## Automated ELK Stack Deployment

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

<https://github.com/charlieumali/Cybersecurity/blob/main/Diagrams/Network%20Diagram.pdf>

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

<https://github.com/charlieumali/Cybersecurity/blob/main/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 direct access to the network.

- The security aspect are two. The first thing is that external users do not have direct access to the servers from the outside and it can authenticate users.

Integrating an ELK server allows users to easily monitor the vulnerable VMs for changes to the file systems on the VMs on the network and system metrics.

Filebeat is a lightweight shipper for forwarding and centralizing log data. Installed as an agent on your servers, Filebeat monitors the log files or locations that you specify, collects log events, and forwards them either to Elasticsearch or Logstash for indexing.

Metricbeat monitors system-level CPU usage, memory, file system, disk IO, and network IO statistics, as well as top-like statistics for every process running on your systems

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 | 10.0.0.1 | Linux

| Web-1 | Web Server | 10.0.0.5 | Linux

| Web-2 | Web Server | 10.0.0.6 | Linux

| Web-3 | Web Server | 10.0.0.9 | Linux

### Access Policies

The machines on the internal network are not exposed to the public Internet.

Only the JumpBoxProvisioner machine can accept connections from the Internet. Access to this machine is only allowed from the following IP addresses:

- 98.167.173.76

Machines within the network can only be accessed by the JumpBoxProvisioner (10.0.0.1).

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

| Name | Publicly Accessible | Allowed IP Addresses |

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

JumpBoxProvisioner Yes 98.167.173.76

Web-1 No 10.0.0.1

Web-2 No 10.0.0.1

Web-3 No 10.0.0.1

### Elk Configuration

Ansible was used to automate configuration of the ELK machine. No configuration was performed manually, which is advantageous because this can be done with multiple machines as the configuration will be the same. Also, the new servers can be added quickly with the same configuration.

- Install docker.io

- Install apt module

- Install python3-pip

- Install Docker Module

- Increase virtual memory

- Maximize memory usage

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

10.0.0.9

We have installed the following Beats on these machines:

Filebeat

Metricbeat

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

Filebeat will sit on the servers and send system logs to Elastisearch or Logstash. Metricbeat will gather information hardware utilization

### 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 configuration file to /etc/ansible/files .

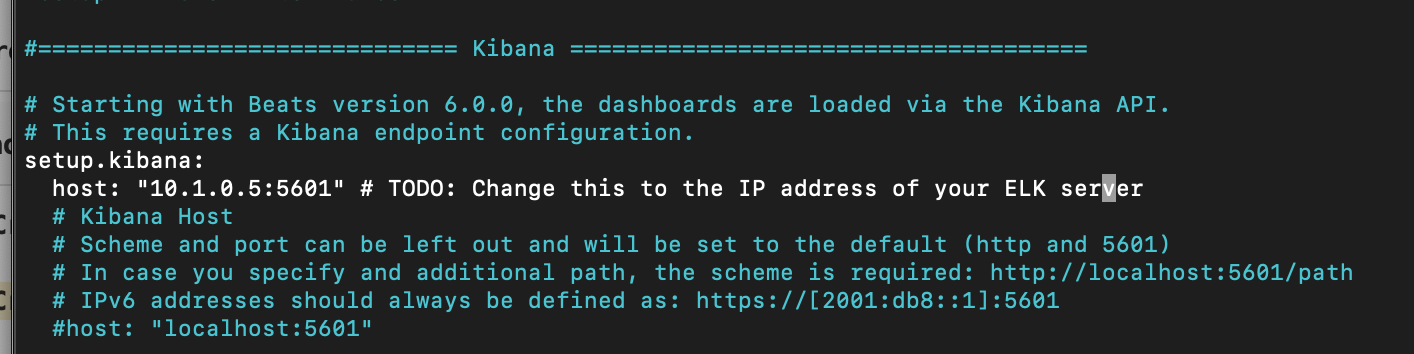
- Update the ansible hosts file to include the dvwa servers (web-1, web-2,web-3)

- Run the playbook, and navigate to <http://13.68.141.29:5601/app/kibana> to check that the installation worked as expected.

Filebeat-config.yml /etc/ansible/files

- Ansible.cfg

- Edit the filebeat-config.yml file



Navigate to <http://13.68.141.29:5601/app/kibana> in order to check that the ELK server is running?

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