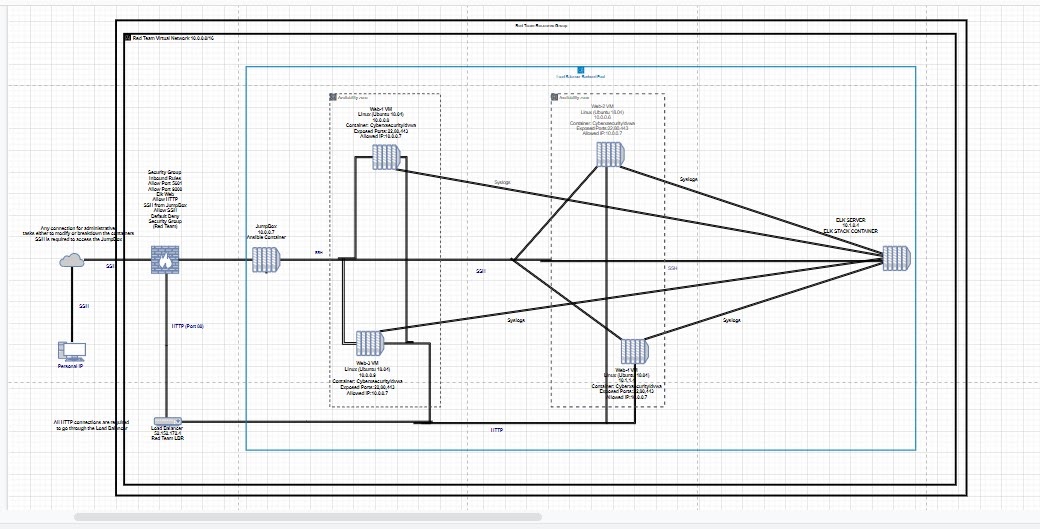
**ELK Stack Deployment.**

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

* The ansible-playbooks [Elk.yml](https://cw.bootcampcontent.com/CW-Coding-Bootcamp/cwr-cle-cyber-pt-04-2020-u-c/blob/master/Elk%20Stack%20Project%20Week/Activities/Stu_Day_1%20080120/Solved/Resources/install-elk.yml), [filebeat-playbook.yml](https://cw.bootcampcontent.com/CW-Coding-Bootcamp/cwr-cle-cyber-pt-04-2020-u-c/blob/master/Elk%20Stack%20Project%20Week/Activities/Stu_Day_1%20080120/Solved/Resources/install-elk.yml), and [metricbeat-playbook.yml](https://cw.bootcampcontent.com/CW-Coding-Bootcamp/cwr-cle-cyber-pt-04-2020-u-c/blob/master/Elk%20Stack%20Project%20Week/Activities/Stu_Day_2%20080420/Solved/config_files/metricbeat-playbook.yml) are needed to create and implement the Elk-Server.

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 Balancing contributes to the Availability aspect of security in regards to the CIA Triad.

What is the advantage of a jump box?

The advantage of a JumpBox is the starting point for launching Administrative Tasks. This ultimately sets the JumpBox as  Secure Admin Workstation. whenever  Administrators are conducting any Administrative Task, it is required to connect to the JumpBox before performing any task/assignment.

Integrating an ELK server allows users to easily monitor the vulnerable VMs for changes to the logs and system traffic.

* What does Filebeat watch for? Filebeat watches for log files/locations and collects log events.
* What does Metricbeat record? Metricbeat records metric and statistical data from the operating system and from services running on the server.

The configuration details of each machine may be found below.

|  |  |  |  |
| --- | --- | --- | --- |
| **Name** | **IP Address** | **Function** | **OS** |
| JumpBox | 10.0.0.7 | Ansible | Linux (ubuntu 18.04) |
| Web-1 | 10.0.0.8 | Docker-DVWA | Linux (ubuntu 18.04) |
| Web-2 | 10.0.0.6 | Docker-DVWA | Linux (ubuntu 18.04) |
| Web-3 | 10.0.0.9 | Docker-DVWA | Linux (ubuntu 18.04) |
| Ubuntu-VM | 10.1.1.4 | Docker-DVWA | Linux (ubuntu 18.04) |
| ELk-Server | 10.1.0.4 | Elk | 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: -Personal IP Address

Machines within the network can only be accessed by SSH.

