**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:

Debian Kali 5.4.0

Purpose:

The Penetration Tester

IP Address:

192.168.1.90

ELK

Operating System:

Ubuntu 18.04

Purpose:

The ELK (Elasticsearch and Kibana) Stack

IP Address:

192.168.1.100

Target 1

Operating System:

Debian GNU/Linux 8

Purpose:

The WordPress Host

IP Address:

192.168.1.110

Target 2

Operating System:

Debian GNU/Linux 8

Purpose:

Vulnerable host to attack

IP Address:

192.168.1.115

Capstone

Operating System:

Ubuntu 18.04

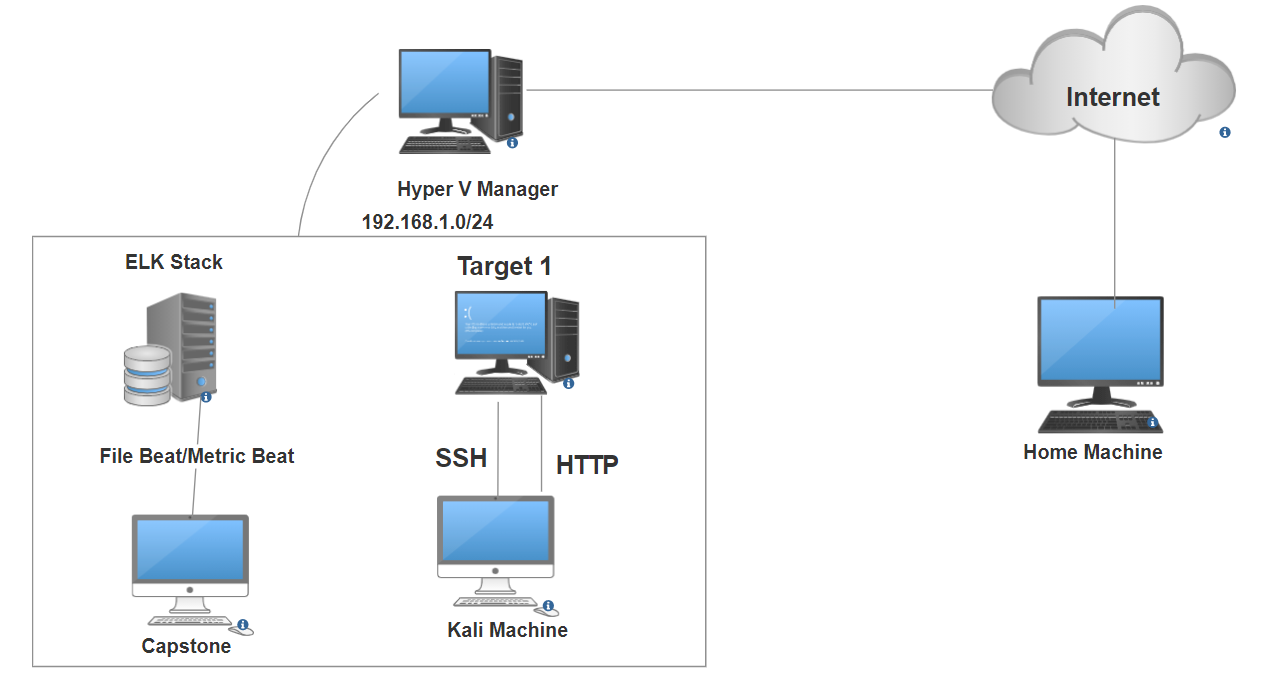
Purpose:

The Vulnerable Web Server

IP Address:

192.168.1.105

**Network Diagram:**



Description of Targets

Target 1 (192.168.1.110) &Target 2 (192.168.1.115) is the 2 VM were vulnerable to attack. But I did only Target 1(192.168.1.110)

All VM as an Apache we server with SSH enable port 80 and 22 are the possible ports of entry .

Monitoring the Targets

Potential points of entry are mentioned below with screen shot.

