**Automated ELK Stack Deployment**

The files in this repository were used to configure the network depicted below.

Graphical user interface, diagram

Description automatically generated

These files have been tested and used to generate a live ELK deployment on Azure. They can be used to either recreate the entire deployment pictured above. Alternatively, select portions of the \_\_\_\_\_ file may be used to install only certain pieces of it, such as Filebeat.

See in the [**Ansible folder**](https://github.com/neelabama/Project-1GitHub-Fundamentals/tree/main/Ansible) for the below

• **Hosts**

**• Ansible Configuration**

**• Ansible ELK Installation and VM Configuration**

**• Filebeat Config**

**• Filebeat Playbook**

**• Metricbeat Config**

**• Metricbeat Playbook**

This document contains the following details:

- Description of the Topologu

- Access Policies

- ELK Configuration

- Beats in Use

- Machines Being Monitored

- How to Use the Ansible Build

**Description of the Topology**

The main purpose of this network is to expose a load-balanced and monitored instance of DVWA, the D\*mn Vulnerable Web Application.

Load balancing ensures that the application will be highly \_\_functional and available\_\_\_, in addition to restricting \_\_traffic\_\_\_ to the network.

What aspect of security do load balancers protect?

The Load balancers add resiliency by rerouting live traffic from one server to another if a server falls prey to a DDoS attack or otherwise becomes unavailable.

What is the advent age of a jump box?

A Jump Box Provisioner is also important as it prevents Azure VMs from being exposed via a public IP Address. This allows us to do monitoring and logging on a single box. We can also restrict the IP addresses able to communicate with the Jump Box, as we've done here

Integrating an ELK server allows users to easily monitor the vulnerable VMs for changes to the \_\_network\_\_\_ and system \_\_logs\_\_\_.

What does Filebeat watch for?\_

Filebeat monitors the log files or locations that you specify, collects log events, and forwards them either to Elasticsearch or Logstash for indexing

What does Metricbeat record?\_

Metricbeat takes the metrics and statistics that it collects and ships them to the output that you specify, such as Elasticsearch or Logstash.

The configuration details of each machine may be found below.

|  |  |  |  |
| --- | --- | --- | --- |
| **Name** | **Function** | **IP Address** | **Operating System** |
| Jump Box | Gateway | 10.0.0.4 / 75.248.172.80 | Linux |
| Web-1 | UbuntuServer | 10.0.0.5 / 20.53.238.207 | Linux |
| Web-2 | UbuntuServer | 10.0.0.6 / 20.53.238.207 | Linux |
| DVWA-VM3 | UbuntuServer | 10.0.0.7 / 20.53.238.207 | Linux |
| ELKVM | UbuntuServer | 10.2.0.4 / 20.84.136.248 | Linux |

Access Policies

The machines on the internal network are not exposed to the public Internet.

Only the \_\_\_Jump-Box-Provisioner\_\_ machine can accept connections from the Internet. Access to this machine is only allowed from the following IP addresses:

- Workstation MY Public IP through TCP 5601

Machines within the network can only be accessed by \_\_Workstation and Jump-Box-Provisioner through SSH Jumb-Box\_\_\_.

Which machine did you allow to access your ELK VM?

Jump-Box-Provisioner IP : 10.1.0.4 via SSH port 22

What was its IP address?\_

Workstation MY Public IP via port TCP 5601

A summary of the access policies in place can be found in the table below.

|  |  |  |
| --- | --- | --- |
| **Name** | **Publicly Accessible** | **Allowed IP Addresses** |
| Jump Box | Yes | 75.248.172.80 (Workstation IP on SSH 22) |
| Web-1 | No | 10.0.0.4 on SSH 22 |
| Web-2 | No | 10.0.0.4 on SSH 22 |
| DVWA-VM3 | No | 10.0.0.4 on SSH 22 |
| ELKVM | No | Workstation MY Public IP using TCP 560 |

**Elk Configuration**

Ansible was used to automate configuration of the ELK machine. No configuration was performed manually, which is advantageous because...

What is the main advantage of automating configuration with Ansible?\_

Ansible lets you quickly and easily deploy multitier applications through a YAML playbook.

No need to write custom code to automate your systems.

Ansible will also figure out how to get your systems to the state you want them to be in.

The playbook implements the following tasks:

In 3-5 bullets, explain the steps of the ELK installation play. E.g., install Docker; download image; etc.\_

To specify a different group of machines

- name: Config elk VM with Docker

hosts: elk

become: true

tasks:

To install Docker.io

- name: Install docker.io

apt:

update\_cache: yes

force\_apt\_get: yes

name: docker.io

state: present

To install Python-pip

- name: Install python3-pip

apt:

force\_apt\_get: yes

name: python3-pip

state: present

# Use pip module (It will default to pip3)

- name: Install Docker module

pip:

name: docker

state: present

`docker`, which is the Docker Python pip module.

To Increase Virtual Memory

- name: Use more memory

sysctl:

name: vm.max\_map\_count

value: '262144'

state: present

reload: yes

Download and Launch ELK Docker Container (image sebp/elk)

- name: Download and launch a docker elk container

docker\_container:

name: elk

image: sebp/elk:761

state: started

restart\_policy: always

Published ports 5044, 5601 and 9200 were made available

published\_ports:

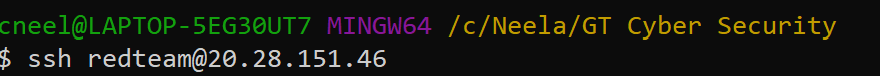
- 5601:5601

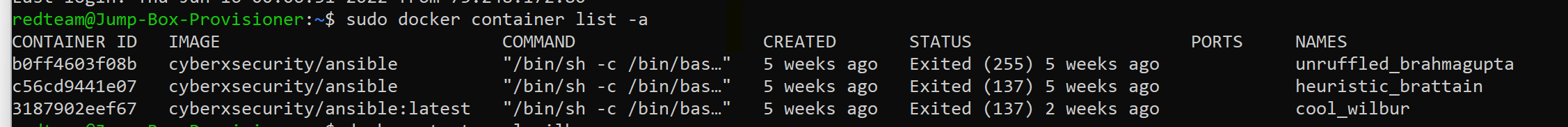
- 9200:9200

- 5044:5044

The following screenshot displays the result of running `docker ps` after successfully configuring the ELK instance.

