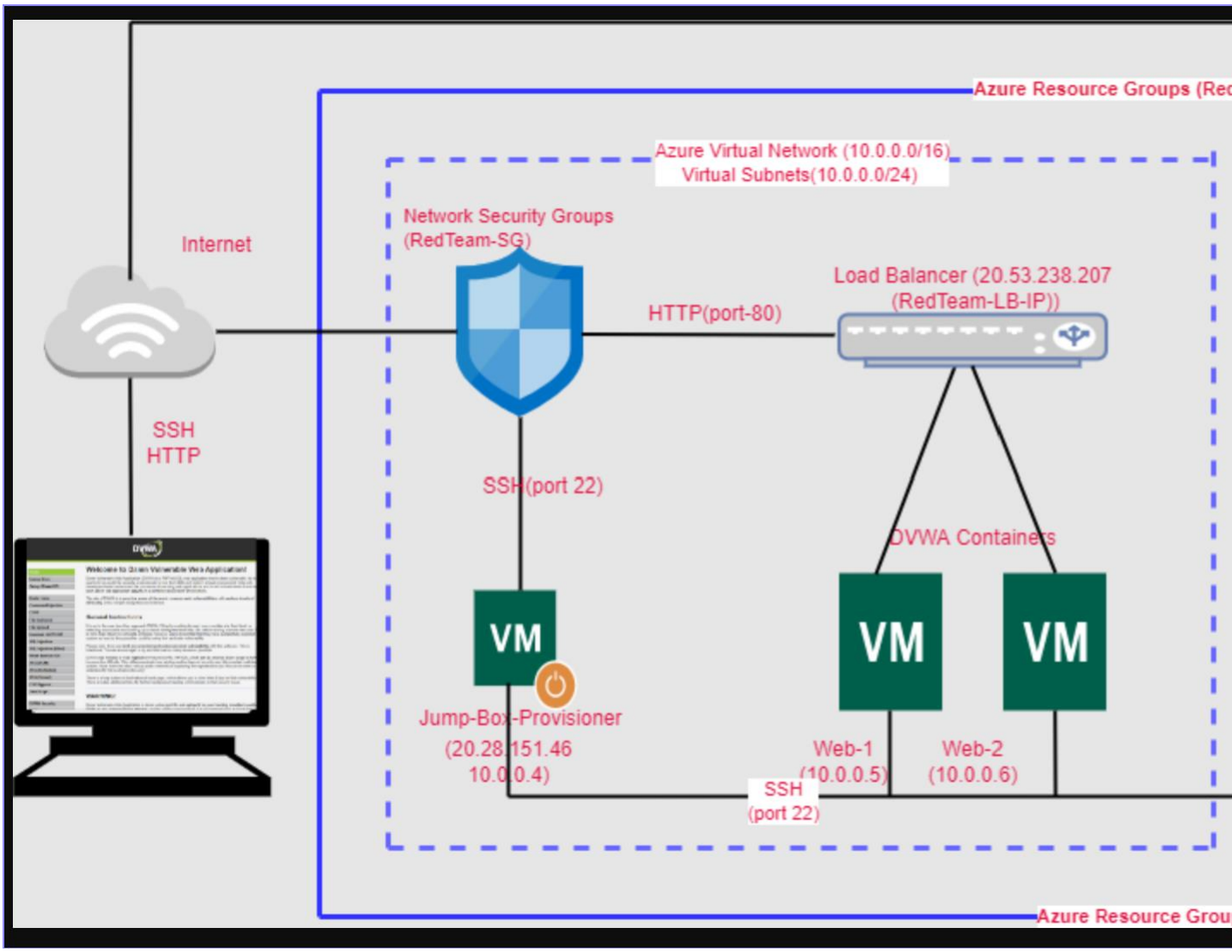
Automated ELK Stack Deployment

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

See in the **Ansible folder** for the below

- **Hosts**
- **Ansible Configuration**
- **Ansible ELK Installation and VM Configuration**
- **Filebeat Config**
- **Filebeat Playbook**
- **Metricbeat Config**
- **Metricbeat Playbook**

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 __functional and available___, in addition to restricting __traffic___ to the network.

