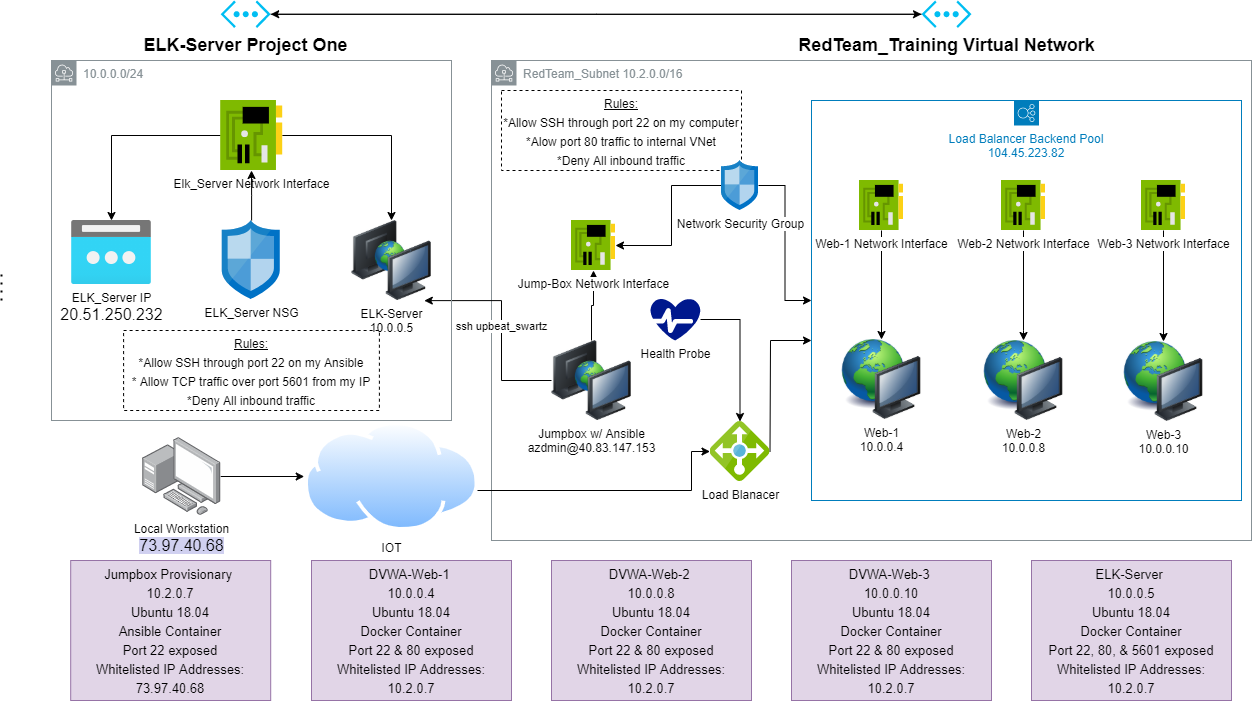
## Automated ELK Stack Deployment

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



/c/Users/mrdrs/Portfolio/Diagrams/Project\_1.png

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.

- 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 availible, in addition to restricting access to the network.

Load balancers protects the system from Distributed Denial of Service (DDoS) attacks by evenly distributing network traffic between the web servers. 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 services and system logs.

Filebeat monitors and logs all information in the file system for changes which has been changed.

Metricbeat takes the metrics and statistics that it collects from the operating system and services that are running on the server 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\_.

| Name | Function | IP Address | Operating System |

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

| JumpBox | Gateway | 10.2.0.7 | Ubuntu 18.04 |

| Web-1 | Webserver | 10.0.0.4 | Ubuntu 18.04 |

| Web-2 | Webserver | 10.0.0.8 | Ubuntu 18.04 |

| Web-3 | Webserver | 10.0.0.10 | Ubuntu 18.04 |

| Elk-Server | Elastic Server | 10.0.0.5 | 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:

- 73.97.40.68

Machines within the network can only be accessed by the Jumpbox.

- From the Jumpbox launch and start the upbeat\_swartz Ansible container from 73.97.40.68.

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

| Name | Publicly Accessible | Whitelisted IP Address |

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

| JumpBox | Yes/No | 73.97.40.68 |

| Web-1 | Webserver | 10.2.0.7 |

| Web-2 | Webserver | 10.2.0.7 |

| Web-3 | Webserver | 10.2.0.7 |

| Elk-Server | Elastic Server | 10.2.0.7 |

### Elk Configuration

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

- The primary benefit of Ansible is it allows IT administrators to automate their daily tasks. Automating daily tasks gives the benefit of removing human error from continued repetition of a mundane task along with allowing the administrators to focus their time on more important tasks.

The playbook implements the following tasks:

- Installs the docker.io (Docker)

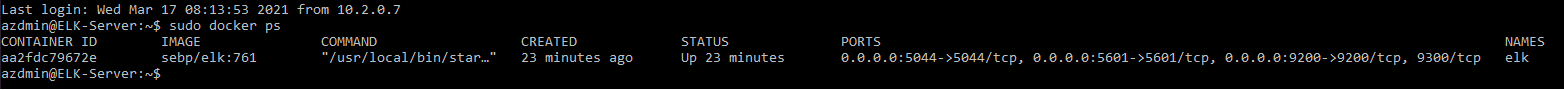
- Installs python-pip (pip3)

- Installs the docker module using pip3

- Increases the virtual memory usage

- Downloads an ELK image for docker and launches it

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



/c/Users/mrdrs/Portfolio/Diagrams/sebp-elk.png

### Target Machines & Beats

This ELK server is configured to monitor the following machines:

- Web-1 10.0.0.4

- Web-2 10.0.0.8

- Web-3 10.0.0.10

We have installed the following Beats on these machines:

- Filebeat

- Metricbeat

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

- Filebeats collects logs generated on the ELK server container. Such examples of logs that are collected are the systemmd of out DVWA virtual machines.

- Metricbeat collects metrics from the system such as CPU usage and RAM usage.

### 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 file to /etc/filebeat directory.

- Update the filebeat.yml file to include where to install the ELK server.

- Run the playbook, and navigate to Docker to check that the installation worked as expected.

- 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 the webserver/elkserver IP addresses.

- \_Which URL do you navigate to in order to check that the ELK server is running? 20.51.250.232:5601

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