**: IS ABOVE 400 FOR THE LAST 5 minutes
* **Vulnerability Mitigated**: Enumeration/Brute Force
* **Reliability**: High. Measuring with an error code of 400 or higher will filter out all normal or successful responses. More than 400 codes are client and server errors of more concern. Especially taking into account those error codes that occur with a high rate.



#### **HTTP Request Size Monitor**

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

* **Metric**: WHEN sum() of http.request.byte OVER all documents
* **Threshold**: IS ABOVE 3500
* **Vulnerability Mitigated**: Code injection in HTTP requests (XSS and CRLF) or DDOS
* **Reliability**: Medium. This alert could create false positives. There can be a lot of non-malicious HTTP requests and legitimate HTTP traffic.



#### **CPU Usage Monitor**

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**: IS ABOVE 0.5
* **Vulnerability Mitigated**: Malicious software
* **Reliability**: HIGH. Even if no malicious program is running, this warning will help you identify where you can improve CPU utilization.