Connect to jump-Box-Provisioner VM





web-1 and web-2 VM docker info

A picture containing chart

Description automatically generated

Text

Description automatically generated

Target Machines & Beats

This ELK server is configured to monitor the following machines:

List the IP addresses of the machines you are monitoring\_

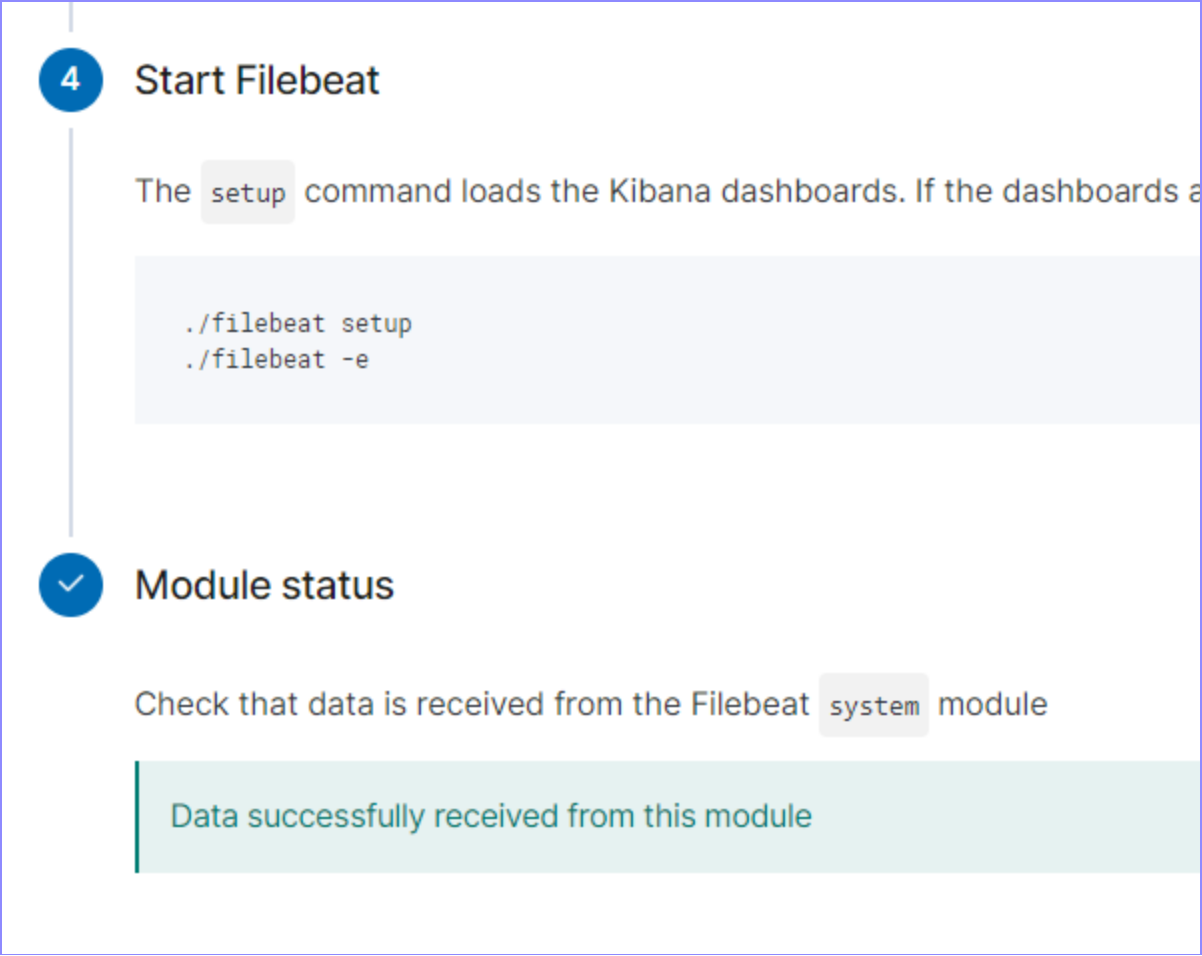
Web-1: 10.0.0.5

Web-2: 10.0.0.6

DVWA-VM3: 10.0.0.7

We have installed the following Beats on these machines:

Filebeat:



Metricbeat:

Graphical user interface, text, application

Description automatically generated

Using the Playbook

In order to use the playbook, you will need to have an Ansible control node already configured. Assuming you have such a control node provisioned:

SSH into the control node and follow the steps below:

- Copy the \_\_yml\_\_\_ file to \_\_ansible folder\_\_\_.

- Update the \_\_config\_\_\_ file to include remote users and ports.

- Run the playbook, and navigate to \_\_\_\_ to check that the installation worked as expected.

\_TODO: Answer the following questions to fill in the blanks:\_

- \_Which file is the playbook?

cd /etc/ansible

ansible-playbook elk.yml

Where do you copy it?\_

- \_Which file do you update to make Ansible run the playbook on a specific machine?

How do I specify which machine to install the ELK server on versus which to install Filebeat on?\_

- \_Which URL do you navigate to in order to check that the ELK server is running?