# Blue Team: Summary of Operations

## Table of Contents

- Network Topology

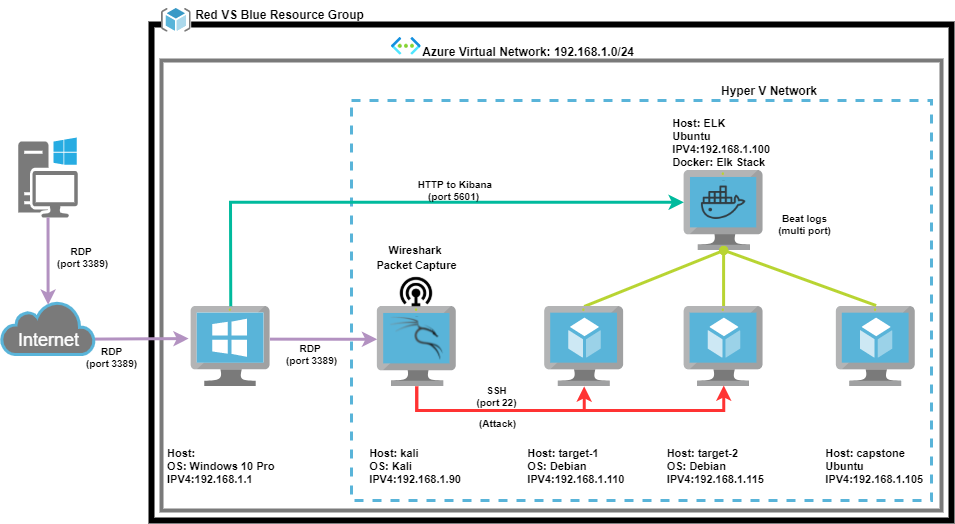
- Description of Targets

- Monitoring the Targets

- Patterns of Traffic & Behavior

- Suggestions for Going Further

### Network Topology



The following machines were identified on the network:

- Name of VM 1

- Target 1

- \*\*Operating System\*\*:

- Apache httpd 2.4.10 (Debian)

- \*\*Purpose\*\*:

- Vulnerable Web Server (WordPress) sends logs to ELK

- \*\*IP Address\*\*:

- 192.168.1.110

- Etc.

### Description of Targets

\_

The target of this attack was: `Target 1 IP 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

Alert 1 is implemented as follows:

- Alert Name: CPU Usage Monitor

- \*\*Metric\*\*: Runs every minute

- \*\*Threshold\*\*: WHEN max() OF system.process.cpu.total.pct OVER all documents IS ABOVE 0.5 FOR THE LAST 5 minutes

- \*\*Vulnerability Mitigated\*\*: Couldn’t really lean on a vulnerability because nothing triggered above 50%

- \*\*Reliability\*\*: low because there could’ve be a lot of reasons why your CPU could be running at 50%

Chart, line chart

Description automatically generated with medium confidence

#### Name of Alert 2

Alert 2 is implemented as follows:

- Alert Name: Excessive HTTP Errors

- \*\*Metric\*\*: Runs a watch every minute

- \*\*Threshold\*\*: WHEN count()GROUPED OVER top 5 ’http.response.status\_code’ IS ABOVE 400 FOR THE LAST 5 minutes

- \*\*Vulnerability Mitigated\*\*: Couldn’t find a vulnerability because this alert didn’t produce any results.

- \*\*Reliability\*\*: Didn’t produce any results so I am putting the reliability as low.

Graphical user interface, text, application, email

Description automatically generated

#### Name of Alert 3

Alert 3 is implemented as follows:

- Alert name: HTTP Request Size Monitor

- \*\*Metric\*\*: runs every minute

- \*\*Threshold\*\*: WHEN sum() OF http.request.bytes OVER all documents IS ABOVE 3500 bytes FOR THE LAST 1 minute

- \*\*Vulnerability Mitigated\*\*: Lots of Web traffic initiated via ip-scanning and remoting via ssh.

- \*\*Reliability\*\*: Medium reliability since it logged a lot of 200 response codes it would be difficult to find a spike without modifying the alert.

Chart

Description automatically generated