**# Project-13**

Hands on project for Bootcamp.

**## Automated ELK Stack Deployment**

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

Description automatically generated with medium confidence

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 yml and config file may be used to install only certain pieces of it, such as Filebeat. [Ansible\Docker\pentest.yml](Ansible/Docker/pentest.yml)

[Ansible\ELK\_Stack\ansible.cfg](Ansible/ELK_Stack/ansible.cfg)

[Ansible\ELK\_Stack\elkpentest.yml](Ansible/ELK_Stack/elkpentest.yml)

[Ansible\ELK\_Stack\hosts](Ansible/ELK_Stack/hosts)

[Ansible\Filebeat\filebeat-config.yml](Ansible/Filebeat/filebeat-config.yml)

[Ansible\Filebeat\filebeat-playbook.yml](Ansible/Filebeat/filebeat-playbook.yml)

[Ansible\Metricbeat\meticbeat-playbook.yml](Ansible/Metricbeat/meticbeat-playbook.yml)

[Ansible\Metricbeat\metricbeat-config.yml](Ansible/Metricbeat/metricbeat-config.yml)

This document contains the following details:

- Description of the Topology

- 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 secure and available, in addition to restricting traffic to the /network.

What aspect of security do load balancers protect?

If a server has a Denial-of-service attack committed upon it or becomes unavailable, a load balancer adds resiliency by rerouting traffic from the downed server to another.

What is the advantage of a jump box?

A jump box is important because it prevents Azure VMs with being exposed by their public IP addresses. We can then do the logging and monitoring on a single box. We can also restrict which IP addresses can communicate with the jump box.

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 log files and locations that the user tells it to. After which, it sends them to either Elasticsearch or Logstash for indexing.

What does Metricbeat record?

Metricbeat collects system metrics and application metrics and sends them to the output you choose, either Elasticsearch or Logstash.

The configuration details of each machine may be found below.

|  |  |  |  |
| --- | --- | --- | --- |
| Name | Function | I.P. Address | Operating System |
| Jump-box-provisioner | Gateway | Public-104.208.32.101  Private-10.0.0.4 | Linux |
| Web-1 | Ubuntu Server | Public-23.99.213.81  Private-10.0.0.5 | Linux |
| Web-2 | Ubuntu Server | Public-23.99.213.81  Private-10.0.0.6 | Linux |
| Web-3 | Ubuntu Server | Public-23.99.213.81  Private-10.0.0.7 | Linux |
| ELK Server | Ubuntu Server | Public-52.159.116.52  Private-10.1.0.4 | 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: My public IP address through my workstation IP

Machines within the network can only be accessed by the jump-box-provisioner with the IP of 10.0.0.4.

Which machine did you allow to access your ELK VM?

My jump-box-provisioner through ssh port 22.

What was its IP address?

The public IP address is 104.208.32.101

|  |  |  |
| --- | --- | --- |
| Name | Publicly Accessible | Allowed IP Addresses |
| Jump-box-provisioner | Yes | 104.208.32.101 on ssh 22 |
| Web-1 | No | 10.0.0.5 on ssh 22 |
| Web-2 | No | 10.0.0.6 on ssh 22 |
| Web-3 | No | 10.0.0.7 on ssh 22 |
| Elk Server | No | My public IP using TCP 5601 |

**### Elk Configuration**

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

* Ansible allows for quick and easy deployment of applications through yml playbook files.
* It reduces the amount of bugs and errors that can occur.
* Ansible makes it possible to have your whole infrastructure as a single script.

The playbook implements the following tasks:

- name: Configure Elk VM with Docker

hosts: elk

remote\_user: azureuser

become: true

tasks:

Installs docker.io

- name: Install docker.io

apt:

update\_cache: yes

name: docker.io

state: present

Installs python3 and pip3

- name: Install pip3

apt:

force\_apt\_get: yes

name: python3-pip

state: present

# Use pip module

- name: Install Docker python module

pip:

name: docker

state: present

Inreases memory

- name: Use more memory

sysctl:

name: vm.max\_map\_count

value: "262144"

state: present

reload: yes

This downloads and launches the docker elk container

- name: download and launch a docker elk container

docker\_container:

name: elk

image: sebp/elk:761

state: started

restart\_policy: always

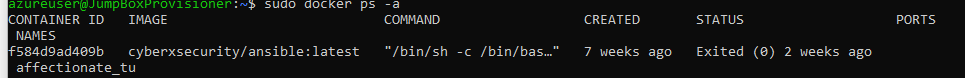
These ports were then made availible

published ports:

