

Blue Team: Summary of Operations

Table of Contents

Network Topology

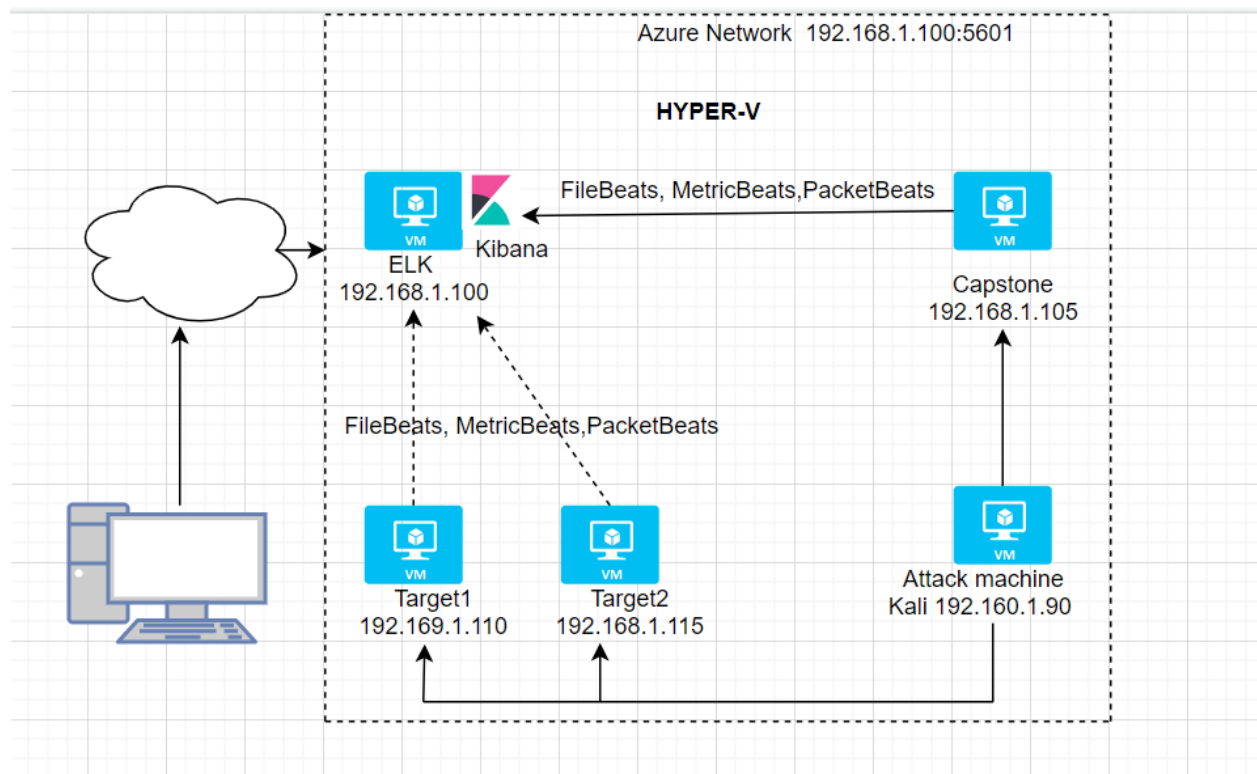
Description of Targets

Monitoring the Targets

Patterns of Traffic & Behavior

Suggestions for Going Further

Network Topology



The following machines were identified on the network:

Capstone

Operating System: Ubuntu 10.04.1 LTS

Purpose: The Vulnerable Web Server

IP Address: 192.168.1.105

Kali

Operating System: Kali GNU/Linux Rolling

Kernel: Linux 5.4.0-kali3-amd64
Purpose: The Penetration Tester
IP Address: 192.168.1.90

ELK

Operating System: Ubuntu 18.04.4 LTS
Purpose: Elasticsearch and Kibana, collecting information by using packetbeats, filebeats, metricbeats.
IP Address: 192.168.1.100

Target1

Operating System: Debian GNU/Linux 8 (jessie)
Purpose: The WordPress Host
IP Address: 192.168.1.110

Target2

Operating System: Debian GNU/Linux 8 (jessie)
Purpose: The WordPress Host
IP Address: 192.168.1.115

Description of Targets

The target of this attack was: Target1 192.168.1.110
Target2 192.168.1.115

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

Excessive HTTP Errors is implemented as follows:

Edit Excessive HTTP Errors

Send an alert when your specified condition is met. Your watch will run every 1 minute.

Name

Excessive HTTP Errors

Indices to query

packetbeat-* x

Time field

event.created v

Run watch every

1

minute v

Use * to broaden your query.

Match the following condition

WHEN count() GROUPED OVER top 5 'http.response.status_code' IS ABOVE 400 FOR THE LAST 5 minutes

No data

Your index and condition did not return any data.

Perform 1 action when condition is met

Add action v

> Logging

Metric: packetbeats, http.response.status_code

Threshold: The TOP 5 get ABOVE 400 for the last 5 minutes

Vulnerability Mitigated: User Enumeration/Brute Force Attack

Reliability:Medium. Threshold is dependent on the quantity of users who engage with the application and it should be adjusted accordingly.

HTTP Request Size Monitor

HTTP Request Size Monitor is implemented as follows:

Edit http request size monitor

Send an alert when your specified condition is met. Your watch will run every 1 minute.

Name

http request size monitor

Indices to query

packetbeat-* x

Time field

@timestamp v

Run watch every

1

minute v

Use * to broaden your query.

Match the following condition

WHEN sum() OF http.request.bytes OVER all documents IS ABOVE 350 FOR THE LAST 1 minute



Perform 1 action when condition is met

Add action v

> Logging

Save alert Cancel

Show request

Metric: packetbeats, WHEN sum() of http.request.bytes OVER all documents

Threshold: ABOVE 350 FOR THE LAST 1 minute

Vulnerability Mitigated: Code injection in HTTP requests

Reliability: Low/medium. Alert can generate lots of false positives/false negatives requests.

CPU Usage Monitor

CPU Usage Monitor is implemented as follows:

Edit cpu usage monitor

Send an alert when your specified condition is met. Your watch will run every 1 minute.

Name: cpu usage monitor

Indices to query: metricbeat-* x Time field: @timestamp Run watch every: 1 minute

Use * to broaden your query.

Match the following condition

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

max()

0.5
0.45
0.4
0.35
0.3
0.25
0.2
0.15
0.1
0.05
0

17:25:00 17:30:00 17:35:00 17:40:00 17:45:00

Perform 1 action when condition is met Add action

> Logging

Save alert Cancel Show request

Metric: Metricbeats, WHEN max() OF system.process.cpu.total.pct OVER all documents

Threshold: ABOVE 0.5 FOR THE LAST 5 minutes

Vulnerability Mitigated: Malicious software, programs running or DDoS Attacks.

Reliability: The alert is reliable, but can be triggered by regular daily usage. Medium.