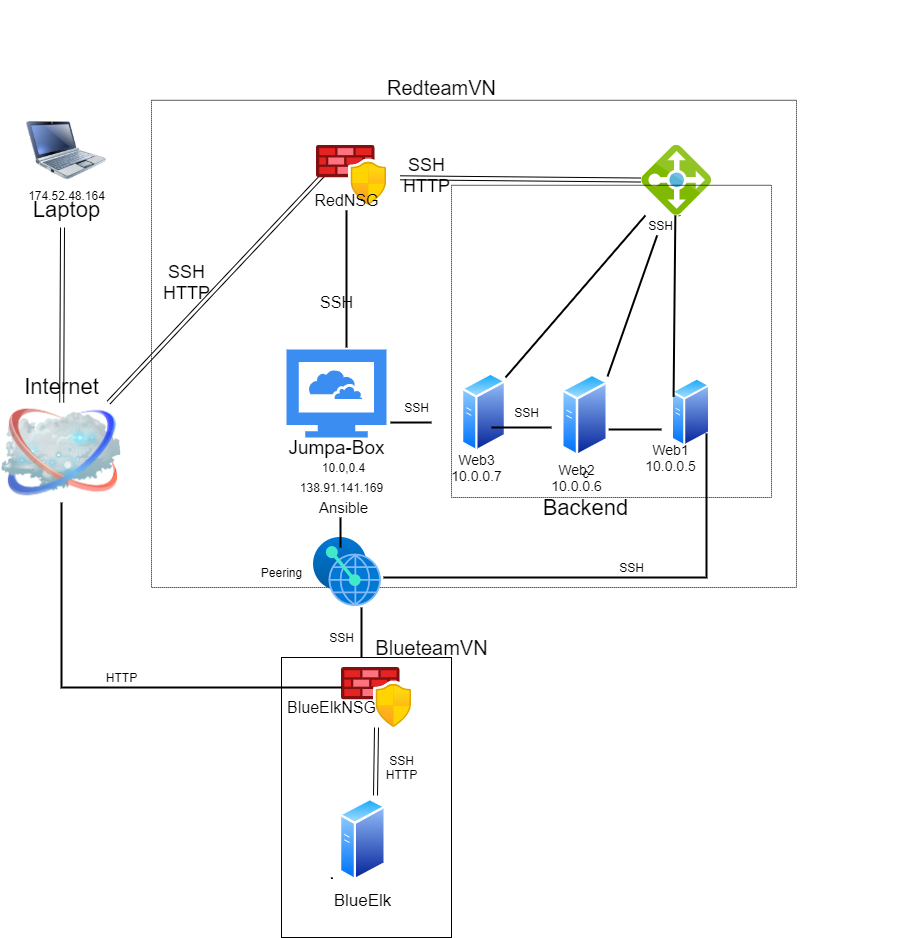
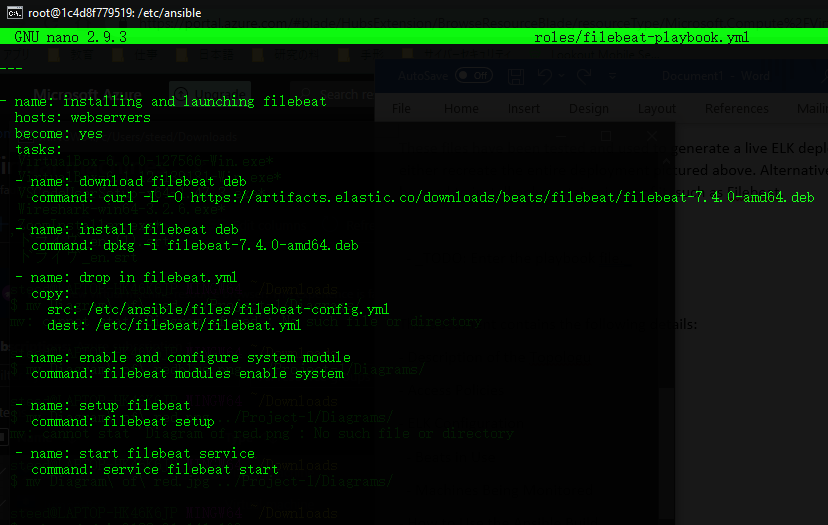
**Automated ELK Stack Deployment**

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

RedTeam and BlueTeam VN



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



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 durable, in addition to restricting traffic to the network.