What aspect of security do load balancers protect?
The Load balancers add resiliency by rerouting live traffic from one server to another if a server falls prey to a DDoS attack or otherwise becomes unavailable.
What is the advent age of a jump box?
A Jump Box Provisioner is also important as it prevents Azure VMs from being exposed via a public IP Address. This allows us to do monitoring and logging on a single box. We can also restrict the IP addresses able to communicate with the Jump Box, as we've done here

Integrating an ELK server allows users to easily monitor the vulnerable VMs for changes to the __network___ and system __logs___.
What does Filebeat watch for?_
Filebeat monitors the log files or locations that you specify, collects log events, and forwards them either to Elasticsearch or Logstash for indexing

What does Metricbeat record?_
Metricbeat takes the metrics and statistics that it collects and ships them to the output that you specify, such as Elasticsearch or Logstash.

The configuration details of each machine may be found below.

Name	Function	IP Address	Operating System
Jump Box	Gateway	10.0.0.4 / 75.248.172.80	Linux
Web-1	UbuntuServer	10.0.0.5 / 20.53.238.207	Linux
Web-2	UbuntuServer	10.0.0.6 / 20.53.238.207	Linux
DVWA-VM3	UbuntuServer	10.0.0.7 / 20.53.238.207	Linux
ELKVM	UbuntuServer	10.2.0.4 / 20.84.136.248	Linux

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:
- Workstation MY Public IP through TCP 5601

Machines within the network can only be accessed by __Workstation and Jump-Box-Provisioner through SSH Jumb-Box___.
Which machine did you allow to access your ELK VM?
Jump-Box-Provisioner IP : 10.1.0.4 via SSH port 22
What was its IP address?_
Workstation MY Public IP via port TCP 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	75.248.172.80 (Workstation IP on SSH 22)
Web-1	No	10.0.0.4 on SSH 22
Web-2	No	10.0.0.4 on SSH 22
DVWA-VM3	No	10.0.0.4 on SSH 22
ELKVM	No	Workstation MY Public IP using TCP 560

Elk Configuration

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

What is the main advantage of automating configuration with Ansible?_
Ansible lets you quickly and easily deploy multitier applications through a YAML playbook.
No need to write custom code to automate your systems.
Ansible will also figure out how to get your systems to the state you want them to be in.

The playbook implements the following tasks:

In 3-5 bullets, explain the steps of the ELK installation play. E.g., install Docker; download image; etc._

To specify a different group of machines
```
  - name: Config elk VM with Docker
    hosts: elk
    become: true
    tasks:
```
To install Docker.io
```
  - name: Install docker.io
    apt:
      update_cache: yes
      force_apt_get: yes
      name: docker.io
```

```
      state: present
To install Python-pip
  - 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
      `docker`, which is the Docker Python pip module.
To Increase Virtual Memory
 - name: Use more memory
   sysctl:
     name: vm.max_map_count
     value: '262144'
     state: present
     reload: yes
Download and Launch ELK Docker Container (image sebp/elk)
 - name: Download and launch a docker elk container
   docker_container:
     name: elk
     image: sebp/elk:761
     state: started
     restart_policy: always
Published ports 5044, 5601 and 9200 were made available
     published_ports:
       -  5601:5601
       -  9200:9200
       -  5044:5044
```

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

Connect to jump-Box-Provisioner VM

```
cneel@LAPTOP-5EG30UT7 MINGW64 /c/Neela/GT Cyber Security
$ ssh redteam@20.28.151.46
```

```
redteam@Jump-Box-Provisioner:~$ sudo docker container list -a
CONTAINER ID   IMAGE                          COMMAND                  CREATED       STATUS                      PORTS     NAMES
b0ff4603f08b   cyberxsecurity/ansible         "/bin/sh -c /bin/bas…"   5 weeks ago   Exited (255) 5 weeks ago              unruffled_brahmagupta
c56cd9441e07   cyberxsecurity/ansible         "/bin/sh -c /bin/bas…"   5 weeks ago   Exited (137) 5 weeks ago              heuristic_brattain
3187902eef67   cyberxsecurity/ansible:latest  "/bin/sh -c /bin/bas…"   5 weeks ago   Exited (137) 2 weeks ago              cool_wilbur
```

