Automated ELK Stack Deployment

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

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 dependable**, in addition to **restricting inbound traffic** to the network.

- What aspect of security do load balancers protect? **Load balancers protect the availability of information and access to Web1 & Web2 by distributing traffic and not allowing server to be overloaded.** What is the advantage of a jump box?_**The advantage of the jump box is it allows secure access from a single IP address.**

Integrating an ELK server allows users to easily monitor the vulnerable VMs for changes to the data_ and system logs_.

- What does Filebeat watch for?_**Monitors log files from different ip addresses and geo-locations and sends it to the Kibana gui for visualization.**

- What does Metricbeat record?_**System metrics or resources as well as application metrics such as Apache and files types accessed.**

The configuration details of each machine may be found below. Note: Use the Markdown Table Generator to add/remove values from the table.

Name	Function	IP Address	Operating System
Jump Box	Gateway	10.0.0.7	Linux
Web-1	Webserver	10.0.0.8	Linux
Web-2	Webserver	10.0.0.9	Linux
Elk-	Monito	10.1.0.4	Linux

Name	Function	IP Address	Operating System
Server	ring		

Access Policies

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

Only the **Jump-box** machine can accept connections from the Internet. Access to this machine is only allowed from the following IP addresses:

- 98.156.72.161 -my personal ip address.

Machines within the network can only be accessed by the **Jump Box**.

- Which machine did you allow to access your ELK VM? **The Docker container within the Jumpbox.** What was its IP address? **The Docker containers IP address is 40.88.126.80**

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

Name	Publicly Accessible	Allowed IP Addresses
Jump Box	No	10.0.0.7
Elk	No	
DVWA1 & DVWA2	No	

Elk Configuration

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

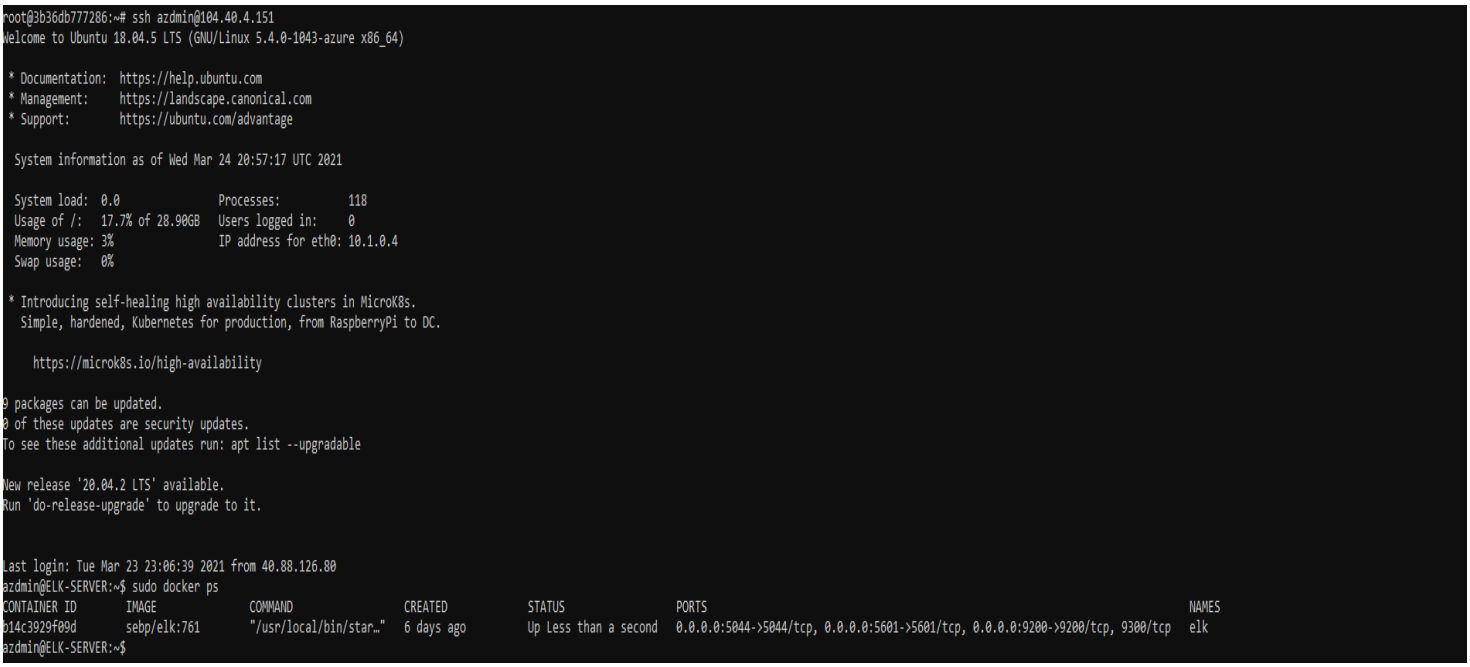
- **Using Ansible to automatically configure the Elk machine is adventageous because it allows you to update all the machines at one time and it allows better security by not needing to access the Elk server directly.**

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.

- **1-Create a new virtual network in a new region, within the resource group.**
- **2-Create a Peer Network Connection** between two virtual networks**
- **3-Create a new virtual network. Deploy a new virtual machine into the new virtual network with it's own Security Group. This virtual machine will host the ELK server.**
- **4-Download and configure the `elk-docker` container onto this new VM.**
- **5-Launch the `elk-docker` container to start the ELK server.**
- **6-Configure the new Security group to connect to ELK via HTTP, and view it through the browser.**

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



Target Machines & Beats

This ELK server is configured to monitor the following machines:

- **10.0.0.8 & 10.0.0.9 or Web-1 & Web-2**

We have installed the following Beats on these machines:

- **Filebeat & Metricbeat**

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

- In 1-2 sentences, explain what kind of data each beat collects, and provide 1 example of what you expect to see. E.g., `Winlogbeat` collects Windows logs, which we use to track user logon events, etc. Filebeat **collects system logs from different locations & ip addresses examples would errors codes and files types.** Metricbeat **collects system and application metrics, examples would be network traffic and system resource usage.**

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 public key file to VM password.
- Update the hosts_ file to include...Webserver IP address & Elk server IP address
- Run the playbook, and navigate to Kibana to check that the installation worked as expected.

Answer the following questions to fill in the blanks:

- _Which file is the playbook? **Docker,Elk, Filebeat, Metricbeat** Where do you copy it? **Copied to the servers.**
- Which file do you update to make Ansible run the playbook on a specific machine? **Ansible.Cfg file by specifying the exact ip addresses.** How do I specify which

machine to install the ELK server on versus which to install Filebeat on? **Alteration of the hostname within the playbook-config file.**

•_Which URL do you navigate to in order to check that the ELK server is running? **Kibana url or in my case "http://104.40.4.151:5601/app/kibana#/home"**