## Automated ELK Stack Deployment

The files in the repository “Bashiri\_Scripts\_and\_Diagrams” were used to configure the network depicted below.

![TODO: Update the path with the name of your diagram](Images/diagram\_filename.png)

<https://drive.google.com/file/d/1P_fIaT8sBg5-BoR0P7jEUrXiGzBhLtZX/view?usp=sharing>

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

- \_TODO: Enter the playbook file.\_

<https://drive.google.com/file/d/1R-bVLKp_6l-hE3LMIUZUPbEMewjl6kc4/view?usp=sharing>

This document contains the following details:

- Description of the Topology

- Access Policies

- ELK Configuration

- Beats in Use

- Machines Being Monitored

### 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 \_\_\_Available\_\_, in addition to restricting \_\_\_Access\_\_ to the network.

- \_TODO: What aspect of security do load balancers protect?

Availability

What is the advantage of a jump box?\_

The jump box enables you to admin the web servers, while the web servers are in a different security domain from the rest of the network.

Integrating an ELK server allows users to easily monitor the vulnerable VMs for changes to the \_\_Application\_\_\_ and system \_\_configuration\_\_\_.

- \_TODO: What does Filebeat watch for?\_

Filebeat watches the log files and forwards log events to Elasticsearch or Logstash for indexing.

- \_TODO: What does Metricbeat record?\_

Metricbeat collects metrics about the OS and services running on the system, then forwards them to Logstash or Elasticsearch or another indexing software.

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 | 10.0.0.4 | Linux |

| WEB1 | DVWA | 10.0.0.5 | Linux |

| WEB2 | DVWA | 10.0.0.6 | Linux |

| Web3 | DVWA | 10.0.0.7 | Linux |

| ELK | Monitoring | 10.1.0.4 | Linux |

### 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: 94.140.9.43 (My personal VPN IP is dynamic and it changes every boot)

- \_TODO: Add whitelisted IP addresses\_

Machines within the network can only be accessed by \_\_The Jump Box\_\_\_.

- \_TODO: Which machine did you allow to access your ELK VM? What was its IP address?\_ The jump box is the only machine that can access the ELK server. 10.0.0.4

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

| Name | Publicly Accessible | Allowed IP Addresses |

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

| Jump Box SSH | Yes | 94.140.9.4 |

| Jump Box Internal network | No | 10.0.0.4 |

| HTTP From Home | Yes | 94.140.9.4 |

### Elk Configuration

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

- \_TODO: What is the main advantage of automating configuration with Ansible?\_

The ELK machine can be easily replaced if it has any issues, or a duplicate can be easily deployed if additional ones are needed on new servers.

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 - Downloads the docker to the system

- Install Python3 - Python2 is the default with the VM, so Python3 is needed for continued support.

- Install Docker module - Installs the docker containing ELK

- Increase virtual memory - Increases the amount of memory allocated to the docker due to the memory requirements of the module

- Enable Docker on boot - gets the docker to start as soon as the VM boots up.

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

![TODO: Update the path with the name of your screenshot of docker ps output]

<https://drive.google.com/file/d/1UYcCmJ_h3-iclyhvMLJ78kTe3M4W0-A8/view?usp=sharing>

### Target Machines & Beats

This ELK server is configured to monitor the following machines:

- \_TODO: List the IP addresses of the machines you are monitoring\_ 10.0.0.5, 10.0.0.6, 10.0.0.7

We have installed the following Beats on these machines:

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

Filebeat was successfully installed and tested.

I ran the .yml file to setup metricbeat, even worked it with my tutor, but we could not get it completely functioning.

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 log data from the system it is installed on and sends the log data to an indexing software like logstash or elasticsearch so the data is ready for the security users.

### 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 \_\_config\_\_\_ file to \_\_/etc/ansible/file/\_\_\_.

- Update the \_\_hosts\_\_\_ file to include... The server IPs for each system type

- Run the playbook, and navigate to \_\_The Kibana UI and check for data for the specific beat type that is feeding data to Kibana\_\_ to check that the installation worked as expected.

\_TODO: Answer the following questions to fill in the blanks:\_

Q. Which file is the playbook? Where do you copy it?\_

A. The playbook is the .yml file. This stays in the ansible container.

Q. 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?\_

A. The config file gets updated with system types - i.e. Webserver or ELK with the IPs of all of the systems of that type, then the playbook calls out the system type, and the commands will be run against all IPs in the config file for that system type.

Q. Which URL do you navigate to in order to check that the ELK server is running?

A. The http://<public IP of the ELK server>:5601/apps/kibana