Target 1

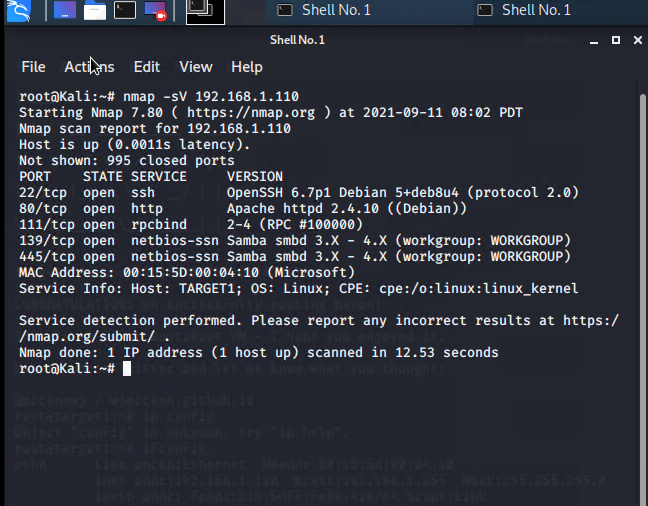
Port 22/TCP Open SSH OpenSSH 6.7p1 Debian 5+deb8u4

Port 80/TCP Open HTTP Apache httpd 2.4.10 (Debian)

Traffic to these services are monitored very carefully .

Excessive HTTP Errors

Excessive HTTP Errors is implemented as follows:

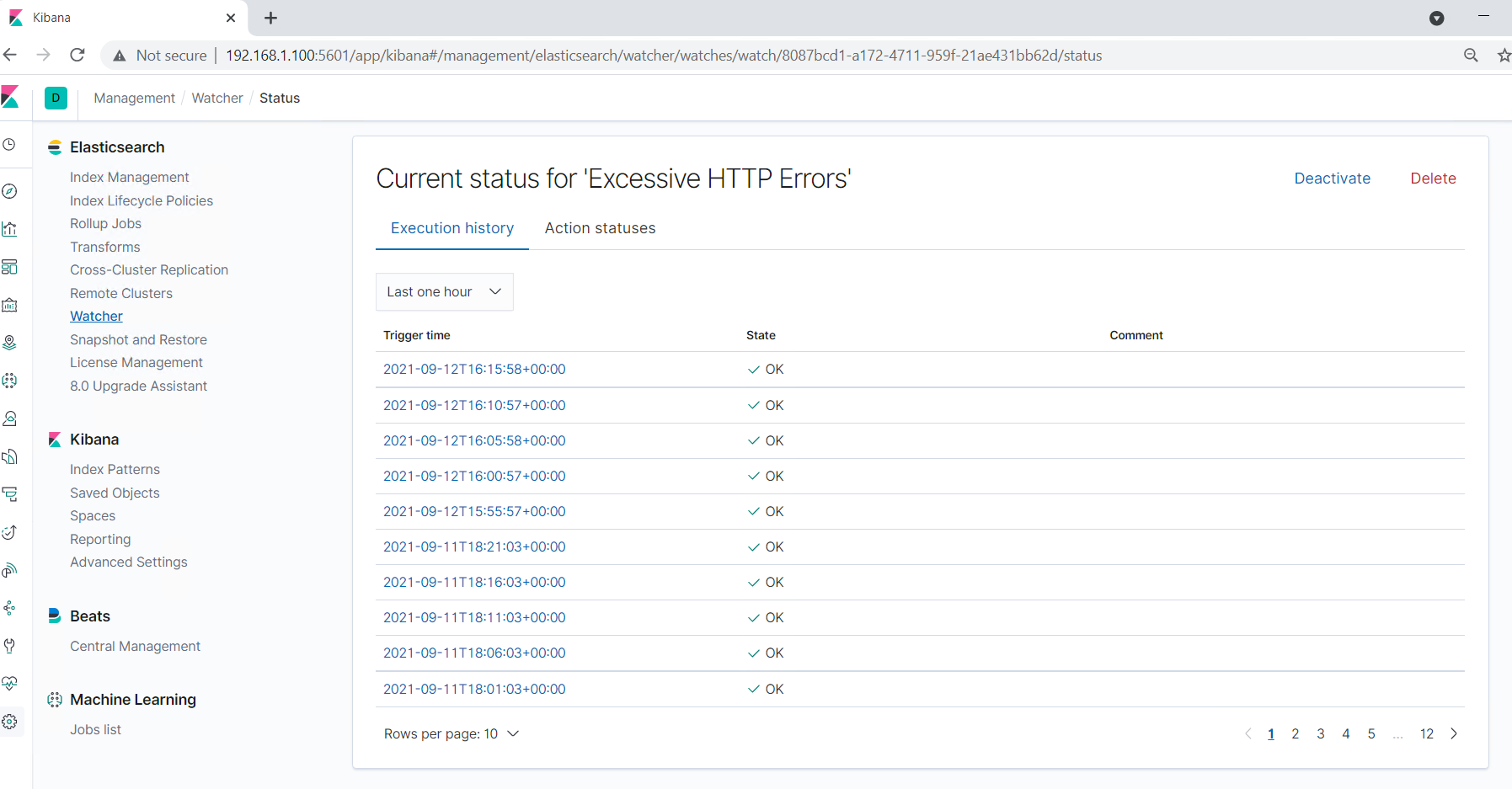


Excessive HTTP Errors

Vulnerability Mitigated:

Brute Force Attack

Alert1:This is high risk alert as we are measuring code more than 400 + will tell is any normal or successful responses.

