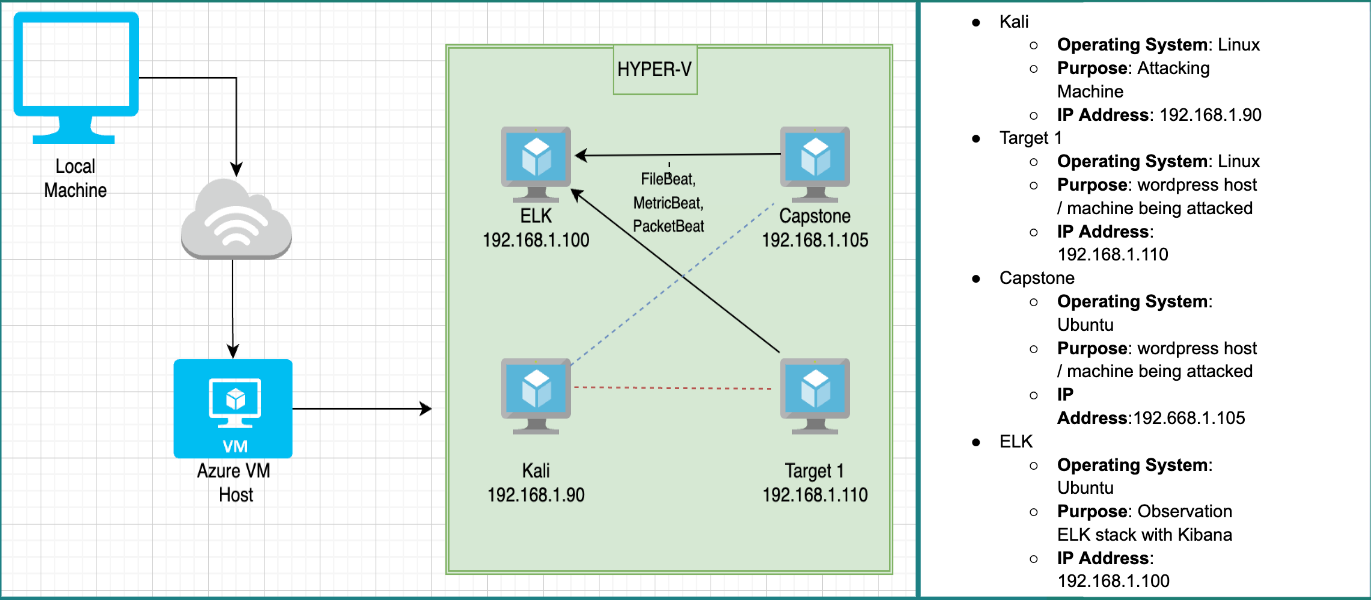
# **Blue Team: Summary of Operations**

## **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 stack
* IP Address: 192.168.1.100

Capstone

* Operating System:Ubuntu 18.04
* Purpose:The Vulnerable Web Server
* IP Address:192.168.1.105

### **Description of Targets**

*TODO: Answer the questions below.*

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:

Alert 1 is implemented as follows:

* Metric: WHEN count() GROUPED OVER top 5 'http.response.status.code
* Threshold: ABOVE 400
* Vulnerability Mitigated: Enumeration/Brute Force
* Reliability: Highly reliable.

#### **Name of Alert 2**

Alert 2 is implemented as follows:

* **Metric**: WHEN sum() of http.request.bytes OVER all documents
* **Threshold**: IS ABOVE 3500
* **Vulnerability Mitigated**: Code injection in HTTP requests (XSS and CRLF) or DDOS
* **Reliability**: Generates false positives. Medium reliability.

#### **Name of Alert 3**

Alert 3 is implemented as follows:

* **Metric**: WHEN max() OF system.process.cpu.total.pct OVER all documents
* **Threshold**: IS ABOVE 0.5
* **Vulnerability Mitigated**: Malicious software
* **Reliability**: Highly Reliable

Each alert above pertains to a specific vulnerability/exploit. Recall that alerts only detect malicious behavior, but do not stop it. For each vulnerability/exploit identified by the alerts above, suggest a patch. E.g., implementing a blocklist is an effective tactic against brute-force attacks. It is not necessary to explain *how* to implement each patch.

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
  + **Patch**: Disable open ports
  + **Why It Works**: no longer allows for visibility of ssh/http ports which are ways to compromise the machines
* Vulnerability 2
  + **Patch**: User credential hardening
  + **Why It Works**: Creating more complex passwords will serve to mitigate brute force attempts made on target 1 instead of using bad credentials like “michael” or “pink84” an example of a more complex password would be: “PinKmich84!”