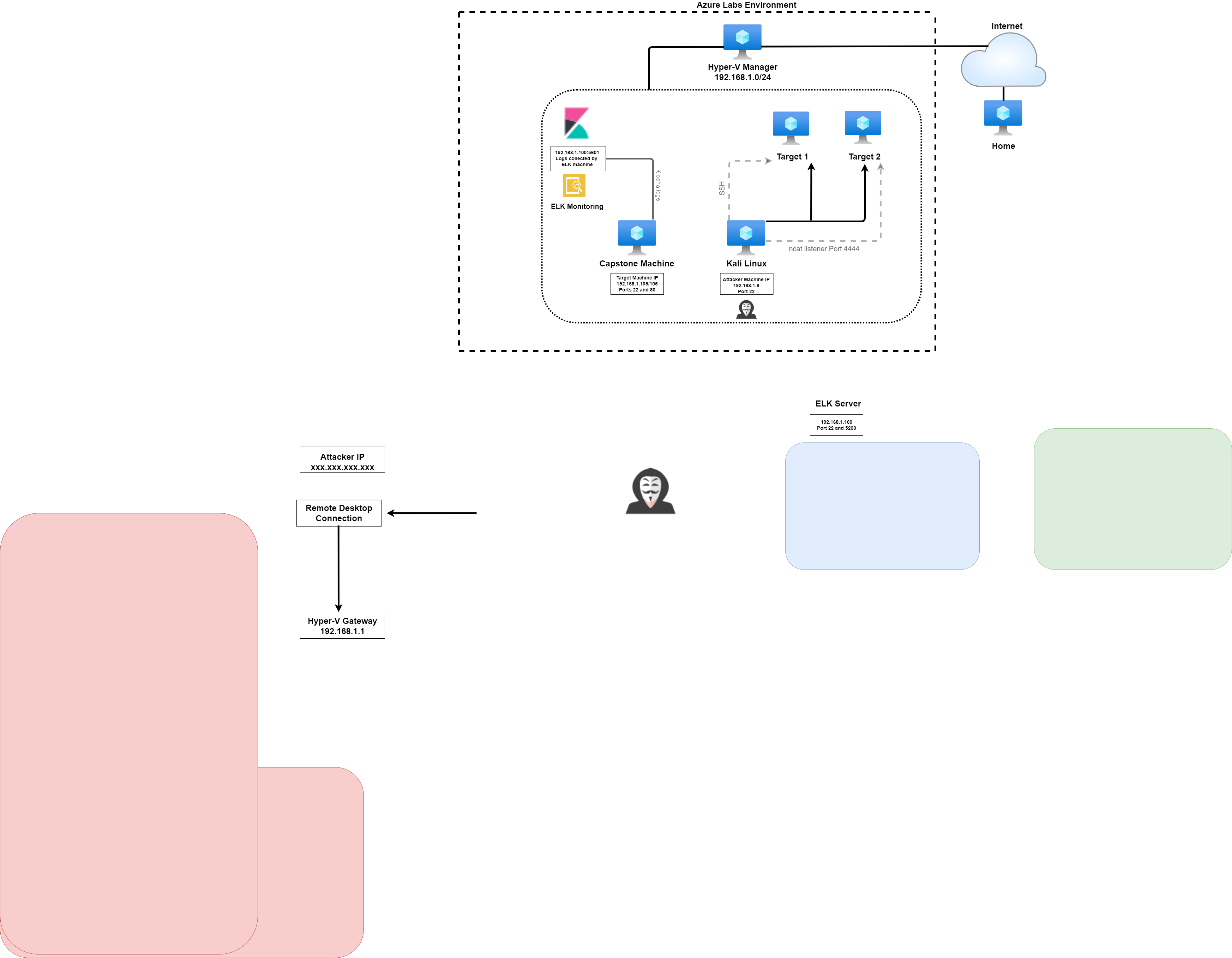
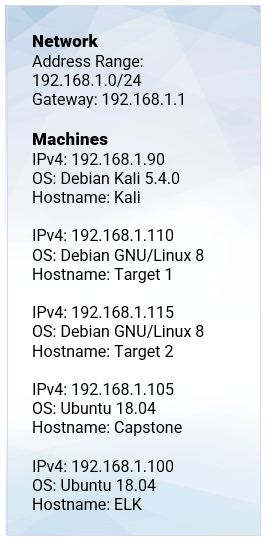
**Blue Team: Summary of Operations**

**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.-
  + **Purpose**: Attack – Pen Testing
  + **IP Address**:192.168.1.8
* Target 1
  + **Operating System**:Debian GNU/Linux 8
  + **Purpose**: WordPress
  + **IP Address**: 192.168.1.110
* Capstone
  + **Operating System**: Ubuntu 18.04
  + **Purpose**: Filebeat/Metricbeat Web Server
  + **IP Address**: 192.168.1.105
* ELK
  + **Operating System**: Ubuntu 18.04
  + **Purpose**: ELK Stack/ capture logs
  + **IP Address**: 192.168.1.100

**Description of Targets**

* The target of this attack was: Target 1
  + **Operating System**:Debian GNU/Linux 8
  + **Purpose**: WordPress
  + **IP Address**: 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:

**Name of Alert 1: Excessive HTTP Errors**

Alert 1 is implemented as follows:

* **Metric**: WHEN count() GROUPED OVER top 5'http.response.status\_code'
* **Threshold**: IS ABOVE 400 FOR THE LAST 5 minutes
* **Vulnerability Mitigated**: Brute Force
* **Reliability**: This should be a high reliability alert, NOT generating any false positives.

**Name of Alert 2: CPU Usage Monitor**

Alert 2 is implemented as follows:

* **Metric**: WHEN max() OF system.process.cpu.total.pct OVER all documents
* **Threshold**: IS ABOVE 0.5 FOR THE LAST 5 minutes
* **Vulnerability Mitigated**: TODO
* **Reliability**: This should also be a high reliability alert, creating minimal false positives.

**Name of Alert 3: HTTP Request Size Monitor**

Alert 3 is implemented as follows:

* **Metric**: WHEN sum() of http.request.bytes OVER all documents Threshold: IS ABOVE 3500 FOR THE LAST 1 minute TODO
* **Threshold**: DDoS or Injection
* **Vulnerability Mitigated**: DDoS or Injection
* **Reliability**: Medium reliability alert with threshold for some false positives.