## Automated ELK Stack Deployment

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

<https://github.com/Jersey007/Cybersecurity/tree/master/Diagrams>

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

https://github.com/Jersey007/Cybersecurity/blob/master/Ansible/filebeat-playbook.yml

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 secure, in addition to restricting traffic to the network.

Load Balancing plays an important security role as computing moves evermore to the cloud. The off-loading function of a load balancer defends an organization against distributed denial-of-service (DDoS) attacks. It does this by shifting attack traffic from the corporate server to a public cloud provider. A jump box is a secure computer that all admins first connect to before launching any administrative task or use as an origination point to connect to other servers or untrusted environments.

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

- \_TODO: 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.

- \_TODO: What does Metricbeat record?\_ It takes the metrics and stats and ships them to the output I specify such as uptime.

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\_.

| Name | Function | IP Address | Operating System |

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

| Jump Box | Gateway | 40. 88.143.96 or 10.2.0.4| Linux |

| Elk | database | 104.42.193.247 | Linux |

| Web-1 | servlit | 40.87.104.204 or 10.2.0.5 | Linux |

|Web-2 | servlet | 10.2.0.6 | 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: 40.88.143.96 (dynamic)

- \_TODO: Add whitelisted IP addresses\_

Machines within the network can only be accessed by Jumpbox.

- \_TODO: Which machine did you allow to access your ELK VM? Web-1 What was is address?\_40.87.104.204

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

| Name | Publicly Accessible | Allowed IP Addresses |

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

| Jump Box | Yes | 40. 88.143.96 or 10.2.0.4 |

| Elk | No |104.42.193.247 or 10.1.0.4 |

| Web-1 | No | 40.87.104.204 or 10.2.0.5 |

### Elk Configuration

Ansible was used to automate the configuration of the ELK machine. No configuration was performed manually, which is advantageous because...it gives the ability to use a single tool.

The playbook implements the following tasks:

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

.Install docker.io--allows you to run linux containers

Install pip3-

Install Docker python module

Download and launch a docker elk container

- ...

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

### Target Machines & Beats

This ELK server is configured to monitor the following machines:

- \_TODO: List the IP addresses of the machines you are monitoring\_

*10.2.0.4 10.2.0.5 10.2.0.6*

We have installed the following Beats on these machines:

- \_TODO: Specify which Beats you successfully installed\_

*Filebeat*

*Metricbeat*

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

- \_TODO: 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-collects data about the file system...it collects the last successful line indexed in a registry and will remember where it left off.*

*Metricbeat-collects machine metrics, such as uptime.*

### 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 *public key* file to your *server*.

- Update the \_\_\_\_\_ file to include...

- Run the playbook, and navigate to *Elk* 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...and you copy it to the Ansible container.*

- \_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? *ansible-playbook filebeat-playbook.yml ...you enter the private address in the yml file.*

- \_Which URL do you navigate to in order to check that the ELK server is running? *Elk public Ip:5601/app/kibana*

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

*Sudo docker start...then container name*

*Sudo docker attach...then container name*

*ansible all -i vyos.example.net, -c network\_cli -u my\_vyos\_user -k -m vyos\_facts -e ansible\_network\_os=vyos*