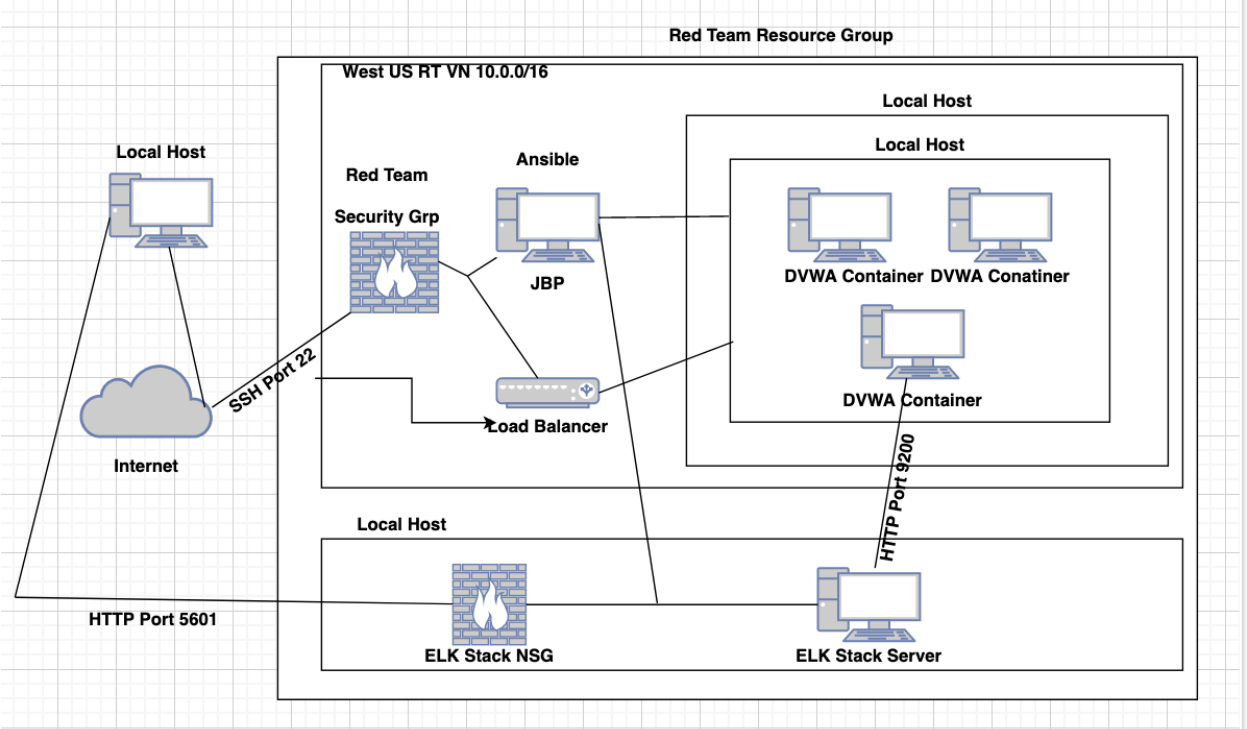
Deployed ELK Stack

The network indicated below was created using the files available in this repository.



The ELK deployment on Azure was created with the following files:

- *DVWA*
- *ELK Installation*
- *Filebeat*
- *Metricbeat*

This document contains the following:

- Topology
- Access Policies
- Configuration
    - Beats in Use
    - Monitored Machines
- Ansible Build How-to

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.

A load-balanced instance offers an application that will be highly available, while restricting access to the network.

- *Load balancers insure availability of servers and services*

- *A jumpbox acts as a gateway to private servers, adding to our security and privacy.*

Utilizing an ELK server aids in monitoring VMs for changes.

- *Metricbeat*
- *Filebeat*

The configuration details of each machine may be found below.

Name	Function	IP Address	Operating System
Jumpbox	Gateway	10.0.0.5	Linux (Ubuntu)
DVWA 1	Webserver	10.0.0.11	Linux (Ubuntu)
DVWA 2	Webserver	10.0.0.6	Linux (Ubuntu)
DVWA 3	Webserver	10.0.0.12	Linux (Ubuntu)
ELK	Elasticsearch Stack	10.1.0.4	Linux (Ubuntu)

Access Policies

The internal machines can’t be accessed from the public Internet.

Only the jumpbox machine can accept connections from the Internet.

Machines within the network can only be accessed by the jumpbox.

- *jumpbox*
    - *Public IP: 20.69.121.39*
    - *Private IP: 10.0.0.5*

Summary of access policies:

Name	Publicly Accessible	Allowed IP Address
Jumpbox	Yes- Port 22 (SSH)	***.***.**.***
DVWA 1,2,3	No	Load Balancer-**.***.**.**
Load Balancer	Yes- Port 80 (HTTP)	*
ELK	Yes- Port 5601 (Kibana), Port 9200 (HTTP API)	10.0.0.0/16

Elk Configuration

The ELK machine used Ansible to automate configuration.

The playbook triggers the below:

- *Installs docker*
- *Installs python3-pip module*
- *Installs docker module for pip3*
- *Increases/Uses more memory*
- *Downloads and launches ELK container*

Target Machines & Beats

This ELK server is configured to monitor the following machines:

- *10.0.0.6*
- *10.0.0.11*
- *10.0.0.12*