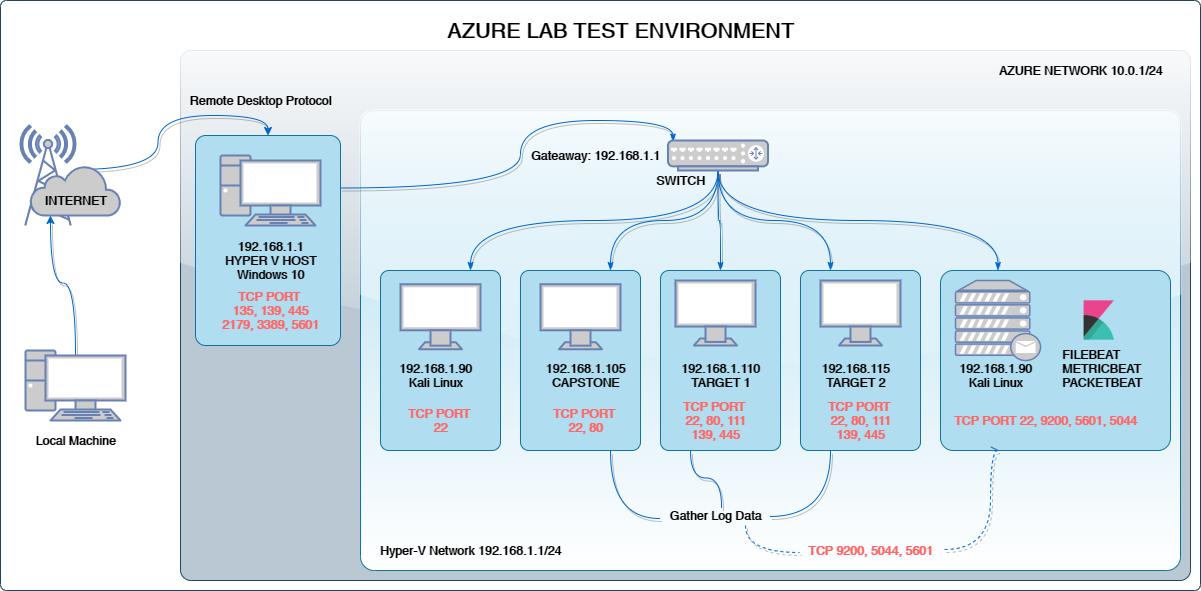
# **Blue Team: Summary of Operations**

## **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**: Penetration Testing
  + **IP Address**: 192.168.1.90
* Elk
  + **Operating System**: Linux
  + **Purpose**: Log all activity from Target1 and Capstone
  + **IP Address**: 192.168.1.100
* Target1
  + **Operating System:** Linux
  + **Purpose:** Exposes vulnerable Wordpress server
  + **IP Address:** 192.168.1.110
* Capstone
  + **Operating System**: Linux
  + **Purpose**: Vulnerable VM
  + **IP Address**: 192.168.1.100
* Hyper V Manager
  + **Operating System**: Windows
  + **Purpose**: Contains the vulnerable machines and the attacking machine
  + **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**: Packetbeat
* **Threshold**: When count() GROUPED OVER top5 ‘http.response.status\_code’ is above 400 for the last 5 minutes
* **Vulnerability Mitigated**: WordPress Hardening
* **Reliability**: Medium.

#### 

#### 

#### 

#### **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**: Code Injection/DDOS Hardening
* **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**: Virus or Malware
* **Reliability**: High