## Automated ELK Stack Deployment

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

![TODO: Update the path with the name of your diagram](Images/diagram\_filename.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 \_\_\_\_\_ file may be used to install only certain pieces of it, such as Filebeat.

\_TODO: Enter the playbook file.\_

/ansible/filebeat-playbook.yml

/ansible/metricbeat-playbook.yml

/ansible/filebeat-config.yml

/ansible/metricbeat.yml

/ansible/pentest.yml

/ansible/elk.yml

This document contains the following details:

- Description of the Topologu

- 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 \_redundant\_\_, in addition to restricting \_traffic\_\_\_ to the network.

- \_TODO: What aspect of security do load balancers protect? What is the advantage of a jump box? Protects Servers from Dos Attackers. The advantage of a jumpbox is it is more secure and limits access to resocurces

Integrating an ELK server allows users to easily monitor the vulnerable VMs for changes to the \_\_data\_\_\_ and system \_logs\_.

- \_TODO: What does Filebeat watch for?\_ changes in the log files

- \_TODO: What does Metricbeat record?\_ metricbeat records metrics and stats of the system

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 | 10.0.0.4 | Linux |

| RedWeb1 |VM | 10.0.0.5 | Linux |

| RedWeb2 |VM | 10.0.0.6 | Linux |

| RedWeb3 |VM | 10.0.0.7 | Linux |

| Elk-VM |HOST | 10.1.0.4 | Linus |

### Access Policies

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

Only the \_Jump Box\_\_\_\_ machine can accept connections from the Internet. Access to this machine is only allowed from the following IP addresses:

My Public IP Address

Machines within the network can only be accessed by jumpbox 20.213.60.24\_\_.

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

| Name | Publicly Accessible | Allowed IP Addresses |

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

| Jump Box | No PORT22 | My personal IP |

| RedWeb-1 NO 10.0.0.5

RedWeb-2 NO 10.0.0.6

RedWeb-3 | NO | 10.0.0.7 |

| Elk-VM | NO Kibana | 10.1.0.4 |

### Elk Configuration

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

- \_TODO: What is the main advantage of automating configuration with Ansible?

The main advantage of automating a configuration with Ansible, is that it allows you to automate the process of systems, instead of logging into 50 different systems, it allows you to connect to all machines through one agent

The playbook implements the following tasks:

- \_TODO: In 3-5 bullets, explain the steps of the ELK installation play. E.g., install Docker; download image; etc.\_

1. Install Docker: Docker containers are used to connect to the server

2. Install Pip3: used to install additional items in docker

3. Docker Mods: used pip3 to install docker modules, uses python

4. Increase memory: needed for a heavy server, allows it to launch

5. Download and launch elk: download this container to use elk

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:

10.0.0.5

10.0.0.6

10.0.0.7

10.1.0.4

We have installed the following Beats on these machines:

- \_TODO: Specify which Beats you successfully installed\_

MetricBeat

Filebeat

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

- \_TODO: MetricBeat: collects data from a Vm or a service. If you use it with Elastic Search, Logstash and Kibana, you can monitor data of the systems. It provides graphs and charts of information collects and can put it in a readable form.

FileBeat: file beat allows you to collect logs and files and provides you with an easier way to store the files than to have massive servers on site. It can also be monitored in Kibana for an easier way to observe and monitor data

### 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.cfg\_\_ file to \_etc/ansible\_\_\_.

- Update the \_host and ansible .cfg\_\_\_\_ file to include The machine IPS (Redweb-1, 2, and 3, and the elk machine later) and the ‘ansible\_python\_interpreter=/usr/bin/python3’ to the hosts IP’s

- Run the playbook, and navigate to \_\_kibana\_\_\_ to check that the installation worked as expected. In my case I would use the Elkserver IP: (Elk\_VM IP:5601)

\_TODO: Answer the following questions to fill in the blanks:\_

- \_Which file is the playbook? Where do you copy it?\_

The YML files for Elk\_Vm were install-elk.yml, and pentest.yml

These files were copied to /etc/ansible

- \_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?\_

- to run the ansible playbook on a specific machine you need to add it through the nano ‘hosts’ file. To set the filebeats you set the location via the filebeat-config.yml.

- \_Which URL do you navigate to in order to check that the ELK server is running? KIBANA (ELK\_VM IP:5601)

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

For this assignment, we were able to download a YML file $ sudo apt-get install python-yaml, then downloaded the file from gitlab. With YML we can create a yml by using the command nano <name\_of\_file>.yml this will allow you to make a playbook. once in you need to include --- to start the file, next you format the files you use a – to separate the commands, once done you run the comman ansible-playbook<name\_of\_file> and it will verify everything in the file.