- Load balancers share the load and will take over in the event of a server going down. A jump box adds another layer of security.

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

- Filebeat monitors the log files and forwards them for indexing and ships them to Elasticsearch and Logstash.

- Microbeat collects the servers operating system metrics and ships them to Elasticsearch and Logstash.

The configuration details of each machine may be found below.

| Name | Function | IP Address | Operating System |

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

| Jumpa-Box | Gateway | 10.0.0.4 | Linux |

| BlueElk | Monitoring | 10.2.0.5 | Linux |

| Web-1 | Container | 10.0.0.5 | Linux |

| Web-2 | Container | 10.0.0.5 | Linux |

| Web-3 | Container | 10.0.0.5 | Linux |

**Access Policies**

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

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

174.52.48.164

Machines within the network can only be accessed by Gateway.

- JumpaBox 138.91.141.169

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

| Name | Publicly Accessible | Allowed IP Addresses |

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

| JumpaBox | Yes | 174.52.48.164 |

| BlueElk | Yes | 138.91.141.169 |

| Web-1 | No | 10.0.0.4 |

| Web-2 | No | 10.0.0.4 |

| Web-3 | No | 10.0.0.4 |

**Elk Configuration**

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

- You save a lot of time and effort.

The playbook implements the following tasks:

- Download the installer for filebeat.

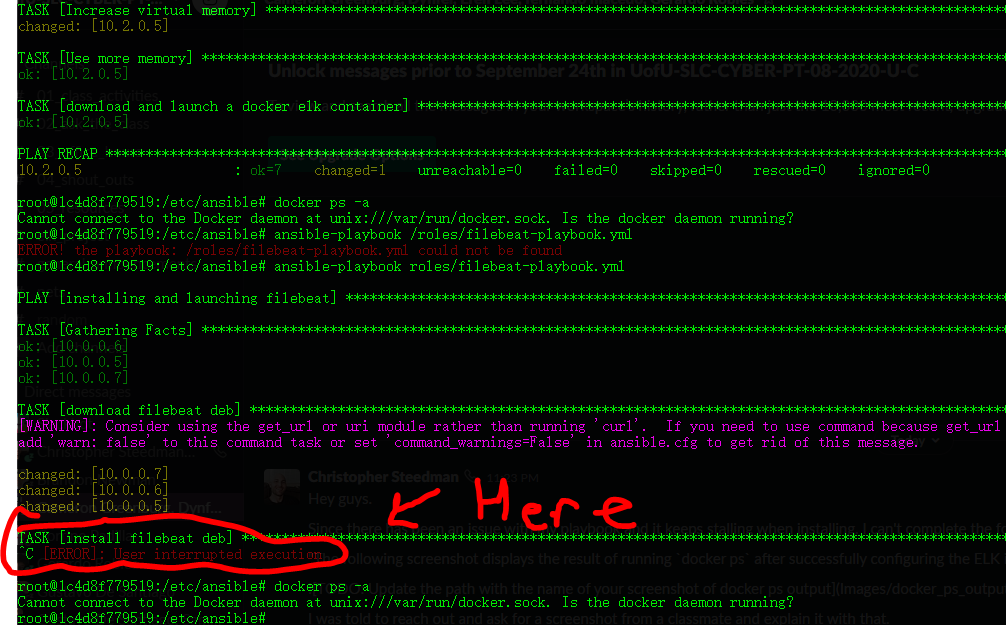
- Install filebeat on the system.

- Set the location.

- Start the system.

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

File beat code is correct and was checked by multiple people, however, the filebeat didn’t successfully install and a screenshot can not be provided.



**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

-web 3: 10.0.0.7

We have installed the following Beats on these machines:

* deb

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

-  It collects log events, and forwards them either to Elasticsearch or Logstash for indexing.

**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 file to ansible directory.

- Update the ansible Host file to include the VMs

- Run the playbook, and navigate to http://[your.VM.IP]:5601/app/kibana to check that the installation worked as expected.