# **Blue Team: Summary of Operations**

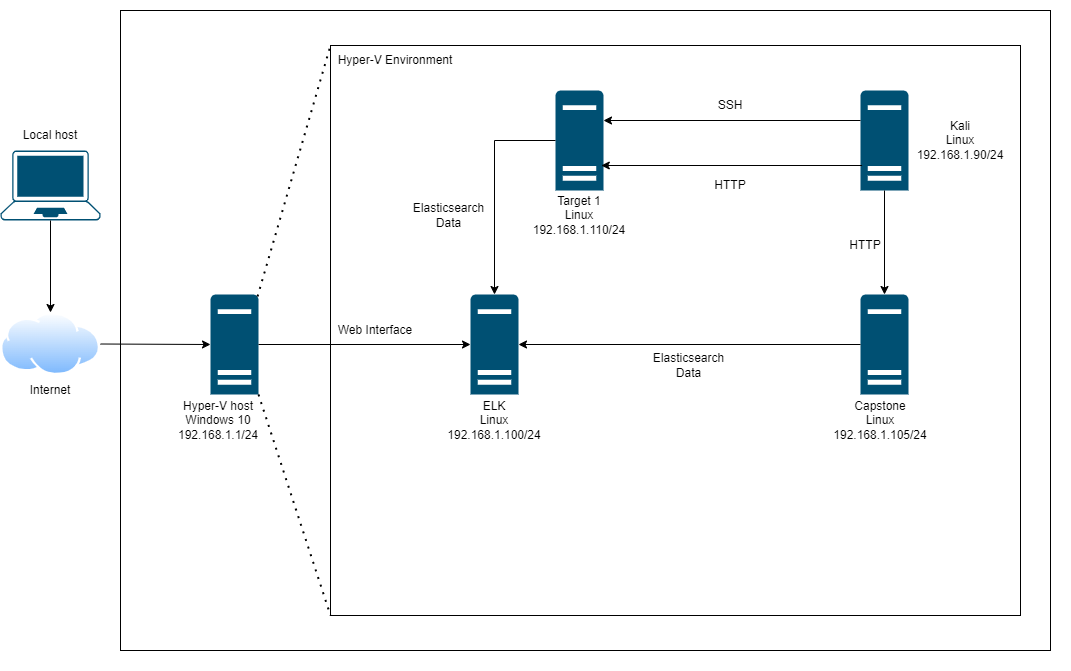
## **Table of Contents**

* 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** | **OS** | **IP Address** | **Purpose** |
| --- | --- | --- | --- |
| Hyper-V | Windows 10 | 192.168.1.1 | Hyper-V host |
| Kali | Linux | 192.168.1.90 | Attacking host |
| ELK | Linux | 192.168.1.100 | Monitoring host |
| Capstone | Linux | 192.168.1.105 | Victim host |
| Target 1 | Linux | 192.168.1.110 | Victim host |



### **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:

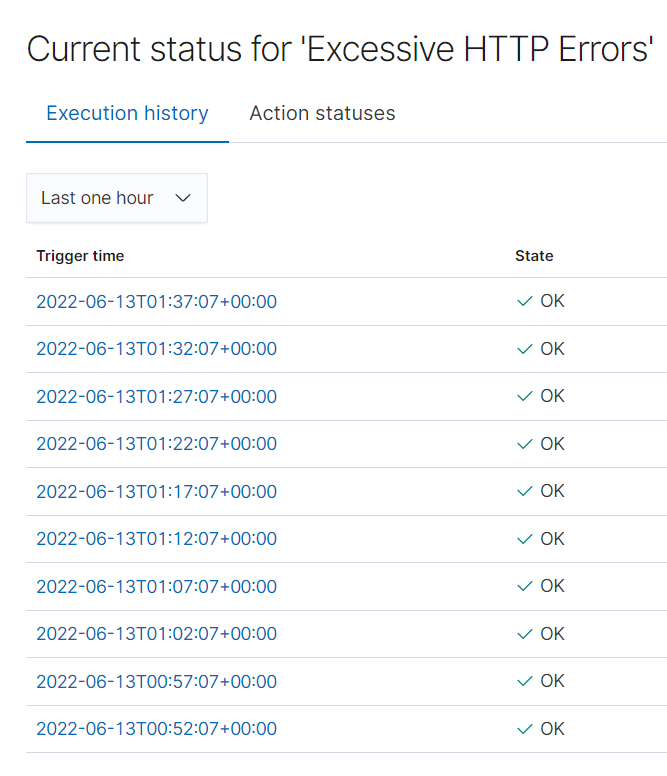
### **Monitoring the Targets**

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

#### **Excessive HTTP Errors**

The Excessive HTTP Errors alert is implemented as follows:

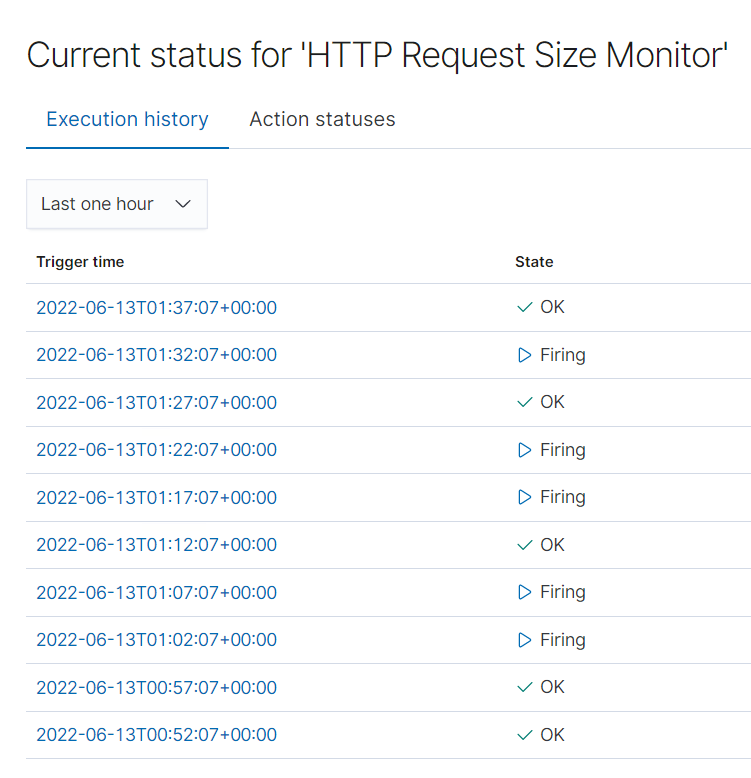
* **Metric**: HTTP Response code
* **Threshold**: Above 400
* **Vulnerability Mitigated**: Brute force/Enumeration
* **Reliability**: high reliablility, when we measure by http response status codes we are able to filter possible errors. Response codes between 400 and 599 are client and server error codes. A response code within this range could indicate an attack.



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

The HTTP Request Size Monitor alert is implemented as follows:

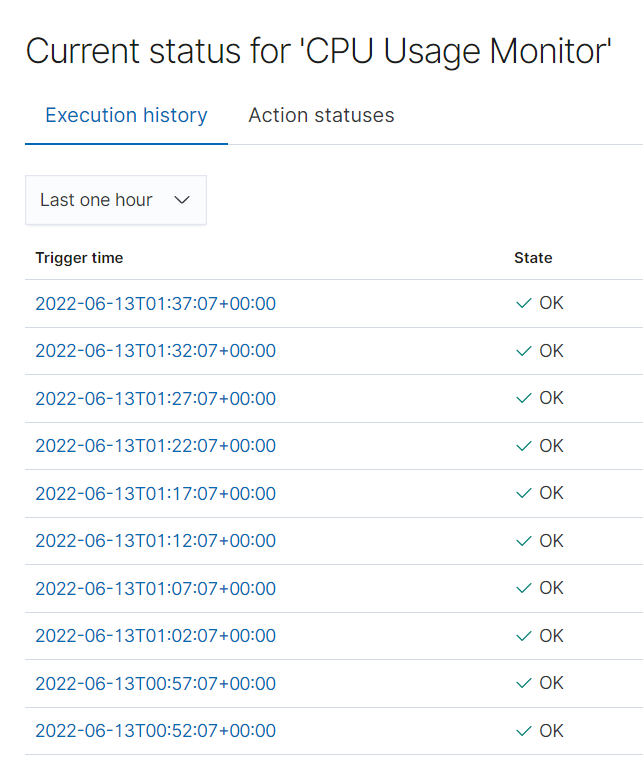
* **Metric**: HTTP Request bytes
* **Threshold**: Above 3500
* **Vulnerability Mitigated**: DDoS and Code injection in HTTP requests (XSS)
* **Reliability**: low reliability, the alert is prone to frequent false positives as there are non-malicious request above 3500 bytes as we can see from the image below. This alert will need more testing in order to locate the correct threshold in order for it to be more reliable.



#### **CPU Usage Monitor**

The CPU Usage Monitor alert is implemented as follows:

* **Metric**: Total amount of System CPU usage by processes
* **Threshold**: above 0.5 (50%)
* **Vulnerability Mitigated**: Malicious software/programs using CPU resources
* **Reliability**: high reliability, measuring by CPU usage allows us to determine if malware of a virus is attempting to compromise the system.



### **Suggestions for Going Further**

The logs and alerts generated during the assessment suggest that this network is susceptible to several active threats, identified by the alerts above. In addition to watching for occurrences of such threats, the network should be hardened against them. The Blue Team suggests that IT implement the fixes below to protect the network:

* Port information exposure (port scanning)
  + **Patch**: enable request blocking on firewall
  + **Why It Works**: A firewall can be configured to use adaptive behaviour to spot and block unusual connection attempts and requests to ports by a suspicous IP that is probing them.
* Insecure Wordpress configuration (user identification)
  + **Patch**: Wordpress information obfuscation
  + **Why It Works**: Remove or disable files containing sensitive information can slow down attackers when attempting to gather information regarding the platform. A few of the files that will need to be re-configured are:
  + Xmlrpc.php
  + ?authors=
  + readme.html
  + wp-cron.php
* Vulnerable SSH authentication (brute force)
  + **Patch**: MFA implementation
  + **Why It Works**: MFA prevents brute force attacks by requiring a second authentication factor in order to successfully use login credentials.
* Server Sensitive Data Exposure (wp-config.php)
  + **Patch**: Restric access to wp-config.php file
  + **Why It Works**: the file has a default location by moving the file to a file outside of the wordpress installation and restricting file permissions we can ensure it is not accessed by unauthorized users.
* Database Sensitive Data Exposure (plain-text data)
  + **Patch**: Implement encryption protocol
  + **Why It Works**: By using encryption protocols, data breaches are less likely to happen. Cybercriminals are therefore unable to access the data even if they get their hands on it.