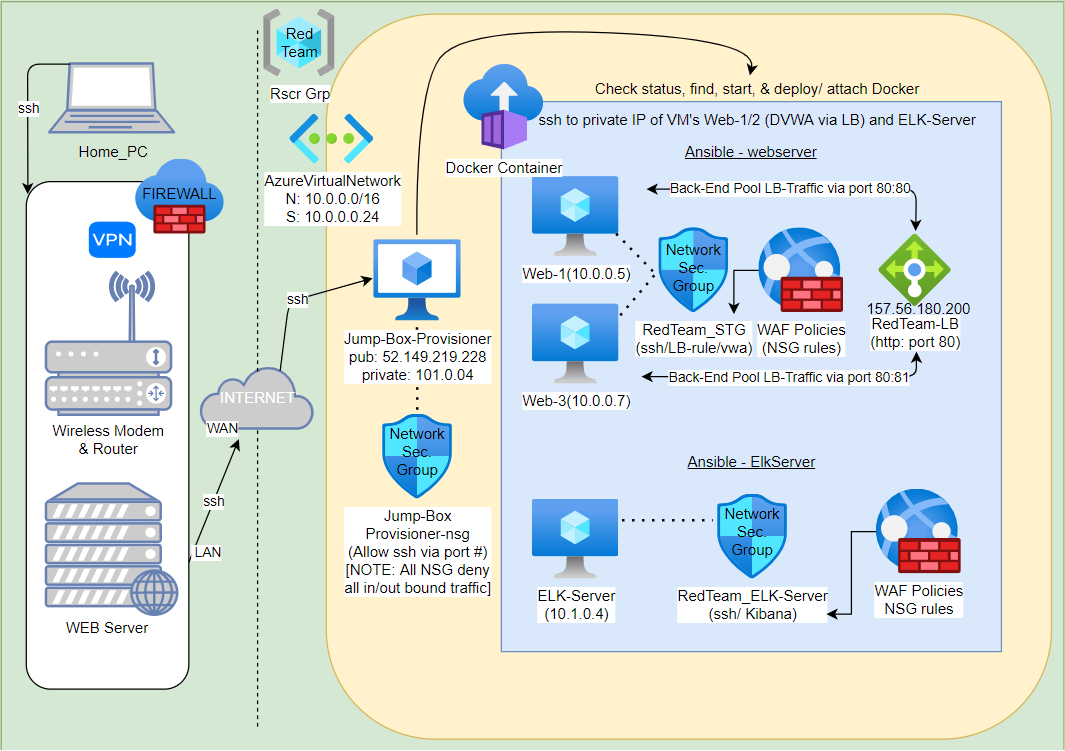
The files in this repository were used to configure the network depicted below.

[(NOTE: The Jump-Box private IP is actually 10.0.0.4)](Images/Azure%20Network%20Topology%20Diagram.png)



(NOTE: The most recent version of the above image is stored in the image folder)

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 (BEATS and/or YAML) file may be used to install only certain pieces of it, such as Filebeat.

