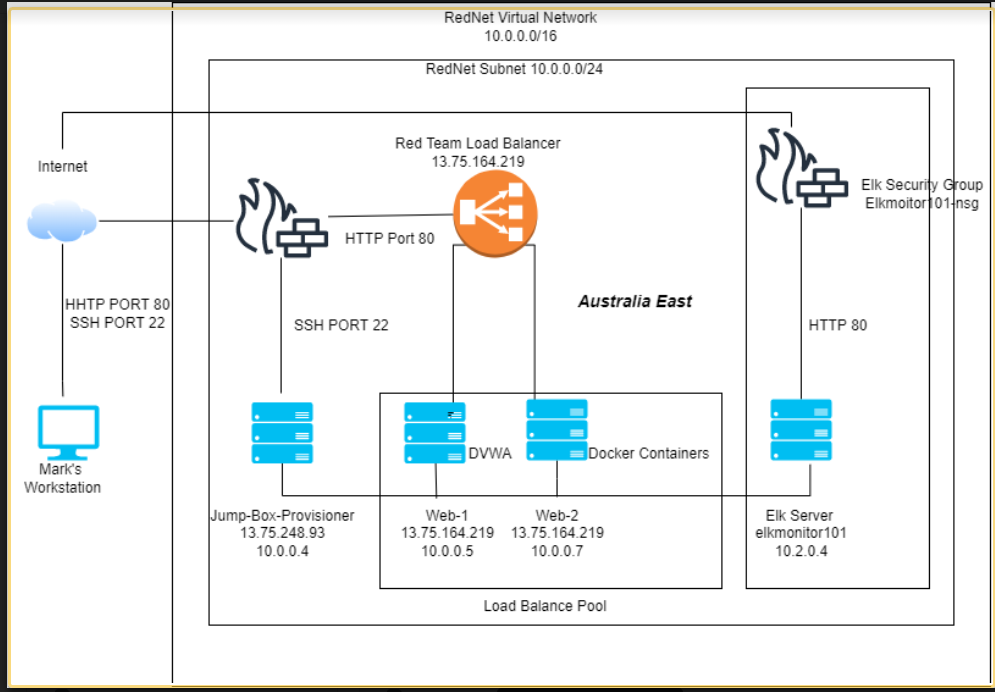
**Project 1 Explanation**

**ELK Stack Deployment**

****

The following files have been used to generate an ELK Stack Deployment. These files can be used to recreate the Network Diagram (shown in the Network Diagram above) or used to install specific portions of the network diagram.

* https://github.com/marklollis1/Mark\_Lollis\_Repo/blob/main/Ansible%20YAML/ansible.cfg.TXT
* https://github.com/marklollis1/Mark\_Lollis\_Repo/blob/main/Ansible%20YAML/ansibleinstall-elk.yml.TXT
* https://github.com/marklollis1/Mark\_Lollis\_Repo/blob/main/Ansible%20YAML/metricbeat-playbook.TXT
* https://github.com/marklollis1/Mark\_Lollis\_Repo/blob/main/Ansible%20YAML/filebeat-playbook.yml.TXT

**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 **available**, in addition to restricting **access** to the network.

What aspect of security do load balancers protect? **Load balancers protect systems from various cyber attacks**

What is the advantage of a jump box?

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

What does Filebeat watch for? **Data collection within the file system**

What does Metricbeat record? **The operational state of the computer machines**

The configuration details of each machine may be found below:

| **Name** | **Function** | **IP Address** | **Operating System** |
| --- | --- | --- | --- |
| JumpBox | Gateway | 10.0.0.4 | Ubuntu |
| Web 1 | Web Server | 10.0.0.5 | Ubuntu |
| Web 2 | Web Server | 10.0.0.7 | Ubuntu |

**Access Policies**

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

Only the **Jump Box Machine** can accept connections from the Internet. Access to this machine is only allowed from the following IP addresses: **SSH Port 22**.

Machines within this network can only be accessed by the **Jump Box Machine**

* Which machine did you allow to access your ELK VM? What was its address?
  + The Jump Box was allowed access to the **ELK VM. It’s address is 10.0.0.4**

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

| **Name** | **Publicly Accessible** | **Allowed IP Address** |
| --- | --- | --- |
| Jump Box | Yes | 10.0.0.4 |
| WEB 1 | No | 10.0.0.5 |
| WEB 2 | No | 10.0.0.7 |
| ELK | No | 10.2.0.4 |

**Elk Configuration**

Ansible was used to make the configuration on the ELK machine. No configuration was performed manually, which will decrease the chances of mistakes.

* https://github.com/marklollis1/Mark\_Lollis\_Repo/blob/main/Ansible%20YAML/ansible.yml.TXT
* https://github.com/marklollis1/Mark\_Lollis\_Repo/blob/main/Ansible%20YAML/ansibleinstall-elk.yml.TXT

What is the main advantage to automating configuration with ansible?

* Automating configuration with Ansible makes it very user friendly
* Automating configuration with Ansible means that users don’t need any specific trainings or coding skills to use the tool
* Automating configuration with Ansible is free which broadens it’s access to users

The playbook implements the following tasks:

* Install Docker and Python3-Pip
* Increases virtual memory
* Download ELK container

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

Docker PS

**Target Machines & Beats**

This ELK server is configured to monitor the following machines:

* Web-1: 10.0.0.5
* Web-2: 10.0.0.7

We have installed the **Filebeats** and **Metricbeats** on these machines

* Filebeats monitor log files and collect data on specific events
  + Citation: ([Filebeat overview | Filebeat Reference [8.3] | Elastic](https://www.elastic.co/guide/en/beats/filebeat/current/filebeat-overview.html#:~:text=Filebeat%20overviewedit,Elasticsearch%20or%20Logstash%20for%20indexing.))
* Metricbeats collect data from the operating system and then ships that data to specific outputs
  + Citation: ([Metricbeat overview | Metricbeat Reference [8.3] | Elastic](https://www.elastic.co/guide/en/beats/metricbeat/current/metricbeat-overview.html))

**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 **ansible**.
* Update the configuration file to include the **appropriate IP address**
* Run the playbook, and navigate to **\_\_\_\_\_\_** to check that the installation worked as expected.