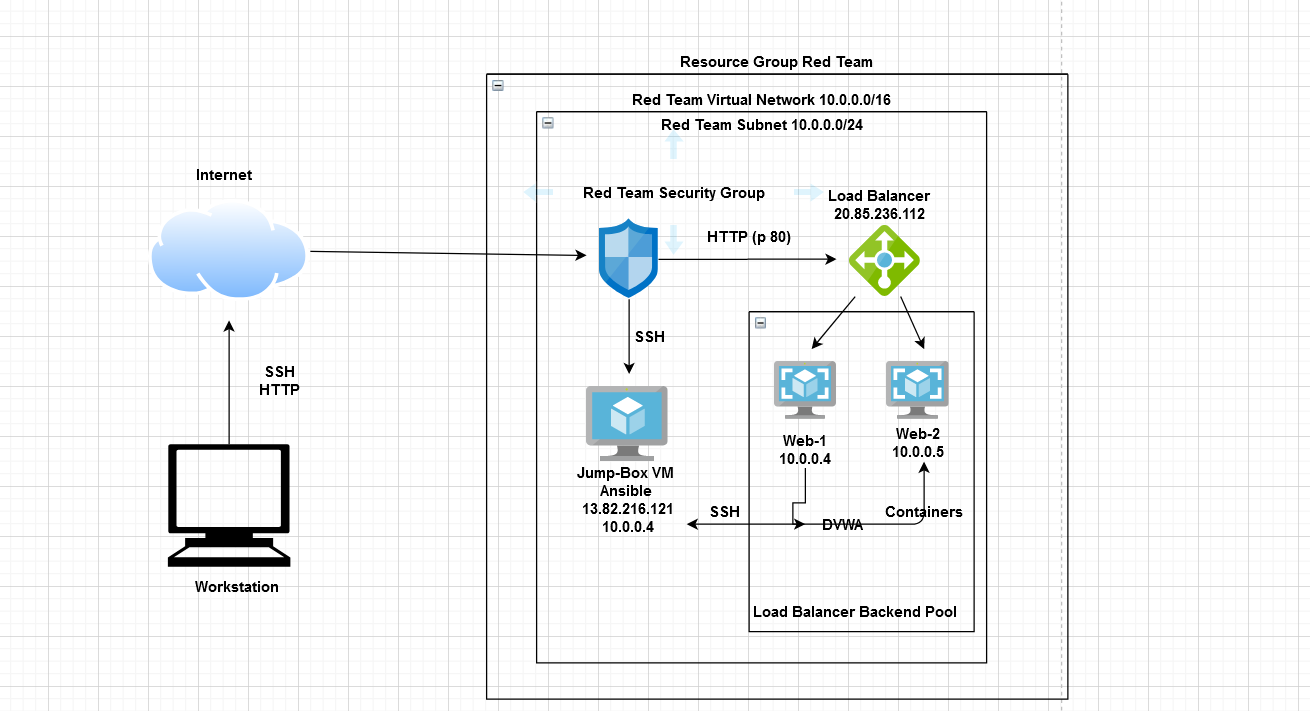
## **Automated ELK Stack Deployment**

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

* filebeat-playbook.yml,metricbeat-playbook.yml,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 access to the network. Load balancers help ensure environment availability through distribution of incoming data to web servers. Jump boxes allow for more easy administration of multiple systems and provide an additional layer between the outside and internal assets.

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

* Filbeats watch for log directories or specific log files.
* Metricbeat helps you monitor your servers by collecting metrics from the system and services running on the server.

The configuration details of each machine may be found below.

|  |  |  |  |
| --- | --- | --- | --- |
| **Name** | **Function** | **IP Address** | **Operating System** |
| Jump Box | Gateway | 10.0.0.4 | Linux (Ubuntu) |
| Web 1 | Server | 10.0.05 | Linux (Ubuntu) |
| Web 2 | Server | 10.0.06 | Linux (Ubuntu) |
| ELK Server | Log Server | 10.1.0.5 | Linux (Ubuntu) |

### **Access Policies**

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

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

-Personal IP address

Machines within the network can only be accessed by the Jump Box. The Elk Machine can have access from personal IP address through port 5601.

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

|  |  |  |
| --- | --- | --- |
| **Name** | **Publicly Accessible** | **Allowed IP Addresses** |
| Jump Box | Yes | Personal |
| Load Balancer | Yes | Open |
| Web 1 | No | 10.0.0.5 |
| Web 2 | No | 10.0.0.6 |
| ELK Server | Yes | Personal |

### Elk Configuration

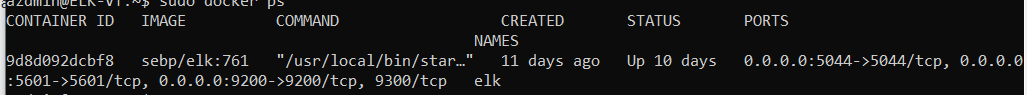
Ansible was used to automate configuration of the ELK machine. No configuration was performed manually, which is advantageous because...

* In case we need to configure more machines,we can just run the ansible playbook instead of going to every machine and configuring individually.

The playbook implements the following tasks:

* Install docker.io
* Install PIP
* Install docker python module
* Download and Install a Docker elk container
* run command to increase the memory

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:

* Web 1 (10.0.0.5)
* Web 2 (10.0.0.6)

We have installed the following Beats on these machines:

* FileBeat
* Metric Beat

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

We have installed the following Beats on these machines:

* Filebeat and Metricbeat

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

* Filebeat will collect any changes made.
* Metric beat will collect the metrics and statistics
* Filebeat watches for the changes in the files in the locations that we specify or the log files and then collects and send the data to logstash/elasticsearch for example the modifications in a file.
* Metricbeat collects the metric data from the services and the operating system and sends it to logstash/elasticsearch such as Apache service

### **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 configuration file from your Ansible container to your Web VM's
* Update the /etc/ansible/hosts file to include the IP address of the Elk Server VM and webservers.
* Run the playbook, and navigate to http://[Elk\_VM\_Public\_IP]:5601/app/kibana to check that the installation worked as expected.
* *Which file is the playbook?* The Filebeat-configuration
* *Where do you copy it?* copy /etc/ansible/files/filebeat-config.yml to /etc/filebeat/filebeat.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?* update filebeat-config.yml -- specify which machine to install by updating the host files with ip addresses of web/elk servers and selecting which group to run on in ansible
* \_Which URL do you navigate to in order to check that the ELK server is running? http://[your.ELK-VM.External.IP]:5601/app/kibana.