* *TODO: Enter the playbook file.*

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

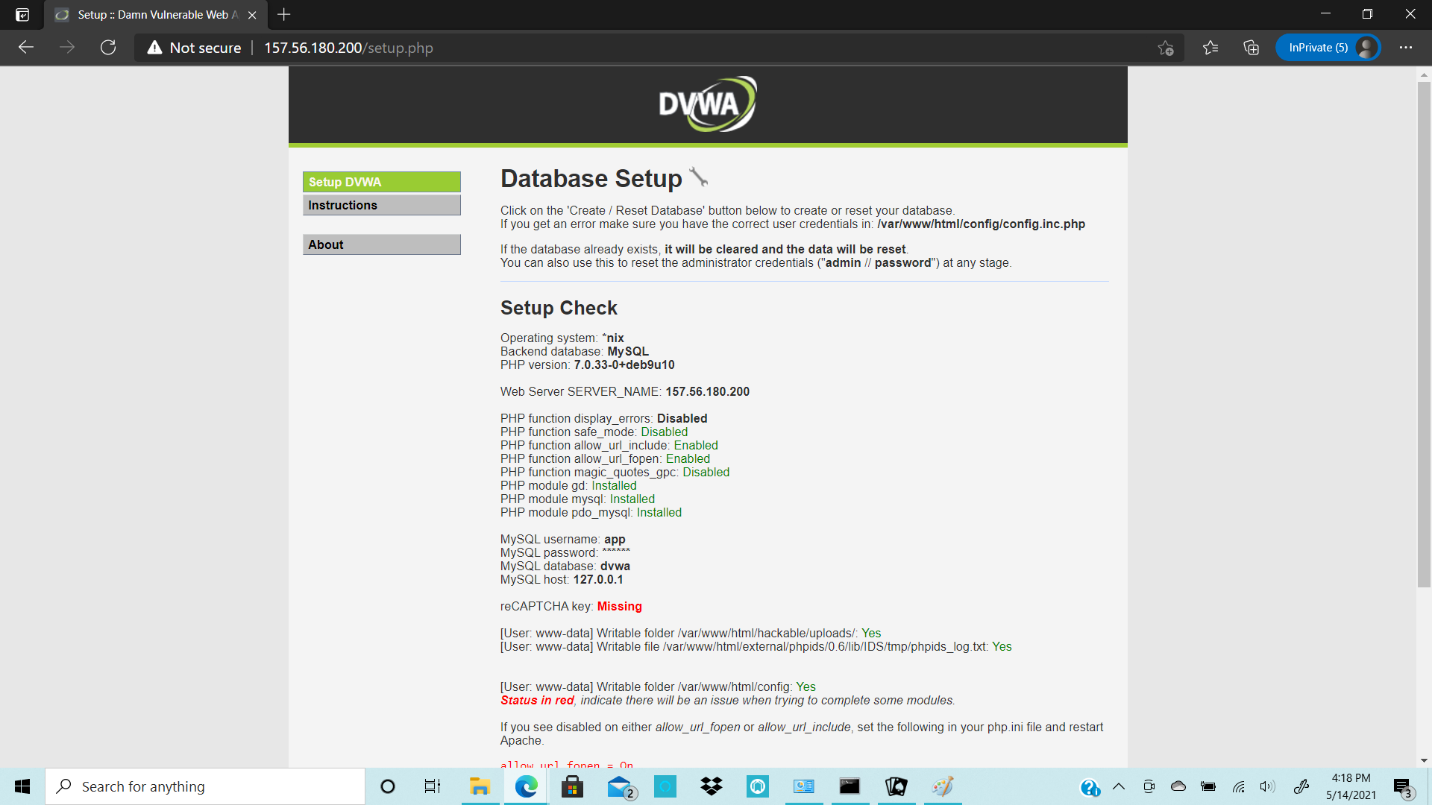
**Description of the Topology**

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 (Dynamic), in addition to restricting (Access) to the network.

* *What aspect of security do load balancers protect? What is the advantage of a jump box?*
  + Load Balancers protect your network from receiving “bad” network traffic. Bad network traffic may include malicious activities, such as: SQL Injections and Cross Site Scripting. Load Balancers can also help secure network traffic between two or more machines with it’s Back-End Pool, via its http port #.
  + To me, the primary advantage to having a Jump Box is accessibility. The Jump Box allow me to gain access to its network server and is the link between its network and mine. Because it’s the primary access point to the other machines on its network, any software programs and/or scripts can easily be pushed to other machines the network is attached to. Jump Boxes usually have an extra layer of security, protecting them from public access. And, the mitigation of resources may be considered as another benefit. That may include disabling what you don’t need; or, gaining peace of mind by providing automated backups

[Example of Load Balancer working:](Images/LB-Verify_Setup.png)



Integrating an ELK server allows users to easily monitor the vulnerable VMs for changes to the (Configuration) and system (Files).

* *What does Filebeat watch for?*
  + FileBeat watches for specified log data to be reviewed, at a future point. Logs are usually forwarded for this review to take place.
* *What does Metricbeat record?*
  + Like FileBeat, MetricBeat searches for and collects data. The difference is that MetricBeat collects metric data from the machines OS.