* The only machine that is able to connect to the Elk-Server (10.1.0.4) is via JumpBox from Private IP (10.0.0.7)

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

|  |  |  |
| --- | --- | --- |
| **Name** | **Publicly Accessible** | **Allowed IP Addresses** |
| Jump Box | No | Personal IP Only |
| Web-1 | No | 10.0.0.7 |
| Web-2 | No | 10.0.0.7 |
| Web-3 | No | 10.0.0.7 |
| Ubuntu-VM | No | 10.0.0.7 |
| ELk-Server | No | 10.0.0.7 & Personal IP |

**Elk Configuration**

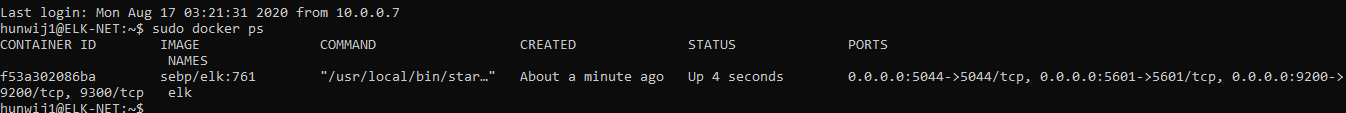
Ansible was used to automate configuration of the ELK machine. No configuration was performed manually, which is advantageous because

* The main advantage of automating configuration through Ansible is the ease of use and an extremely easy learning curve. Through the use of Playbooks you can configure multiple Machines through the use of a single command after initial configuration.

The playbook implements the following tasks:

* Create a New VM (should be named something simple "Elk-Server") Keep note of the Private IP (10.1.0.4) and the Public IP (0.0.0.0) you will need the Private IP to SSH into the VM and the Public IP to connect to the Kibana Portal (HTTP Site) to view all Metrics/Syslogs.
* Download and Configure the "elk-docker" container " in the [Host.conf](https://cw.bootcampcontent.com/CW-Coding-Bootcamp/cwr-cle-cyber-pt-04-2020-u-c/blob/master/Elk%20Stack%20Project%20Week/Activities/Stu_Day_1%20080120/Solved/Resources/hosts).conf you will need to add a new group [elkservers] and the Private IP (10.1.0.4) to the group. Then you need to create a new ansible-playbook ([elk.yml](https://cw.bootcampcontent.com/CW-Coding-Bootcamp/cwr-cle-cyber-pt-04-2020-u-c/blob/master/Elk%20Stack%20Project%20Week/Activities/Stu_Day_1%20080120/Solved/Resources/install-elk.yml)) that will download, install, configures the "Elk-Server" to map the following ports [5601,9200,5044], and starts the container.
* Launch and expose the container "After installing and starting the new container. You can verify that the container is up and running by SSHing into the container from your JumpBox. Once you are in the [Elk-Server] run the command [sudo docker ps]
* Create new Inbound Security Rules to allow Ports: 5601 and 9200 "The Inbound Security Rules should allow access from your Personal Network"
* Open a new browser and type in the [Public IP:5601] to access the Kibana Portal Site

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



**Target Machines & Beats**

This ELK server is configured to monitor the following machines:

* [10.0.0.6, 10.0.0.8,10.0.0.9, 10.0.1.1.4]

   We have installed the following Beats on these machines:

* Filebeat and Metricbeat

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

* Filebeat is a lightweight shipper for forwarding and centralizing log data. Filebeat monitors log files or locations you specify, collects log events, and forwards them either to Elasticsearch or Logstash for indexing.
* Metricbeat collects metrics from the operating system and from services running on the server. Metricbeat then takes the metrics and statistics that it collects and ships them to the output that you specify.

