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 available, in addition to filtering access to the network.

* Load balancing is effective at preventing DDoS attacks. The advantage of the Jump Box is essentially to provide a gateway router to your private network ensuring that all of your other machines in the network do not directly face the internet providing a more secure network.

Integrating an ELK server allows users to easily monitor the vulnerable VMs for changes to the network and to monitor and correlate system logs.

* Filebeat collects data about the file system, including which files have changed and when they were changed.
* Metricbeat collects machine metrics, such as uptime.

The configuration details of each machine may be found below.

| Name | Function |-------------| IP Address | Operating System | |----------|----------|-------------|-------------------------------| | Jump Box | Gateway Router | 10.0.0.4 | Linux | | Web-1 | DVWA Container | 10.0.0.5 | Linux | | Web-2 | DVWA Container | 10.0.0.6 | Linux || ELK | ELK Server | 10.1.0.4 | Linux |

**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:

* 76.100.248.254

Machines within the network can only be accessed by JumpBox.

* The ELK server may be accessed from the Web-1, Web-2 and JumpBox machines.

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

| **Name** | **Publicly Accessible** | **Allowed IP Addresses** |
| --- | --- | --- |
| JumpBox | No | 10.0.0.1 // 10.0.0.2 |
| Web-1 | No | 10.0.0.4 // 10.1.0.4 |
| Web-2 | No | 10.0.0.4 // 10.1.0.4 |
| Final-Project-VM-1 | No | 10.0.0.4 // 10.0.0.7 // 10.0.0.8 // 10.0.0.9 |

**Elk Configuration**

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

* The main advantage of automating configuration with Ansible is that it enables IT administrators the ability to automate your daily work tasks and give the administrator more time to focus on the needs of the business, thus providing more value to the company.

The 'install-elk.yml' playbook implements the following tasks:

* Configure Elk VM with Docker
* Install docker.io
* Install pip3
* Download and launch a docker elk container

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

Upload image her and enter the github path

**Target Machines & Beats**

This ELK server is configured to monitor the following machines:

* Web-1 // 10.0.0.4
* Web-2 // 10.0.0.4

We have installed the following Beats on these machines:

* Filebeat
* Metricbeat

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

* Filebeat collects data about the file system, including which files have changed and when they were changed.
* Metricbeat collects machine metrics, such as uptime.

**Using the Playbook**

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 YAML file to '/etc/ansible' directory.
* Update the /etc/ansible/hosts' file to include 'hosts' group, private IP address, the following line 'ansible\_python\_interpreter=/usr/bin/python3'
* Run the playbook and navigate to 'curl localhost/setup.php' to check that the installation worked as expected.
* The playbooks are listed as 'install-elk.yml' // 'filebeat-playbook.yml' // 'metricbeat-playbook.yml' // 'ansible\_config.yml' and are meant to be copied in the '/etc/ansible' directory.
* Update the '/etc/ansible/hosts' directory with the hosts group name with the correlating IP addresses underneath to specify on which machines to run the playbooks.
* To check if the ELK server is running, navigate to 'http://[your.VM.IP]:5601/app/kibana'
* install-elk.yml: This will install the ELK stack on the VM in your <hosts> group.
* install-filebeat.yml: This will install Filebeat on your <hosts> group.
* install-metricbeat.yml: This will install Metricbeat on your <hosts> group.