web-1 and web-2 VM docker info

```
redteam@Jump-Box-Provisioner:/var/run$ sudo docker start cool_wilbur
cool_wilbur
redteam@Jump-Box-Provisioner:/var/run$ sudo docker attach cool_wilbur
root@3187902eef67:~# cd /etc/ansible
root@3187902eef67:/etc/ansible# ls
ansible.cfg  elk.yml  filebeat-config.yml  hosts  pentest.yml
root@3187902eef67:/etc/ansible# ansible-playbook /etc/ansible/pentest.yml
[WARNING]: ansible.utils.display.initialize_locale has not been called, this may result in incorrectly calculated text widths that can cause Display to print
incorrect line lengths

PLAY [Config Web VM with Docker] ***********************************************************************************************************************

TASK [Gathering Facts] *********************************************************************************************************************************
ok: [10.0.0.6]
ok: [10.0.0.5]

TASK [docker.io] ***************************************************************************************************************************************
ok: [10.0.0.5]
ok: [10.0.0.6]

TASK [Install pip3] ************************************************************************************************************************************
ok: [10.0.0.5]
ok: [10.0.0.6]

TASK [Install Docker python module] ********************************************************************************************************************
ok: [10.0.0.6]
ok: [10.0.0.5]

TASK [download and launch a docker web container] ******************************************************************************************************
[DEPRECATION WARNING]: The container_default_behavior option will change its default value from "compatibility" to "no_defaults" in community.docker 2.0.0. To
remove this warning, please specify an explicit value for it now. This feature will be removed from community.docker in version 2.0.0. Deprecation warnings can
be disabled by setting deprecation_warnings=False in ansible.cfg.
changed: [10.0.0.6]
changed: [10.0.0.5]

TASK [Enable docker service] ***************************************************************************************************************************
ok: [10.0.0.5]
ok: [10.0.0.6]

PLAY RECAP *********************************************************************************************************************************************
10.0.0.5                   : ok=6    changed=1    unreachable=0    failed=0    skipped=0    rescued=0    ignored=0
10.0.0.6                   : ok=6    changed=1    unreachable=0    failed=0    skipped=0    rescued=0    ignored=0

root@3187902eef67:/etc/ansible#
```

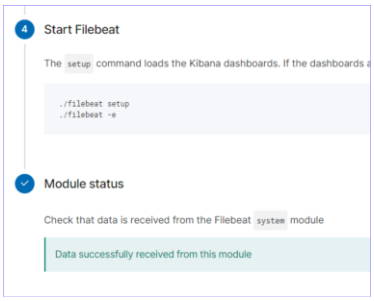
```
exit
redteam@Jump-Box-Provisioner:~$ sudo docker ps
CONTAINER ID   IMAGE     COMMAND   CREATED   STATUS    PORTS     NAMES
redteam@Jump-Box-Provisioner:~$ sudo docker container list -a
CONTAINER ID   IMAGE                          COMMAND                  CREATED       STATUS                      PORTS
    NAMES
b0ff4603f08b   cyberxsecurity/ansible         "/bin/sh -c /bin/bas…"   5 weeks ago   Exited (255) 5 weeks ago
    unruffled_brahmagupta
c56cd9441e07   cyberxsecurity/ansible         "/bin/sh -c /bin/bas…"   5 weeks ago   Exited (137) 5 weeks ago
    heuristic_brattain
3187902eef67   cyberxsecurity/ansible:latest  "/bin/sh -c /bin/bas…"   5 weeks ago   Exited (0) 13 seconds ago
    cool_wilbur
redteam@Jump-Box-Provisioner:~$ sudo docker container start cool_wilbur
cool_wilbur
redteam@Jump-Box-Provisioner:~$ sudo docker container attach cool_wilbur
root@3187902eef67:~# cd /etc/ansible
root@3187902eef67:/etc/ansible# ls
ansible.cfg  elk.yml  filebeat-config.yml  filebeat-playbook.yml  hosts  pentest.yml
root@3187902eef67:/etc/ansible#
```

Target Machines & Beats
This ELK server is configured to monitor the following machines:

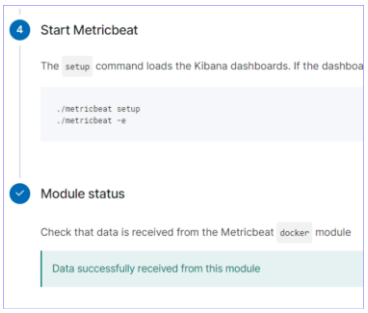
List the IP addresses of the machines you are monitoring_
Web-1: 10.0.0.5
Web-2: 10.0.0.6
DVWA-VM3: 10.0.0.7

We have installed the following Beats on these machines:

Filebeat:



Metricbeat:



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 __yml___ file to __ansible folder___.
- Update the __config___ file to include remote users and ports.
- Run the playbook, and navigate to ____ to check that the installation worked as expected.

TODO: Answer the following questions to fill in the blanks:
- _Which file is the playbook?
cd /etc/ansible
ansible-playbook elk.yml
Where do you copy it?_
- _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?_
- _Which URL do you navigate to in order to check that the ELK server is running?