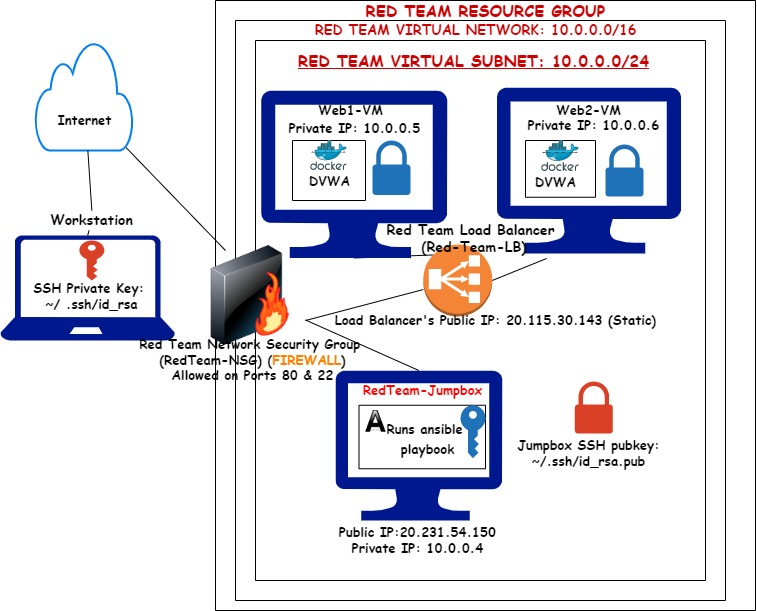
**###** Automated ELK Stack Deployment

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

* Filebeat.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 protect servers from cyber attacks such as a Distributed Denial-of-Service (DDos) attack. By distributing traffic amongst servers to lighten the load of said malicious traffic. One benefit of using a jump box is that it restricts access and protects the machine machines from the Internet.

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

What does Filebeat watch for? **Logs files monitored by Filebeat**

What does Metricbeat record? **Metrics monitored by Metricbeat**

The configuration details of each machine may be found below.

| \*\*Name\*\* | \*\*Function\*\* | \*\*IP Address\*\* | \*\*Operating System\*\* |

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

| Jumpbox | Gateway | 10.0.0.4 | Ubuntu 18.04-LTS |

| Web-1 | VM | 10.0.0.8 | Ubuntu 18.04-LTS |

| Web-2 | VM | 10.0.0.9 | Ubuntu 18.04-LTS |

| ELKbase | ELKStack | 10.1.0.5 | Ubuntu 18.04-LTS |

### 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:

* Home-IP

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

* 10.0.0.4

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

| \*\*Name\*\* | \*\*Publicly Accessible\*\* | \*\*Allowed IP Address\*\* |

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

| Jump Box | No | Home-IP |

| Web VMs | No | 10.0.0.4 & Home-IP |

| ELKbase | No | 10.0.0.4 & Home-IP |

### Elk Configuration

Ansible was used to automate configuration of the ELK machine. No configuration was performed manually, which is advantageous because it minimizes the likelihood of human error. However, it should be noted that the syntax/commands used within the configuration files and playbooks may need to be changed to tailor to the virtual machine(s).

* Ansible ensures that provisioning scripts can be identically ran between systems ans users.

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

* Installs Docker.io on the ELK machine
* Installs Python3-pip
* Installs docker module
* Uses sysctl to increase System Virtual Memory
* Downloads and launches a docker elk container with exposed ports

Sample from configuration file for docker:

```bash

---

-name: Configure Elk VM with Docker

hosts: elk

remote\_user: RedAdmin

become: true

tasks:

# Use apt module

- name: Install docker.io

apt:

update\_cache: yes

force\_apt\_get: yes

name: docker.io

state: present

# Use apt module

- name: Install python3-pip

apt:

force\_apt\_get: yes

name: python3-pip

state: present

# Use pip module (It will default to pip3)

- name: Install Docker module

pip:

name: docker

state: present

```

### Target Machines & Beats

This ELK server is configured to monitor the following machines:

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

We have installed the following Beats on these machines:

* Filebeat
* Metricbeat

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

* Filebeat collects log events, which we use to track and monitor user log messages.
* Metricbeat collects metric data, which we use to track user system health and metrics.

### 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 files and the playbooks to etc/ansible.

- Update the hosts file to include the private IP address of the machine you wish to install and configure ELK in.

- Run the playbook, and navigate to Kibana (Public\_IP:5601) to check that the installation worked as expected.

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

**The playbook file would be the YAML file that is provided; it should be copied into the /etc/ansible directory in the ansible container.**

- \_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?

**One must update the hosts file in the /etc/ansible directory. If one needs to specify the machine to install the ELK server, the private IP address of a specific machine(s) is needed.**

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

**http://[your.VM.IP]:5601/app/kibana**