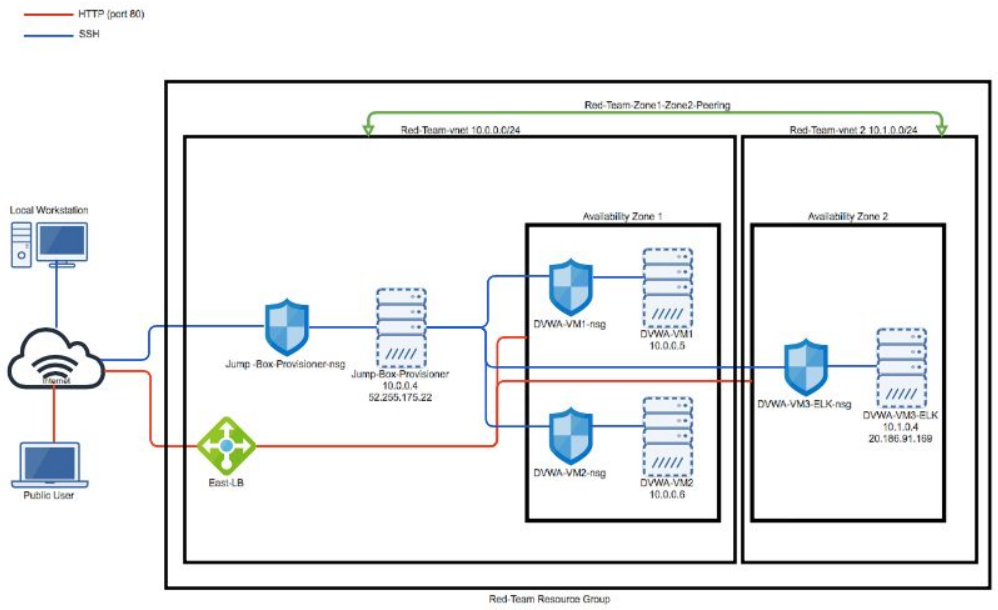
Automated ELK Stack Deployment

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



Project1/Project_1_Red-Team Network Diagram.png
https://tinyurl.com/yayqcrrp

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 main.yml playbook file may be used to install only certain pieces of it, such as Filebeat.
Project1/filebeat-playbook.png https://tinyurl.com/ybpjhgw8

```
---
- name: installing and launching filebeat
  hosts: webservers
  become: true
  tasks:

  - name: download filebeat deb
    command: curl -L -O
https://artifacts.elastic.co/downloads/beats/filebeat/filebeat-7.4.0-amd64.deb

  - name: install filebeat deb
    command: dpkg -i filebeat-7.4.0-amd64.deb

  - name: drop in filebeat.yml
    copy:
      src: ./files/filebeat-configuration.yml
      dest: /etc/filebeat/filebeat.yml

  - name: enable and configure system module
    command: filebeat modules enable system

  - name: setup filebeat
    command: filebeat setup

  - name: start filebeat service
    command: service filebeat start
```

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 efficient, in addition to restricting access to the virtual network. This incorporates added security measures through preventing DoS attacks from shutting down a machine, affecting the entire network. The load balancers spread network traffic across multiple servers as well as perform health probes to ensure that they are functioning properly before directing traffic to them. The advantage of the jump box is that it forces all traffic through a single, monitored node.

Integrating an ELK server allows users to easily monitor the vulnerable VMs for changes to the network and system health. Filebeat creates logs of data regarding the network filesystem, while Metricbeat collects data regarding machine metrics such as CPU, memory, and runtime.

The configuration details of each machine may be found below.

Name	Function	IP Address	Operating System
Jump-Box-Provisioner	Gateway	10.0.0.4	Linux
DVWA-VM1	Virtual Network	10.0.0.5	Linux
DVWA-VM2	Virtual Network	10.0.0.6	Linux
DVWA-VM#-ELK	Server/Network Manager	10.1.0.4	Linux

Access Policies

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

Only the ELK machine can accept connections from the Internet. Access to this machine is only allowed from the following IP addresses:
73.137.27.116, 10.0.0.4, 10.0.0.5, 10.0.0.6, 10.1.0.4

Machines within the network can only be accessed by ssh. The local host machine is the only machine that is able to access the ELK VM via ssh with IP address 73.137.27.116.

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

Name	Publicly Accessible	Allowed IP Addresses
Jump-Box-Provisioner	yes	10.0.0.4, 73.137.27.116
DVWA-VM1	no	10.0.0.5

| DVWA-VM2 | no | 10.0.0.6 |
| DVWA-VM#-ELK | yes | 10.1.0.4, 73.137.27.116 |

Elk Configuration

Ansible was used to automate configuration of the ELK machine. No configuration was performed manually, which is advantageous because automated deployments make it easy to configure and patch multiple systems at once. This can help to mitigate certain security risks that may come along with a much more lengthy manual patch deployment method.

The playbook implements the following tasks:
-increase virtual memory to 262144
-install docker and python
-download image and create sebp/elk container
-configure machine with mapping for ports 5601, 9200, and 5044

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

```
ansibleadmin@DVWA-VM3-ELK:~$ sudo docker ps
CONTAINER ID        IMAGE               COMMAND             CREATED             STATUS              PORTS
    NAMES
ansibleadmin@DVWA-VM3-ELK:~$ sudo docker start elk
elk
ansibleadmin@DVWA-VM3-ELK:~$ sudo docker ps
CONTAINER ID        IMAGE               COMMAND                  CREATED             STATUS              PORTS
                                                                NAMES
275ed5151161        sebp/elk            "/usr/local/bin/star…"   12 days ago         Up 4 seconds        0.0.0.0:50
44->5044/tcp, 0.0.0.0:5601->5601/tcp, 0.0.0.0:9200->9200/tcp, 9300/tcp   elk
ansibleadmin@DVWA-VM3-ELK:~$
```

Project1/Docker-ps.png
https://tinyurl.com/y8pnmend

Target Machines & Beats
This ELK server is configured to monitor the following machines:
DVWA-VM1 | 10.0.0.5
DVWA-VM2 | 10.0.0.6

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 network file logs, which allows for easy access to specific desired log types through filtered searches. Metricbeat collects metric information for the operating system and services that are running on a network including uptime, CPU, and memory. The elasticsearch output can be easily viewed and sent using Kibana.

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 to </etc/ansible/roles/files>

.
- Update the configuration file to include the private IP address of the ELK VM (10.1.0.4)
- Run the playbook, and navigate to the ELK VM to check that the installation worked as expected. You should also go to the ELK stack server GUI by typing http://[your.VM.IP]:5601 into the host machine web browser. In this case the ELK public IP that would be inserted into the above web address is 20.186.91.169.

FAQs
- *Which file is the playbook? Where do you copy it?_*
    The playbook file is “filebeat-playbook.yml and it is copied to the /etc/filebeat/ directory created by running the playbook.
- *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?_*
    The host file must be updated with the IPs of the DVWA and ELK VMs before running the playbook as shown below. The IPs are split into [webservers] for the DVWA machines and [elkservers] for the ELK machine in order to specify in the playbook which machines it should run on.

…
```
# /etc/ansible/hosts
  [webservers]
  10.0.0.5
  10.0.0.6

  [elkservers]
  10.1.0.4
```
…

- Which URL do you navigate to in order to check that the ELK server is running?
    In order to ensure that the ELK server is running you should navigate to http://[your.VM.IP]:5601 from the host machine web browser. In this case the address would be http://20.186.91.169:5601.