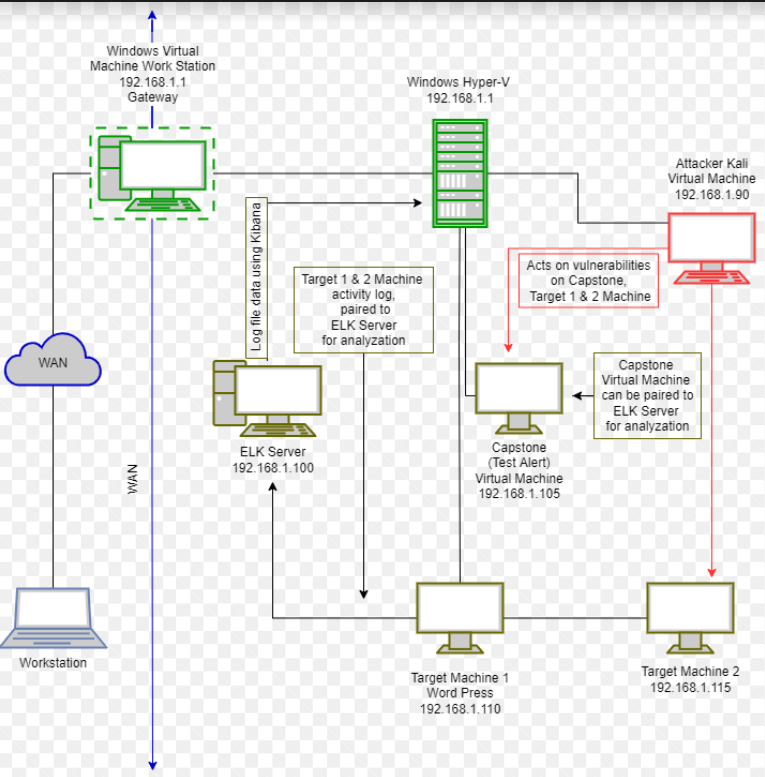
# **Blue Team: Summary of Operations**

## **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:

* Hyper-V Host Manager
  + **Operating System**: Windows 10
  + **Purpose**: contains the vulnerable machines and attacking machines
  + **IP Address**: 192.168.1.1
* Kali
  + **Operating System**: Linux
  + **Purpose**: the attacking machine
  + **IP Address**: 192.168.1.90
* Capstone
  + **Operating System:** Linux
  + **Purpose**: Vulnerable Web Server
  + **IP Address:** 192.168.1.105
* ELK
  + **Operating System**: Linux
  + **Purpose**: used for gathering the information from the victim machine through metricbeat, filebeat, and packetbeat
  + **IP Address**: 192.168.1.100
* Target 1
  + **Operating System**: Linux
  + **Purpose**: contains WordPress; the vulnerable server
  + **IP Address**: 192.168.1.110
* Target 2
  + **Operating System**: Linux
  + **Purpose**: contains WordPress; the vulnerable server
  + **IP Address**: 192.168.1.115

### **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**: packetbeat
* **Threshold**: When count() GROUPED OVER top 5 'http.response.status\_code' IS ABOVE 400 FOR THE LAST 5 minutes
* **Vulnerability Mitigated**:
  + Intrusion detection will prevent brute force attacks
  + Ability to block suspicious IP addresses
  + Manage accounts to have users change their passwords every 30 days
* **Reliability**: high reliability

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

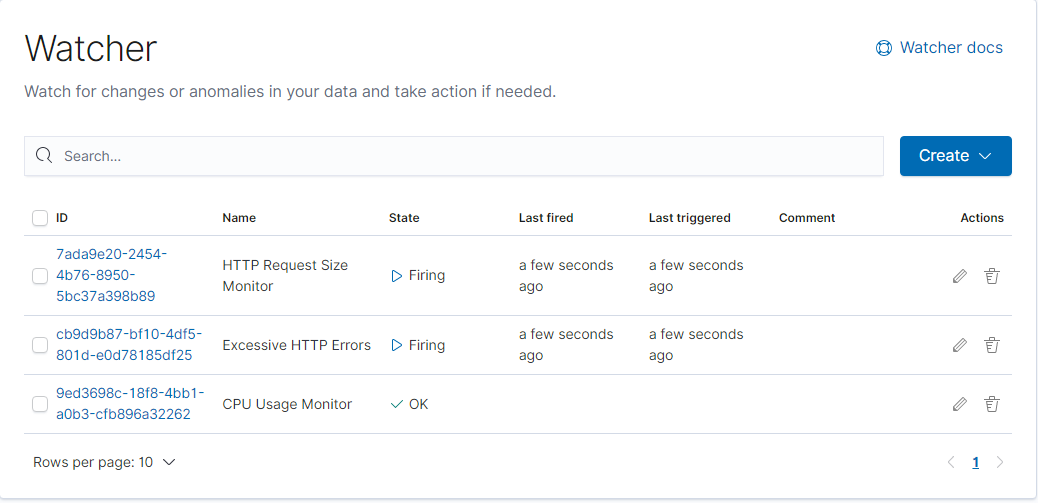
Alert 2 is implemented as follows:

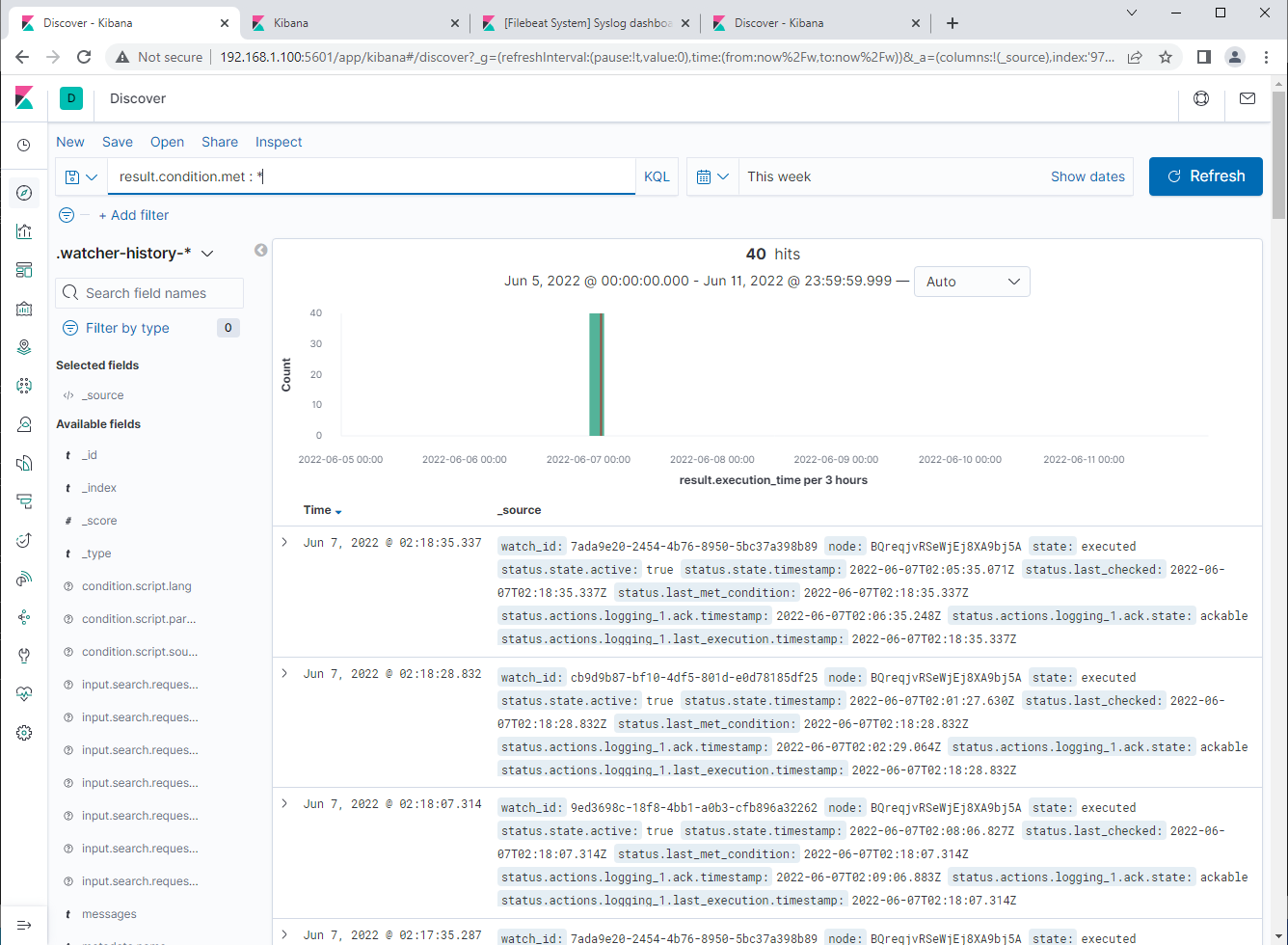
* **Metric**: packetbeat
* **Threshold**: WHEN sum() of http.request.bytes OVER all documents IS ABOVE 3500 FOR THE LAST 1 minute
* **Vulnerability Mitigated**: The ability to monitor and detect DDoS attacks by the http requests and their sizes
* **Reliability**: Medium

#### **CPU Usage Monitor**

Alert 3 is implemented as follows:

* **Metric**: metricbeat
* **Threshold**: WHEN max() OF system.process.cpu.total.pct OVER all documents IS ABOVE 0.5 FOR THE LAST 5 minutes
* **Vulnerability Mitigated**: the ability to detect a possible virus or malware by monitoring the CPU usage percentage, ensuring it does not go above 50%
* **Reliability**: Low





### **Suggestions for Going Further (Optional)**

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:

* **Vulnerability 1**
  + Close and swap port 80 for a more secure port providing the same function as port 443. Flag and observe all 401 Unauthorized Error Codes; soon locking out accounts after multiple bad attempts. Enforce Service Protection API Limits Error Code 429 to any user performing excessive HTTP method requests in a short amount of time blocking them from sending future HTTP requests.
  + <https://docs.microsoft.com/en-us/power-apps/developer/data-platform/webapi/compose-http-requests-handle-errors>
* **Vulnerability 2**
  + Enforce Error Code 413, blocking any request payload too large. Monitor all 404 Error Code to observe Post HTTP requests; later blocking all Post request not related to the site. Deny all Post Request using “HTTP 1.0”, which is prone to malicious acts due to the protocol not requiring a Host header.
  + <https://perishablepress.com/protect-post-requests/>
* **Vulnerability 3**
  + The best option to patch high suspicious CPU Usage would be, to install an antivirus software capable of scanning running programs including background running programs on your system. Exposing the cause, allowing further actions needed to deter the use of unwanted high CPU Usage.
  + <https://windowsreport.com/empty-task-manager-high-cpu/>