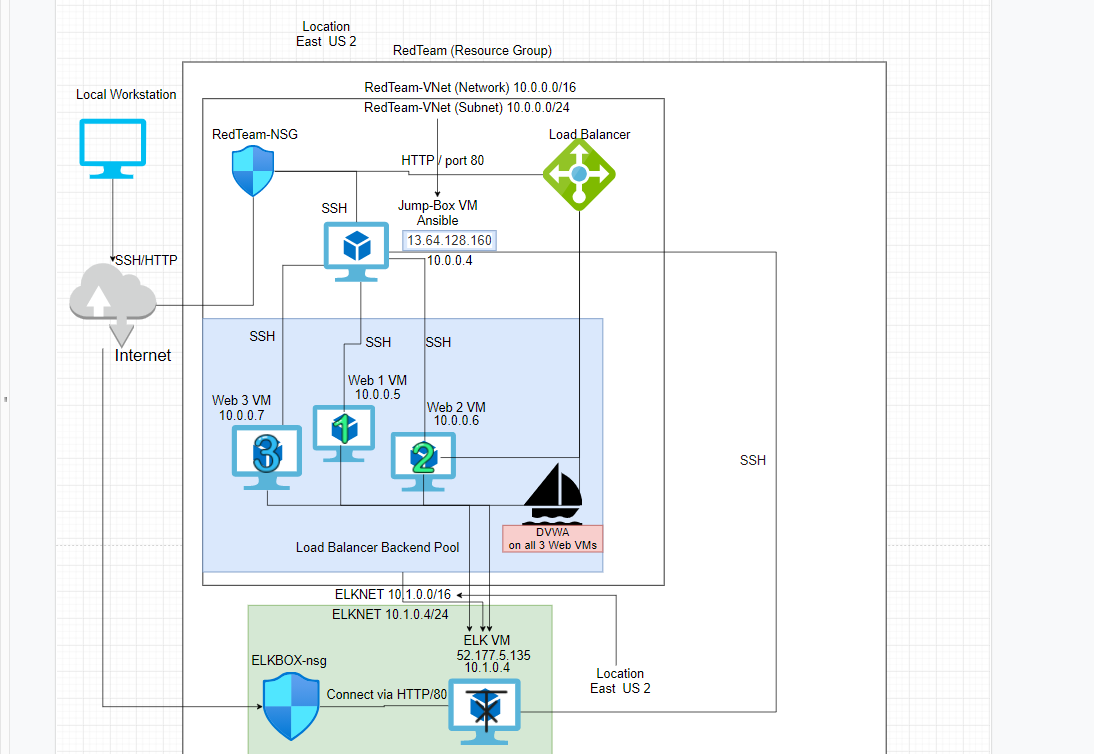
## Automated ELK Stack Deployment

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 config and yaml files may be used to install only certain pieces of it, such as Filebeat/Metericbeat .

<https://github.com/OdellT99/ELK-Project/tree/main/Playbooks>

The link above will guide you to all the following playbooks you will need in order to successfully run the deployment fully.

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,(or known as D\*mn Vulnerable Web App actual name)

Load balancing ensures that the application will be highly available, in addition to restricting traffic to the network.

A aspect load balancers protect , Web traffic as it distributes network and application traffic among servers

A advantage of a jump box is its access control and automation. These virtual environments can automate different operating systems to exist simultaneously on the same machine. While allowing easy maintenance and recovery to access on the virtual machine.

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 is a lightweight shipper for forwarding and centralizing log data.

What does Metricbeat record? Metricbeat is a lightweight shipper that you can install on your servers to periodically collect metrics 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 |

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

| Jump Box | Gateway | 10.0.0.1 | Linux |

| WEB1 |Pentest training | 10.0.0.5 | Linux |

| WEB2 |Pentest training | 10.0.0.6 | Linux |

| WEB3 |Pentest training | 10.0.0.7 | Linux |

| ELKBOX | ELK Server | 10.1.0.4 | Linux |

| Red-Team-LB| Load Balancer | 157.56.162.96 (Red-Team-LB)| N/A

### Access Policies

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

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

ELKServers Public IP: 52.177.5.135 or (What your ELKServers public IP if changed).

Machines within the network can only be accessed by Jump-Box.

This machine allowed me to access your ELK VM.

