Diagram

Description automatically generatedThese 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.   
*/etc/ansible/my-elkservers.yml*

*name: Installing and Launch Filebeat  
hosts: webservers  
become: yes*

*Tasks:*Use command module *name: Download filebeat .deb file  
command: curl -L -O* [*https://artifacts.elastic.co/downloads/beats/filebeat/filebeat-7.4.0-amd64.deb*](https://artifacts.elastic.co/downloads/beats/filebeat/filebeat-7.4.0-amd64.deb)

Use command module *name: Install filebeat .deb  
command: dpkg -i filebeat-7.4.0-amd64.deb*

Use copy module *name: Drop in filebeat.yml  
Copy:  
src: /etc/ansible/files/filebeat-config.yml  
dest: /etc/filebeat/filebeat.yml*

Use command module *name: Enable and Configure System Module  
command: filebeat modules enable system*

Use command module  
*name: Setup filebeat  
command: filebeat setup*

Use command module *name: Start filebeat service  
command: service filebeat start*

Use systemd module *name: Enable service filebeat on boot  
Systemd:  
name: filebeat  
enabled: yes*

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 *ACCESSIBLE*, 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 protect the system from DDoS attacks by shifting attack traffic. The advantage of a jump box is to give access to the user from a single node that can be secured and monitored.*

Integrating an *ELK* server allows users to easily monitor the vulnerable VMs for changes to the *APPLICATIONS* and system *LOGS*.

TODO: What does Filebeat watch for? *Filebeat monitors the file system for any changes and it documents when they are being made.*

TODO: What does Metricbeat record?   
*Metricbeat takes the metrics and statistics that collects and ships them to the output you specify.*

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\_.

Table

Description automatically generated

Access Policies

The machine 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:

TODO: Add whitelisted IP addresses:   
*My public IP address is: 99.90.35.179*

Machines within the network can only be access by *JUMPBOX*.

TODO: Which machine did you allow to access your ELK VM? What was its IP Address?   
*10.0.0.7*

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

Description automatically generated

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?  
*The advantage was the that you could put commands into multiple servers from a single playbook.*

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: python-pip*

*Install: docker*

*Command: sysctl -w vm.max\_map\_count=262144*

*Launch docker container: elk*

Target Machines & Beats

This ELK server is configured to monitor the following machines:

TODO: List the IP addresses of the machines you are monitoring:   
*DVWA-VM1 10.0.0.5   
DVWA-VM2 10.0.0.6*

We have installed the following Beats on these machines:

TODO: Specify which Beats you successfully installed   
*Filebeat and 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 the changes done. Metric beat collects metrics and statistics.*

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 *ANSIBLE HOSTS FILE* file to */ETC/ANSIBLE*.  
Update the *HOSTS* file to include… *INTERNAL IP ADDRESS OF THE WEB SERVERS, ELK SERVERS, AND THE REMOTE USER INFORMATION*Run the playbook, and navigate to *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? */etc/ansible/file/filebeat-configuration.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? *edit the /etc/ansible/host file to add webserver/elkserver ip addresses*
* \_Which URL do you navigate to in order to check that the ELK server is running? [www.publicip:5601](http://www.publicip:5601) (Kibana) OR 99.90.35.179:5601

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