The configuration details of each machine may be found below. *Note: Use the* [*Markdown Table Generator*](http://www.tablesgenerator.com/markdown_tables) *to add/remove values from the table*.

| Machine Name | Function | IP Address | OS |

|:--------------------:|:--------:|:----------:|:-----:|

| Jump-Box-Provisioner | Gateway | 10.0.0.4 | Linux |

| Web-1 | Server | 10.0.0.5 | Linux |

| Web-2 | Server | 10.0.0.7 | Linux |

| ELK-Server | Server | 10.4.0.1 | 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:

* *Add whitelisted IP addresses*
  + 52.149.218.228

Machines within the network can only be accessed by (The Docker within the JumpBOX machine).

* *Which machine did you allow to access your ELK VM? What was its IP address?*
  + Machine Name: Jump-Box-Provisioner
  + Machine Private IP: 10.0.0.4
  + Note: The Gateway Machine is the only medium, within the network, that can gain remote access to the other three machines (Web-1, Web-2, ELK-Server)

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

| Machine Name | Publicly Accessible | Allowed IP Address | OS |

|:--------------------:|:-------------------:|:------------------:|:-----:|

| Jump-Box-Provisioner | Yes | 52.149.219.228 | Linux |

| Web-1 | No | 10.0.0.5 | Linux |

| Web-2 | No | 10.0.0.7 | Linux |

| ELK-Server | No | 10.4.0.1 | Linux |

**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?*
  + The Main advantage is that anything that is changed, or manipulated, can be easily pushed to other VM’s, via the use of the ansible playbooks. If they’re multiple machines that need to stay uniform, ansible is a good tool to implement standardization and consistency. Automation helps with mitigating time, and time management, by the use of prewritten tasks within the ansible playbook. An example would be the file/ metric beat YAML-configuration files. (Note: Ansible was used to configure and manipulate all VM’s within the docker)

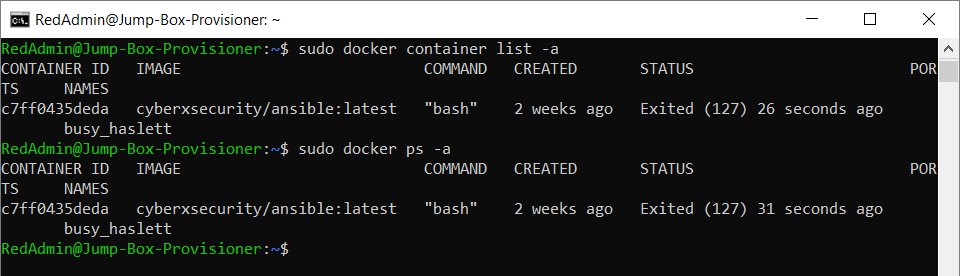
The playbook implements the following tasks:

* *In 3-5 bullets, explain the steps of the ELK installation play. E.g., install Docker; download image; etc.*
  + Install docker.io
  + Install python3-pip
  + Install Docker Module
  + Increase Virtual Memory for use
  + Download and Launch the Docker ELK container

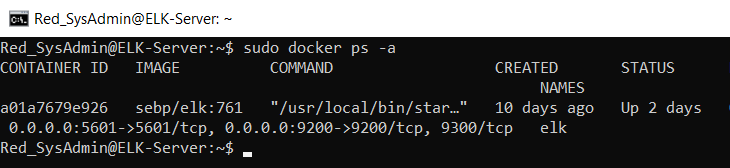
The following screenshots displays the result of running “ ps-a ” within the command line, the same result if ran within the ELK Server, and the return of successfully accessing the ELK Server instance (after successfully having it configured).

