ELK Stack Project

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: **/etc/ansible/files/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 reliable, in addition to restricting traffic to the network.

- _TODO: What aspect of security do load balancers protect? What is the advantage of a jump box?_ **Load balancers defends and protects the systems against distributed-denial-of-service (DDoS)for an organization. The main advantage of using a Jump-Box the use of a virtual machine, which provides access from a single node to the user that is secured and monitored. In addition, able to manage the other VMs within the overall network.**

Integrating an ELK server allows users to easily monitor the vulnerable VMs for changes to the _machine____ and system _logs____.
- _TODO: What does Filebeat watch for? _ **Monitors and collects data about the file system to a specify location.**
- _TODO: What does Metricbeat record? _ **Collects machine metrics and statistics, such as uptime which outputs the result to a specify location.**

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	10.0.0.8	Linux
Web_2	Webserver	10.0.0.7	Linux
Web_3	Webserver	10.0.0.5	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: Add whitelisted IP addresses_ **40.117.138.27**

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

- _TODO: Which machine did you allow to access your ELK VM? What was its IP address?_ **The Jump Box is allow to access the ELK VM. IP address for the Jump Box 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	40.117.250.32
Web1	No	10.0.0.4
Web2	No	10.0.0.4
Web3	No	10.0.0.4
ELK Server	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...
- _TODO: What is the main advantage of automating configuration with Ansible?_ **Administrators has the ability to enter commands into multiple servers from a single playbook, which enables the administrator to automate configurations and tasks.**

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._

- **Install: docker.io**
- **Install: python3-pip**
- **Install: docker python module**
- **Set the vm.max_map_count to 262144**
- **Download and launch docker elk 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](**diagram/docker_ps_output.png**)

Target Machines & Beats
This ELK server is configured to monitor the following machines:
- _TODO: List the IP addresses of the machines you are monitoring_
    Web-1 10.0.0.7
    Web-2 10.0.0.8
    Web-3 10.0.0.5

We have installed the following Beats on these machines:
- _TODO: Specify which Beats you successfully installed_
  - **Filebeat**
  - **Metricbeat**

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 collects and monitors log files to be view for changes the log files received.**
  - **Metricbeat forwards statistics and metrics data about the operating system, providing an overview of services running, CPU usage, RAM usage, etc. used on the webservers which provides a visual dashboard.**

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 _____.
- Update the _____ file to include...
- Run the playbook and navigate to ____ 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?_
    - **Filebeat configuration File Template to /etc/ansible/files/filebeat-config.yml**

- _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?_
    - **Update /etc/ansible/hosts file to add the webserver VM to include elkserver IP address**
    - **Scroll to line #1106 [“10.1.0.4:9200”] and scroll to line # 1806 [“10.1.0.4:5601”] to add the ELK server**

- _Which URL do you navigate to in order to check that the ELK server is running?
    - **http://[your.VM.IP]:5601/app/kibana (diagram/ELK_Server_Running_Kibana)**