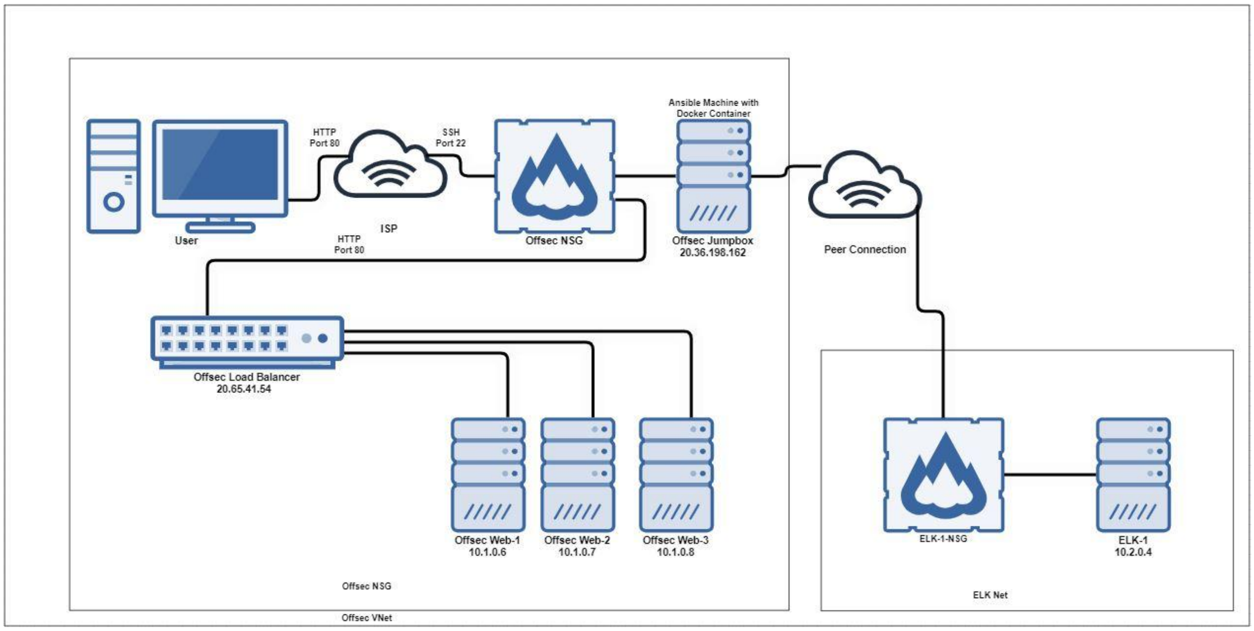
Automated ELK Stack Deployment

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

- ***https://github.com/averettsm/GTech-Cybersecurity/tree/main/Ansible%20Docker%20Scripts***

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 **_Redundant_** , in addition to restricting **_Unauthorized Access_** to the network.

- ***Load balancers protect the availability of the network.***
- ***A jump box provides a secure means of accessing a network without exposing it to the public internet.***

Integrating an ELK server allows users to easily monitor the vulnerable VMs for changes to the **_network_** and system **_files_.**

- *What does Filebeat watch for?* ***Filebeat watches the network for files and events, then forwards them.***
- *What does Metricbeat record?* ***Metricbeat collects metric data from the operating system running on the server.***

Name	Function	IP Address	OS
Jump Box	Gateway	20.36.168.192	Linux
Web1-Offsec	Server	10.1.0.5	Linux
Web1-Offsec	Server	10.1.0.6	Linux
Web1-Offsec	Server	10.1.0.7	Linux
Elk-1	Monitor	10.2.0.4	Linux

Access Policies

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

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

- ***67.191.197.137***

Machines within the network can only be accessed by **_SSH into the private IP_**.

- ***Jumpbox,* 10.1.0.5**

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

Name	Publicly Accessible	Allowed IP Addresses
Jump Box	Yes/No	**67.191.197.137 (My IP)**
Web 1	No	**20.36.198.162 (Jumpbox IP)**
Web 2	No	**20.36.198.162 (Jumpbox IP)**
Web 3	No	**20.36.198.162 (Jumpbox IP)**
Elk	Yes	**67.191.197.13**, **20.36.198.162 (My IP and Jumpbox IP)**

