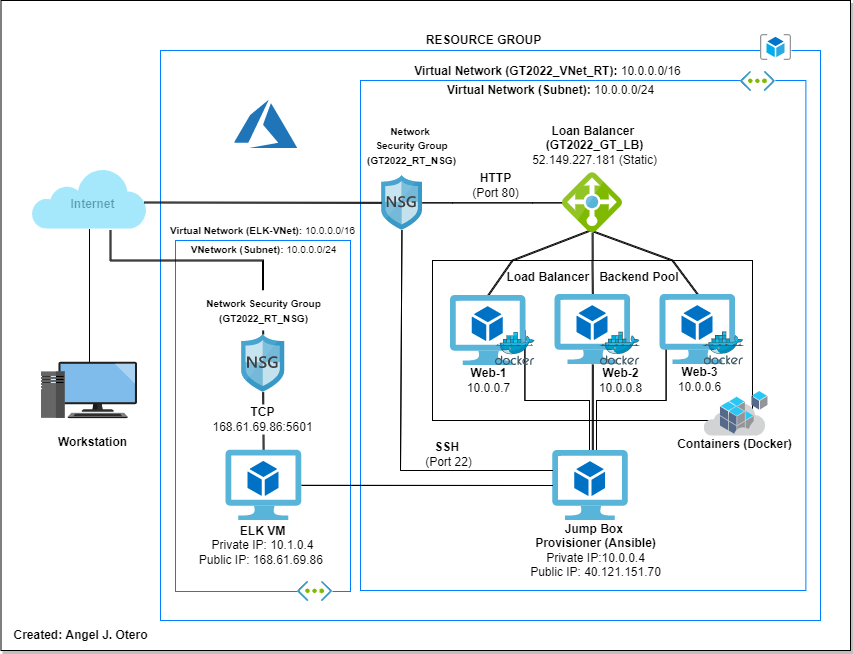
**Homework 13 - Angel J. Otero**

**Automated ELK Stack Deployment**

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

**Note**: The following image link needs to be updated. Replace diagram\_filename.png with the name of your diagram image file.



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 **filebeat-playbook.yml** file may be used to install only certain pieces of it, such as Filebeat.

* **filebeat-playbook.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 availability, in addition to restricting overprocessing to the network.

* *What aspect of security do load balancers protect?* **overprocessing**
* *What is the advantage of a jump box?* **availability**

Integrating an ELK server allows users to easily monitor the vulnerable VMs for changes to the logs and system metric data.

* **System logs**
* **Metric data**

The configuration details of each machine may be found below. *Note: Use the* [*Markdown Table Generator*](http://www.tablesgenerator.com/markdown_tables) *to add/remove values from the table*.

| **Name** | **Function** | **IP Address** | **Operating System** |
| --- | --- | --- | --- |
| Jump Box | Gateway | 10.0.0.4 | Linux |
| Web-1 | Webserver | 10.0.0.7 | Linux |
| Web-2 | Webserver | 10.0.0.8 | Linux |
| Web-3 | Webserver | 10.0.0.6 | Linux |
| VM-ELK | Log Server | 10.1.0.4 | Linux |

**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: 40.121.151.70

* *TODO:* **40.121.151.70**

Machines within the network can only be accessed by Jump Box [10.0.0.4].

* *TODO: Which machine did you allow to access your ELK VM?* **Jump Box**
* *What was its IP address?* **10.0.0.4**

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

| **Name** | **Publicly Accessible** | **Allowed IP Addresses** |
| --- | --- | --- |
| Jump Box | Yes | 40.121.151.70 |
| VM ELM | Yes | 168.61.69.86 |
| Web-1 | No |  |
| Web-2 | No |  |
| Web-3 | No |  |

**Note:** Servers with public IP address are reachable. The firewall (Network Security Group) allows or deny access to server.

**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?*

**Answer:**Automation saves time and minimizes human error. During updates it is faster and requires minimal human technical knowledge.

The playbook implements the following tasks:

* Install docker.io.
* install python3.pip.
* Install docker module.
* Increase the use of virtual memory to 262144.
* Maintain the virtual memory increment after boot.
* Download and configure the ELK docker container.
* Run docker service automatically with every boot.

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

**Note**: The following steps were performed to get the screenshot.

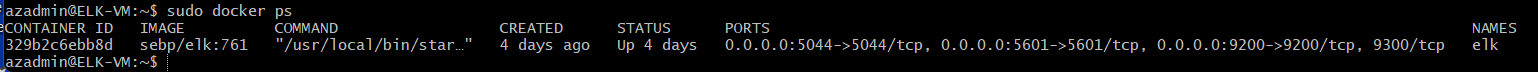
ssh azadmin@40.121.151.70 #Connect to containers.

sudo container start upbeat\_galileo #Connect to the desire container.

sudo container attach

ssh azadmin@10.1.0.4 #Connect to ELK Server.

sudo container ps #The command shows that ELK is running.



**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 [10.0.0.7]**

**Web-2 [10.0.0.8]**

**Web-3 [10.0.0.6]**

We have installed the following Beats on these machines:

* *Specify which Beats you successfully installed*

**Filebeat** and **Metricbeat**

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

**Filebeat** is part of the Elastic Stack, meaning it works seamlessly with Logstash, Elasticsearch, and Kibana. Whether you want to transform or enrich your logs and files with Logstash, fiddle with some analytics in Elasticsearch, or build and share dashboards in Kibana.

**Metricbeat** is part of the Elastic Stack, meaning it works seamlessly with Logstash, Elasticsearch, and Kibana. Whether you want to transform or enrich your metrics with Logstash, fiddle with some analytics in Elasticsearch, or build and share dashboards in Kibana.

**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 **yaml playbook** file to **ansible**.
* Update the **hosts** file to include... in line 30 down add in section [webservers] the following line "**ansible\_python\_interpreter=/usr/bin/python3**" with the IPs of the machines in where the beats will be installed.

(e.g., 10.0.0.7 ansible\_python\_interpreter=/usr/bin/python3)

* Run the playbook, and navigate to **kibana (10.1.0.4)** to check that the installation worked as expected.

*Answer the following questions to fill in the blanks:*

* *Which file is the playbook? Where do you copy it?* **/etc/ansible/roles/filebeat-playbook.yml /etc/ansible/roles/metricbeat-playbook.yml**
* *Which file do you update to make Ansible run the playbook on a specific machine?* ***hosts.yml*** *How do I specify which machine to install the ELK server on versus which to install Filebeat on?* **The ansible hosts files.**
* Which URL do you navigate to in order to check that the ELK server is running?

**http://168.61.69.86:5601/app/kibana**