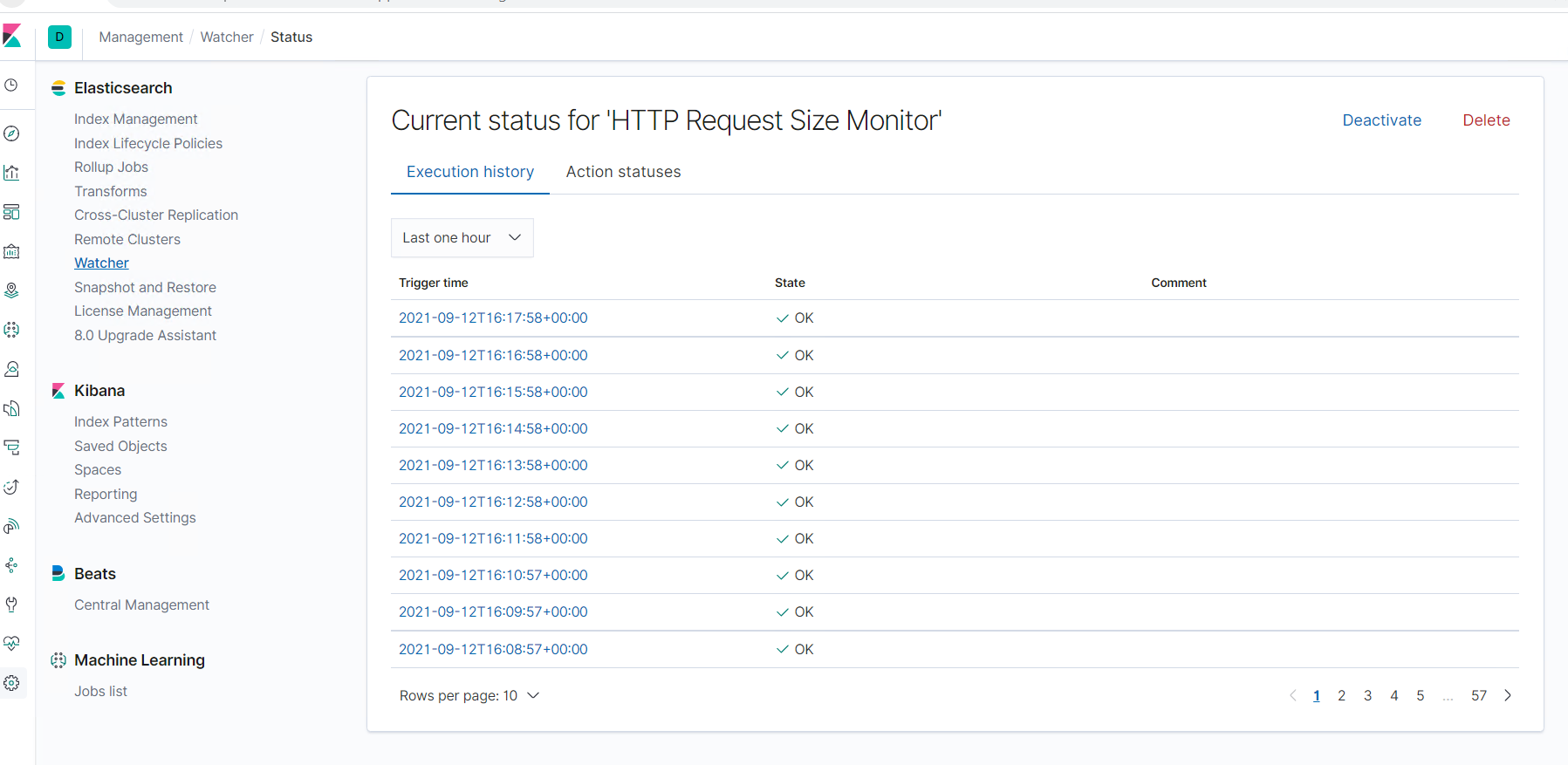


2.HTTP Request Size Monitor

Alert2

Code injection in HTTP requests DDOS

Alert will be medium and possible of large non malicious HTTP traffic.



3.CPU Usage Monitor

Alert: Malicious software

Reliability: CPU usage can be seen on this alert