The IP address is

Jump-Box- 13.64.128.160

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

| Name | Publicly Accessible | Allowed IP Addresses |

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

| Jump Box | Yes/No |13.64.128.160 / 10.0.0.4|

| WEB 1 | No | 10.0.0.5 |

| WEB 2 | No | 10.0.0.6 |

| WEB 3 | No | 10.0.0.7 |

|Elk-Server| Yes/No | |

### Elk Configuration

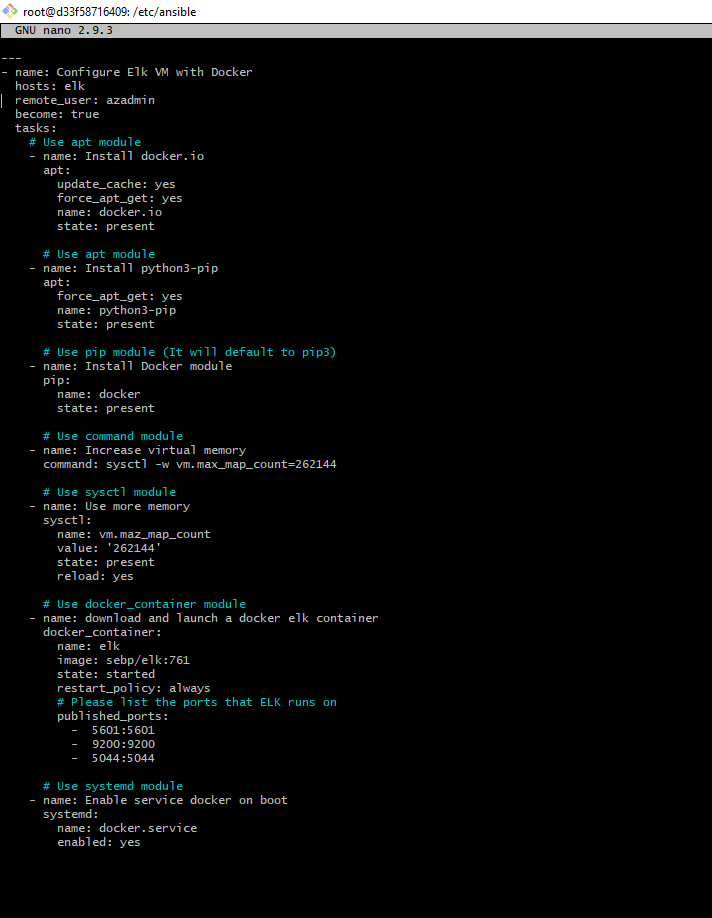
Ansible was used to automate the configuration of the ELK machine. No configuration was performed manually, which is advantageous because…

What is the main advantage of automating configuration with Ansible?

Using Ansible created a configuration process that avoided manual steps into making it easy to deploy specifications and codes to other systems. This allowed users to be able to skip tedious work for writing custom scripts for multiple machines.

The playbook implements the following tasks:

(Click and save to enlarge the image.\_



- Install the following services Docker.io, Python3-pip, Docker module

- Download and launch a docker elk container

-Also Specify remote user (From the SSH key user name) and the group of machines.

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

![TODO: Update the path with the name of your screenshot of docker ps output](Images/docker\_ps\_output.png)

### Target Machines & Beats

This ELK server is configured to monitor the following machines:

WEB Virtual machines 1-3

IP address 1. 10.0.0.5,

2. 10.0.0.6,

3. 10.0.0.7

We have installed the following Beats on these machines:

-Filebeats and Metricbeats

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

FIlebeats: To log events

Metricbeats

These beats were utilized to collect the following information from each machine.

* Filebeats

### 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-config.yml file to /etc/ansible/files/.

- Update the filebeat-playbook.yml file to include the installer curl -L -O https://artifacts.elastic.co/downloads/beats/filebeat/filebeat-7.6.1-amd64.deb

- Run the playbook, and navigate to Kibana, Logs : Add log data, System logs. To check that the installation worked as expected.

- \_Which file is the playbook?

Under your Ansible Files, if you open the files directory you will find the playbook.

- To navigate and check if the ELK server is running use the link below.

http://:5601/app/kibana

Provide the specific commands the user will need to run to download the playbook, update the files, etc.

nano (Will be used to edit config files for specific machines and playbooks.)

Ansible-playbook (Command used to run playbooks and install yml files.)

What is a playbook?

Ansible playbooks are ansible executable language they are written in yml (also known as YAML). We use these playbooks to start different instructions for ansible to follow.

-How to use Ansible playbooks

In order to run playbooks you will have to use the Ansible control node that is already preconfigured.Your first playbook that you will run and called pentest.yml (file provided in folder). Will install Docker.io (Docker is the name of the open platform for developers and sysadmins to build, ship, and run distributed applications. Docker.io) We will use this to ship and create other web containers that you will SSH into

-How to install filebeat

Use this link to install the latest version of Filebeat/Metricbeat <https://www.elastic.co/elastic-stack> Alerentalevly you can find this in your Kibana session (navigating to Metric data then to Docker Metrics, for Metricbeats. You can find filebeat using this curl command curl -L -O https://gist.githubusercontent.com/slape/5cc350109583af6cbe577bbcc0710c93/raw/eca603b72586fbe148c11f9c87bf96a63cb25760/Filebeat > /etc/ansible/files/filebeat-config.ym).

-How to setup Filebeat

You will then update the config file which will be found in /etc/ansible/files where you will edit the filebeat-config.yml using the nano command (In my playbook I have the folder listed as files1 so please edit your playbook to match your folders name). If you don’t have these files make a new directory and move the config file there. The lines that are needed to be updated is line 1806 which looks shows this.

output.elasticsearch:

#Array of hosts to connect to.

hosts: ["10.1.0.4:9200"]

username: "elastic"

password: "changeme”

Once you find this line replace the IP address with the private IP address of your ELK machine.

The second line of code you need to edit is on line 1106 where you will do the same thing in line 1806.

setup.kibana:

host: "10.1.0.4:5601"

Finally, run the playbook using this command ansible-playbook filebeat-playbook.yml and navigate back to Kibana -> Logs to then Add log data. Check the system logs and view the status. If you see data there you have installed it successfully.