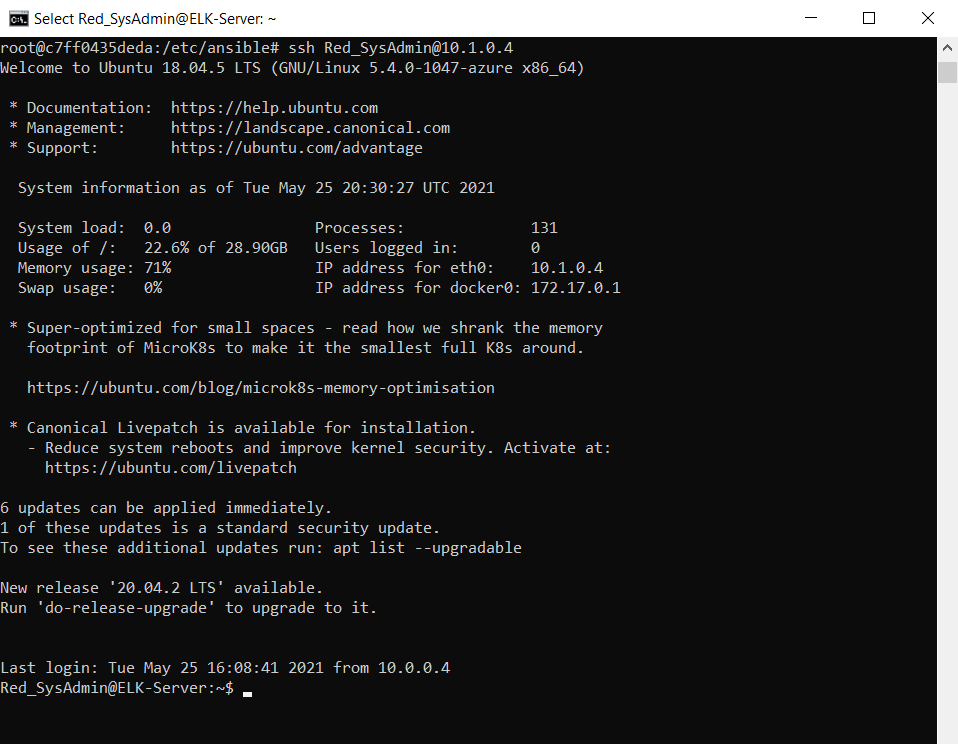
(NOTE: Images can be found in Images folder )

[PS-A\_output.png](Images/PS-A_output.png)



[ELK\_PS-A\_output.png](Images/ELK_PS-A_output.png)



[ELK-docker\_output.png](Images/ELK-docker_output.png)

**Target Machines & Beats**

This ELK server is configured to monitor the following machines:

* *List the IP addresses of the machines you are monitoring*
  + 10.0.0.5 & 10.0.0.7

We have installed the following Beats on these machines:

* *Specify which Beats you successfully installed*
  + I successfully installed filebeat-playbook.yml & metricbeat-playbook.yml

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

* *In 1-2 sentences, explain what kind of data each beat collects, and provide 1 example of what you expect to see. E.g., Winlogbeat collects Windows logs, which we use to track user logon events, etc.*
  + FileBeat: Sends syslogs and auditd logs to Kibana for monitoring
  + MetricBeat: A shipper that monitors performance, metric data and takes statistics before sending that info to predetermined destinations

