## Automated ELK Stack Deployment

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

Diagram

Description automatically generated

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.

**-/etc/ansible/install-elk.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? What is the advantage of a jump box? **Load Balancing contributes to the Availability aspect of security in regards to the CIA Triad.**

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.

\_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 |

|----------|----------|------------|------------------|

| **JumpBox** | **Gateway** | **10.0.0.4** |**Linux(ubuntu 18.4)**|

| **DVWA-VM-1**| **Webserver**| **10.0.0.5** |**Linux(ubuntu 18.4)**|

| **DVWA-VM-2**| **Webserver**| **10.0.0.6** |**Linux(ubuntu 18.4)**|

|**ELK Server**| **ElKserver**| **10.1.0.5** |**Linux(ubuntu 18.4)**|

### 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**.

- Which machine did you allow to access your ELK VM? What was its IP address?\_ **Docker Container within the JumpBox from Private IP (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**  | **Personal IP only** |

| **DVWA-VM-1**| **No** | **10.0.0.4** |

| **DVWA-VM-2**| **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...

- **It minimizes the potential for error and increases potential to save time. Roles were used to increase utility and functionality.**

The playbook implements the following tasks:

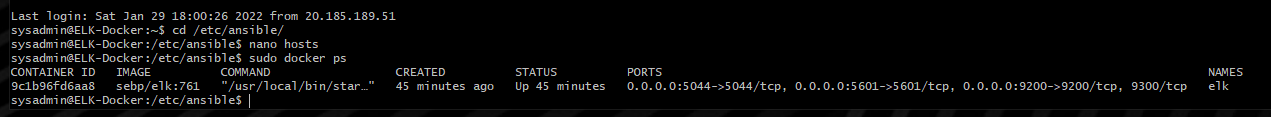
- **Configure Webservers**

- **Install ELK Server**

- **Install File Beat**

- **Install Metric Beat**

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:

- **10.0.0.5**

- **10.0.0.6**

We have installed the following Beats on these machines:

- **Filebeat**

- **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-playbook.yml** and **metricbeat-playbook.yml** file to **/etc/ansible/roles directory.**

- Update the **configuration** file to include **the Private IP of the Elk-Server to the ElasticSearch and Kibana sections of the configuration file located in the "/etc/ansible/files/" directory.**

- Run the playbook and navigate to **HTTP://<ELKServer\_Public\_IP>:5601** to check that the installation worked as expected.

Answer the following questions to fill in the blanks:

- Which file is the playbook? Where do you copy it? **The playbook is called** [**filebeat-playbook.yml**](https://uci.bootcampcontent.com/EmperorForgotten/elk-stack-project/blob/master/Ansible-Playbooks/filebeat-playbook.yml) and **metricbeat-playbook.yml. You copy the file to the "/etc/ansible/roles/" 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 host.confg** **file which is a configuration file. When you update that file in the ansible directory you will need to create a new group called [webservers] and add the private IP of the machines you want to install the filebeat and metricbeat to the group. After that you will create a new group called [elk] and add the private IP of the elk server.**

- Which URL do you navigate to in order to check that the ELK server is running? **http://20.114.232.193:5601/**