Elk Configuration

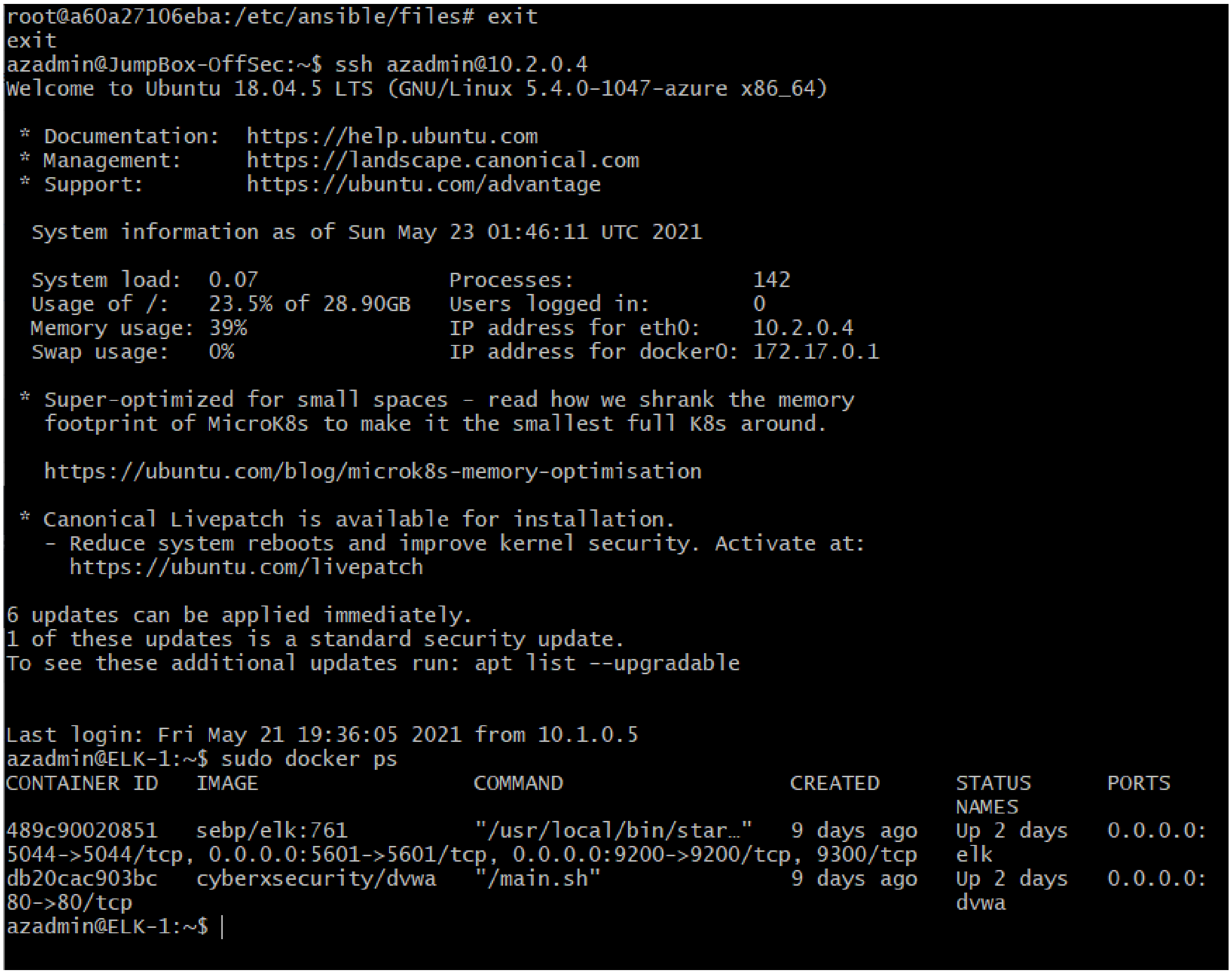
Ansible was used to automate configuration of the ELK machine. No configuration was performed manually, which is advantageous because...

- ***Automation with Ansible enables multiple machines to be set up in a uniform configuration which minimizes errors during deployment.***

The playbook implements the following tasks:

- **Made our Jumpbox only accessible via port 22.**
- **Created a Virtual Network.**
- **Added our Network Security Group (firewall)**
- **Created three new WebVMs, and set up using Ansible.**

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



```
root@a60a27106eba:/etc/ansible/files# exit
exit
azadmin@JumpBox-OffSec:~$ ssh azadmin@10.2.0.4
Welcome to Ubuntu 18.04.5 LTS (GNU/Linux 5.4.0-1047-azure x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

  System information as of Sun May 23 01:46:11 UTC 2021

  System load:  0.07               Processes:              142
  Usage of /:   23.5% of 28.90GB   Users logged in:        0
  Memory usage: 39%                IP address for eth0:    10.2.0.4
  Swap usage:   0%                 IP address for docker0: 172.17.0.1

 * Super-optimized for small spaces - read how we shrank the memory
   footprint of MicroK8s to make it the smallest full K8s around.

   https://ubuntu.com/blog/microk8s-memory-optimisation

 * Canonical Livepatch is available for installation.
   - Reduce system reboots and improve kernel security. Activate at:
     https://ubuntu.com/livepatch

6 updates can be applied immediately.
1 of these updates is a standard security update.
To see these additional updates run: apt list --upgradable


Last login: Fri May 21 19:36:05 2021 from 10.1.0.5
azadmin@ELK-1:~$ sudo docker ps
CONTAINER ID   IMAGE                 COMMAND                  CREATED      STATUS      PORTS
                                                                         NAMES
489c90020851   sebp/elk:761          "/usr/local/bin/star…"   9 days ago   Up 2 days   0.0.0.0:
5044->5044/tcp, 0.0.0.0:5601->5601/tcp, 0.0.0.0:9200->9200/tcp, 9300/tcp   elk
db20cac903bc   cyberxsecurity/dvwa   "/main.sh"               9 days ago   Up 2 days   0.0.0.0:
80->80/tcp                                                               dvwa
azadmin@ELK-1:~$ |
```

Target Machines & Beats

This ELK server is configured to monitor the following machines:

- **Web1-Offsec 10.1.0.5**
- **Web2-Offsec 10.1.0.6**
- **Web1-Offsec 10.1.0.7**

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 data about the log traffic on each webserver.**
- **Metricbeat collects data on the servers themselves, like OS, RAM, CPU etc.**

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-playbook.yml** and **metricbeat-playbook.yml_** files to **_/etc/ansible/roles_**.
- Update the **_ansible.cfg_** file to include...
- Run the playbook, and navigate to **_40.122.108.227:5601/app/kibana_** to check that the installation worked as expected.

TODO: Answer the following questions to fill in the blanks:

- *Which file is the playbook? Where do you copy it? -* ***filebeat-playbook.yml is the playbook, it must be copied into the filebeat directory to be run properly.***
- *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 /etc/ansible/hosts file must be updated to designate machines to run the playbook on. Servers are specified by IP in the webservers section of the playbook.***
- _Which URL do you navigate to in order to check that the ELK server is running? **-40.122.108.227:5601/app/kibana**