**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.yml](https://cw.bootcampcontent.com/CW-Coding-Bootcamp/cwr-cle-cyber-pt-04-2020-u-c/blob/master/Elk%20Stack%20Project%20Week/Activities/Stu_Day_2%20080420/Unsolved/Resources/filebeat-configuration.yml) and [metricbeat.yml](https://cw.bootcampcontent.com/CW-Coding-Bootcamp/cwr-cle-cyber-pt-04-2020-u-c/blob/master/Elk%20Stack%20Project%20Week/Activities/Stu_Day_2%20080420/Solved/config_files/metricbeat-configuration.yml) file to the /etc/ansible/roles/files/ directory.
* Update the configuration files to include the Private IP of the Elk-Server to the ElasticSearch and Kibana sections of the configuration file.
* Create a new ansible-playbook [filebeat-playbook.yml](https://cw.bootcampcontent.com/CW-Coding-Bootcamp/cwr-cle-cyber-pt-04-2020-u-c/blob/master/Elk%20Stack%20Project%20Week/Activities/Stu_Day_2%20080420/Solved/config_files/filebeat-playbook.yml) in the /etc/ansible/roles/ directory that will install, drop in the [filebeat.yml](https://cw.bootcampcontent.com/CW-Coding-Bootcamp/cwr-cle-cyber-pt-04-2020-u-c/blob/master/Elk%20Stack%20Project%20Week/Activities/Stu_Day_2%20080420/Unsolved/Resources/filebeat-configuration.yml) and [metricbeat.yml](https://cw.bootcampcontent.com/CW-Coding-Bootcamp/cwr-cle-cyber-pt-04-2020-u-c/blob/master/Elk%20Stack%20Project%20Week/Activities/Stu_Day_2%20080420/Solved/config_files/metricbeat-configuration.yml) files from the /etc/ansible/roles/files/ directory, update the configuration files, and start the service for both Filebeat and Metricbeat.
* Run the playbook, and navigate to ELk-Server to check that the installation worked as expected. [docker ps]
* Which file is the playbook? Where do you copy it?

The playbook is called [filebeat-playbook.yml](https://cw.bootcampcontent.com/CW-Coding-Bootcamp/cwr-cle-cyber-pt-04-2020-u-c/blob/master/Elk%20Stack%20Project%20Week/Activities/Stu_Day_2%20080420/Solved/config_files/filebeat-playbook.yml). You copy the file to the "/etc/ansible/hosts/" directory.

* 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?

The file you need to update is the [filebeat.yml](https://cw.bootcampcontent.com/CW-Coding-Bootcamp/cwr-cle-cyber-pt-04-2020-u-c/blob/master/Elk%20Stack%20Project%20Week/Activities/Stu_Day_2%20080420/Unsolved/Resources/filebeat-configuration.yml) file which is a configuration file that will be dropped into the Elk-Server during the run of the ansible-playbook. When you update the host.cfg file in the ansible directory you will need to create a new group called [elkservers] and add the Private IP of the Elk-Server to the group. Then when configuring the [filebeat.yml](https://cw.bootcampcontent.com/CW-Coding-Bootcamp/cwr-cle-cyber-pt-04-2020-u-c/blob/master/Elk%20Stack%20Project%20Week/Activities/Stu_Day_2%20080420/Unsolved/Resources/filebeat-configuration.yml) file you need to designate the Private IP of the Elk-Server in two lines of the .yml file. Lines 1106 and 1806 are needed to be updated with the Private IP.

* Which URL do you navigate to in order to check that the ELK server is running? The URL to use to verify the Elk-Server is running is the Public IP (0.0.0.0:5601)

The commands needed to run the Ansible configuration for the Elk-Server are:

* ssh RedAdmin@JumpBox(PrivateIP)
* sudo docker container list -a (locate your ansible container)
* sudo docker start container (name of the container)
* sudo docker attach container (name of the container)
* cd /etc/ansible/
* ansible-playbook elk.yml (configures Elk-Server and starts the Elk container on the Elk-Server) wait a couple minutes for the implementation of the Elk-Server
* cd /etc/ansible/roles/
* ansible-playbook filebeat-playbook.yml (installs Filebeat and Metricbeat)
* open a new web browser (Elk-Server PublicIP:5601) This will bring up the Kibana Web Portal

You will need to ensure all files are properly placed before running the ansible-playbooks.