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.

TODO: Update the path with the name of your diagram

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

* \_TODO: - filebeat.yml

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 available, in addition to restricting Access\_ to the network.

* \_TODO: - Load balancers help protect servers from cyber attacks such as (DDoS) attacks. By distributing traffic amongst servers to lighten the load of malicious traffic. One benefit of using a jump box is that it restricts access and protects your virtual machines from the internet.

Integrating an ELK server allows users to easily monitor the vulnerable VMs for changes to the log files\_ and system \_metrics.

* \_TODO: Logfiles
* \_TODO: Metricts

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*.

Jumpbox | Gateway | 10.0.0.6 | linux |

| Web 1 | VM | 10.0.0.7 | linux | |

| Web 2 | VM | 10.0.0.8 | linux | |

| Elk Base | Elk Stack | 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:

* \_TODO: Home ip

Machines within the network can only be accessed by \_SSH via the jump box

* \_TODO:Jump box 10.0.0.6

### **Elk Configuration**

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

* \_TODO: - Ansible can ensure that provisioning scripts can be identically run between systems and users.

The playbook implements the following tasks:

* *TODO: In 3-5 bullets, explain the steps of the ELK installation play. E.g., install Docker; download image; etc.*
* Installs [Docker.io](http://docker.io/) on the ELK machine
* Installs Python3-pip
* pip installs docker module
* Uses sysctl to increase System Virtual Memory
* Downloads and launches a docker elk container with exposed ports

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

Note: The following image link needs to be updated. Replace docker\_ps\_output.png with the name of your screenshot image file.

TODO: Update the path with the name of your screenshot of docker ps output

### **Target Machines & Beats**

This ELK server is configured to monitor the following machines:

* \_TODO: Web 1 / 10.0.0.7 Web 2 / 10.0.0.8

We have installed the following Beats on these machines:

* \_TODO: Filebeat and Metricbeat

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

* \_TODO: Filebeat collects all the files within the jump box and metricbeat looks at data of the website

### **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 configuration file to *ansible*\_\_\_.
* Update the \_hosts file to include private IP address of the machine you wish install and configure ELK in.
* Run the playbook, and navigate to Kibana (Public\_IP:5601) to check that the installation worked as expected.

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

* *Which file is the playbook? Where do you copy it?* The playbook file would be the YAML file that is provided. And it should be copied into the /etc/ansible directiory in the ansible container.
* \_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? You must update the hosts file in the etc/ansible directory. By adding the private ip address of the specific machine or machines you wish to install ELK or Filebeat on.
* \_Which URL do you navigate to in order to check that the ELK server is running? http://[your.VM.IP]:5601/app/kibana