## ELK Stack Deployment

- The ansible-playbooks elk.yml and the filebeat-playbook.yml are needed to create and implement the Elk-Server.

- The main purpose of this network is to expose a load-balanced and monitored instance of DVWA

-Load Balancing contributes to the Availability aspect of security in regards to the CIA Triad.

-JumpBox is the orgination point for launching Administrative Tasks.

-Integrating an ELK server allows users to easily monitor the vulnerable VMs for changes

- Filebeat watches for log files/locations and collects log events.

- Metricbeat records metric and statistical data from the operating system and from services running on the server.

| Name | Publicly Accessible | IP Addresses

|---------- |---------------------|----------------------

| Jump Box | No | 10.0.0.4

| Web 2 | No | 10.0.0.7

| ELk-Server | No | 10.0.0.8

- Ansible was used to automate configuration of the ELK machine.

- The playbook implements the following tasks:

* Create a New VM
* Download and Configure the "elk-docker" container "
* Launch and expose the container
* Create new Inbound Security Rules to allow Ports: 5601 and 9200