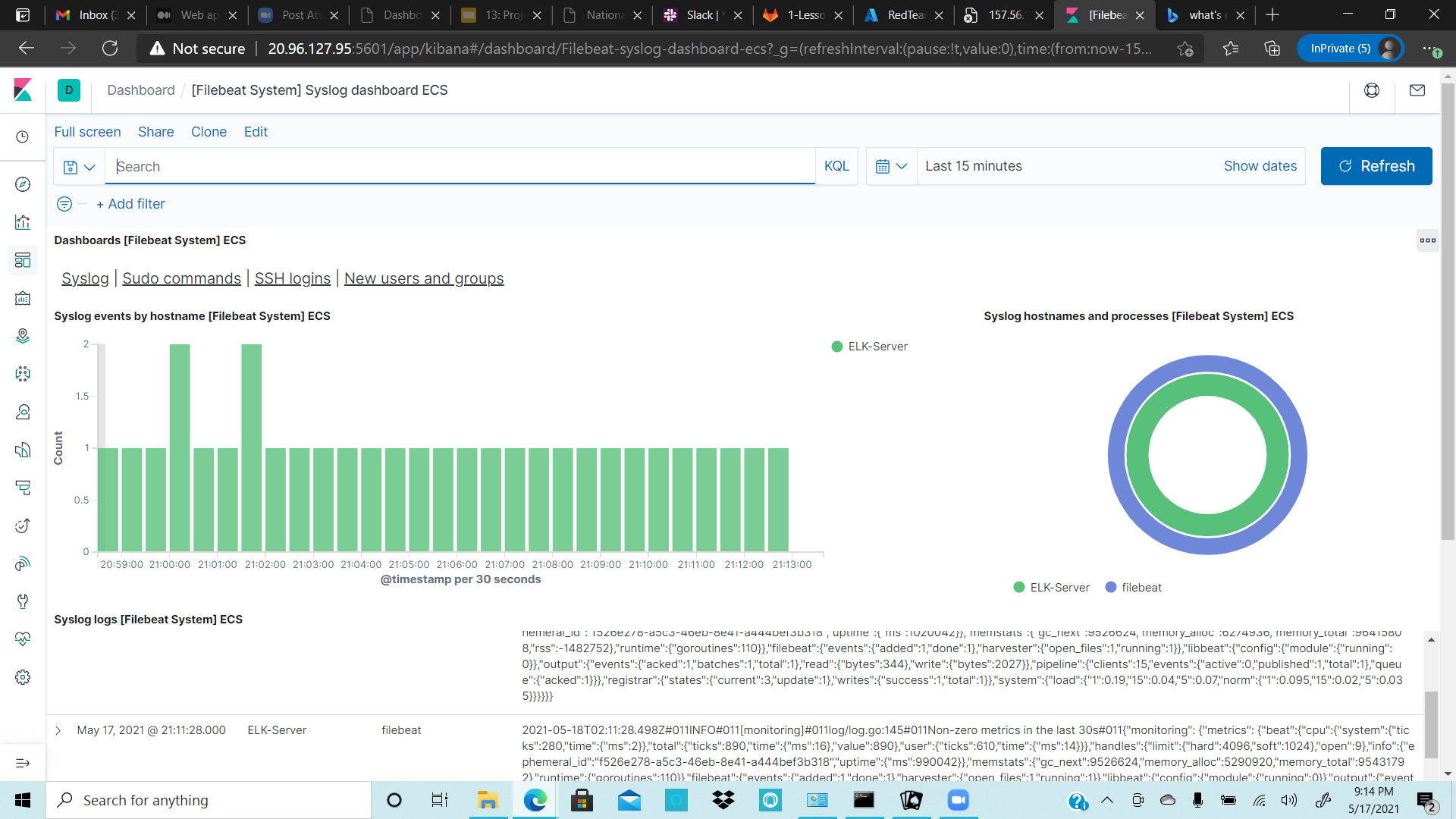
**Using the Playbook**

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 (/etc/ansible sub-directory).
* Update the (hosts) file to include (host IP under the correct webservers group).
* Run the playbook, and navigate to (Kibana) to check that the installation worked as expected.

[Example of Kibana working:](Images/filebeat_kirbana_VerifyIncomingData.png)



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

* *Which file is the playbook? Where do you copy it?*
  + The playbook is named: 05\_install-elk.yml
  + Once I ssh into the JumpBOX and attach to the docker (becoming root), Copy the YAML file to the “ /etc/ansible ” sub-directory.
* *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?*
  + Update the host private IP under the appropriate webserver group w/n the host file
  + You specify which playbook gets installed by first opening the playbook. Then, type in the appropriate webserver group name, on the host line. Lastly, edit the configuration file and type in the appropriate username being used to gain access
* Which URL do you navigate to in order to check that the ELK server is running?
  + URL: 20.96.127.95:5601/app/kibana

*As a* ***Bonus****, provide the specific commands the user will need to run to download the playbook, update the files, etc.*

* ansible-playbook <YAML\_File\_Name>.yml