Automated ELK Stack Deployment

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

![TODO: Update the path with the name of your diagram](Images/diagram_filename.png)

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.

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 available in addition to restricting access to the network.
What aspect of security do load balancers protect?**Load balancers protect servers from a denial of service (DDoS) attack**
What is the advantage of a jump box? **The advantage of a jump box is that after a user successfully logs into the jump box system and is authenticated, they can communicate with other serves without another login requirement**

Integrating an ELK server allows users to easily monitor the vulnerable VMs for changes to the **logs** and system **performance**.
What does Filebeat watch for? **Filebeat is a lightweight shipper for forwarding and centralizing log data.**
-What does Metricbeat record? **Metricbeat records metric data from your target servers**

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-Provisioner	Gateway	10.0.0.4	Linux ubuntu 18.04
Web1	VM	10.0.0.5	Linux ubuntu 18.04
Web2	VM	10.0.0.6	Linux ubuntu 18.04
ELK-vm	ELK-Stack	10.1.0.4	Linux ubuntu 18.04

Access Policies

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

Only the Jumpbox machine can accept connections from the Internet. Access to this machine is only allowed from the following IP addresses:
71.71.68.202 is my personal IPV4 address

Machines within the network can only be accessed by port 22.
Which machine did you allow to access your ELK VM?**This machine can access my ELK VM using IP 71.71.68.202 - my personal machine IPV4 address** 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 Provisioner	Yes	10.0.0.4, 71.71.68.202
Web1	No	10.0.0.5
Web2	No	10.0.0.6
Elk-vm	No	10.1.0.4, 71.71.68.202

Elk Configuration

Ansible was used to automate configuration of the ELK machine. No configuration was performed manually, which is advantageous because**.you don't need to install any other software or firewall ports on the client systems you want to automate. You also don't have to set up a separate management structure**

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._
- **Install Docker**
  Download Image
  Configure Container
  Create playbook and install container with Docker and Filebeat and Metricbeat
  Run playbook to launch the container

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

![TODO: Update the path with the name of your screenshot of docker ps output](Images/docker_ps_output.png)

Target Machines & Beats
This ELK server is configured to monitor the following machines:
List the IP addresses of the machines you are monitoring_

10.0.0.5 Web1
10.0.0.6 Web2

We have installed the following Beats on these machines:
Specify which Beats you successfully installed_

filebeat-7.4.0-amd64.deb
metricbeat-7.4.0-amd64.deb

These Beats allow us to collect the following information from each machine:
- _TODO: 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 monitors and collects log events on specified servers such as my Web-1 and Web-2 VM servers. Filebeat is used to send log files to Kibana.

Metricbeat collects metrics from the operating system as well as services running on the server. It then sends the collected metrics to a specified output, such as Elasticsearch

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 filebeat-playbook.yml file to /etc/filebeat/filebeat.yml.**
  - Update the filebeat-config.yml file to include the ELK server private IP in lines 1106 and 1806.
  - Run the playbook, and navigate to [Elk-Public-IP]:5601/app/kibana 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?_
- _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?

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