* 5601:5601
* 9200:9200
* 5044:5044

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

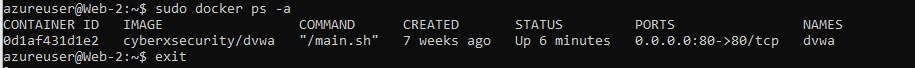
**Jump-Box-Provisioner**

****

**Web-1**



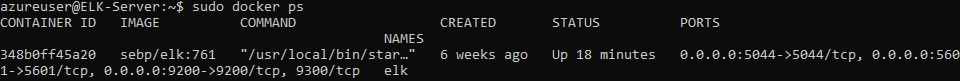
**Web-2**



**Web-3**

****

**Elk-Server**

****

**### Target Machines & Beats**

This ELK server is configured to monitor the following machines:

* Web-1: 10.0.0.5
* Web-2: 10.0.0.6
* Web-3: 10.0.0.7

We have installed the following Beats on these machines:

Filebeat

Graphical user interface, text, application, email

Description automatically generated

Metricbeat

Graphical user interface, text, application, email

Description automatically generated

These Beats allow us to collect the following information from each machine:

Filebeat is used to monitor the log files and locations. In my case it monitors mySQL, webservers, and Microsoft Azure tools.

Metricbeat is used for collecting the metrics and stats of the operating system and putting them in a file you specify.

**### Using the Playbook**

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

* Check the public IP address to see if it has changed.
* If it has changed update the security rules to allow the new public IP address.

SSH into the control node and follow the steps below:

* Copy the yaml file to the ansible folder.
* Update the config file to include remote users and ports.
* Run the playbook and navigate to Kibana to check that the installation worked as expected. (Your\_IP\_Address:5601)

Which file is the playbook? Where do you copy it?

* For ansible use [Ansible\Docker\pentest.yml](file:///C:\Users\adamf\Documents\CybersecurityBootcamp\Project-13\Ansible\Docker\pentest.yml)
* For Filebeat use [Ansible\Filebeat\filebeat-playbook.yml](file:///C:\Users\adamf\Documents\CybersecurityBootcamp\Project-13\Ansible\Filebeat\filebeat-playbook.yml)
* For Metricbeat use [Ansible\Metricbeat\meticbeat-playbook.yml](file:///C:\Users\adamf\Documents\CybersecurityBootcamp\Project-13\Ansible\Metricbeat\meticbeat-playbook.yml)

These files are copied to /etc/ansible

Which file do you update to make Ansible run the playbook on a specific machine?

/etc/ansible/hosts, then you update the IP address of the VM you want to add.

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

I have set up 2 different groups in /etc/ansible/hosts. One group has the 3 IP’s and VMs that have filebeat installed on them. The other group has the ELK server and a the VM the ELK server is installed on.

Which URL do you navigate to in order to check that the ELK server is running?

http://Elk\_VM\_IP:5601/app/kibana

As a \*\*Bonus\*\*, provide the specific commands the user will need to run to download the playbook, update the files, etc.

‘ssh azureuser@jump-box-IP’ – log in to the jump-box-provisioner

‘ssh-keygen’ - create an ssh key to connect to VMs

‘ssh azureuser@Web-1-IP’ – login to Web-1 server

‘ssh azuresuer@Web-2-IP’ – login to Web-2 server

‘ssh azuresuer@Web-3-IP’ – login to Web-3 Server

‘ssh azuresuer@ELK-server-IP’ – login to Elk-server

‘sudo docker container list -a’ – list all docker containers

‘sudo docker ps -a’ – list all active and inactive containers

‘sudo docker start affectionate\_tu’ – start the docker container affectionate\_tu

‘sudo docker attach affectionate\_tu’ – ssh and attach to the docker container affectionate\_tu

‘nano /etc/ansible/hosts’ – to edit the hosts file

‘nano /etc/ansible/ansible.cfg’ - to edit the ansible config file

‘nano /etc/ansible/pentest.yml’ – to edit the ansible playbook

‘ansible-playbook (location) (filename)’ – run the ansible playbook

‘sudo docker run -ti cyberxsecurity/ansible bash’ – run and create the docker container

‘sudo systemctl status docker’ – check the status of the docker app

‘sudo systemctl start docker’ – start the docker service

‘sudo apt install docker.io’ – install the docker container app

‘sudo service docker start’ start the docker app

‘sudo apt-get update’ – run this to update all of the packages

‘curl -L -O (The file on the web path)’ – use this to download a file from the web.

‘dpkg -I (filename)’ – use this option to install the file

‘http://Public\_IP\_VM:5601/app/kibana’ – the URL to navigate to kibana

‘nano filebeat-config.yml’ – create and edit the filebeat config file

‘nano filebeat-playbook.yml’ – create and edit the filebeat playbook

‘nano metricbeat-config.yml’ – create and edit the metricbeat config file

‘nano metricbeat-playbook.yml’ – create and edit the metricbeat playbook.