Automated ELK Stack Deployment

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

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

- _TODO: Enter the playbook file._

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 protected, in addition to restricting traffic to the network. A Jump Box prevents Azure VMs from public explosure. RDP connects here.

Integrating an ELK server allows users to easily monitor the vulnerable VMs for changes to the logs and system system traffic.
Filebeat watches locations and or log files. It also collects log events which are then sent to Logstash or Elasticsearch.
Metricbeat records metrics from the operating system and services running on the server. These statistics are then forwarded to a user specified output.

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	Server	10.0.0.5	Linux
Web-2	Server	10.0.0.6	Linux
Web-3	Server	10.0.0.7	Linux
Elk	Monitoring	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:
5061 Port (Kibana)

Machines within the network can only be accessed by Jumpbox. Its private IP address is 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	52.189.196.236
Web-1	No	10.0.0.4
Web-2	No	10.0.0.4
Web-3	No	10.0.0.4
Elk	No	10.0.0.4

Elk Configuration

Ansible was used to automate configuration of the ELK machine. No configuration was performed manually, which is advantageous because you don't have to do the work yourself. It's a simple, effective tool that is free to use.

The playbook implements the following tasks:
Install docker.io
Install pip
Install python docker
Virtual memory increase
Download and launch docker

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

(https://github.com/anyagall/Cybersecurity-Bootcamp/blob/0a8d215996d93b508ea2ded4e8c2c184551a00b2/Project%201.PNG)

Target Machines & Beats
This ELK server is configured to monitor the following machines:
Web-1 IP 10.0.0.5
Web-2 IP 10.0.0.6
Web-3 IP 10.0.0.7

We have installed the following Beats on these machines:
Filebeat

These Beats allow us to collect the following information from each machine:
Filebeat collects details on log events.

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 file to playbook file to ansible.
- Configure the host file. Include elk and web servers.
- Run the playbook, and navigate to kibana to check that the installation has worked.

The playbook is a yml file which can be created in the same way as any other file. Navigate to the Kibana webpage **(http://20.36.45.148:5601/app/kibana#/home)** to figure out if the elk is running. It will only connect to the Kibana web[age if the installation/configuration has been successful.

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

sudo ansible-playbook (playbook name)