## Automated ELK Stack Deployment

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

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

\README\Images\Project\_1\_Diagram.png

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.\_

\README\Images\Day\_2\filebeat.png

\README\Images\Day\_2\metricbeat.png

This document contains the following details:

- Description of the Topology

- 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 \*{ EFFICIENT AND RESPONSIVE TO USERS }\*, in addition to restricting \*{ UNWANTED ACCESS }\* to the network.

- \_TODO:

-What aspect of security do load balancers protect?

--- \*{ THEY PROTECT SERVERS FROM GETTING OVERLOADED AND THE POSSIBILITY OF THEM BREAKING DOWN. OVERALL, LOAD BALANCERS HELP WITH IMPROVING SERVICE AVAILABILITY AND PREVENTING DOWNTIME. }\*

-What is the advantage of a jump box?\_

--- \*{ JUMP BOX PREVENTS OUR VMs FROM BEING EXPOSED TO THE PUBLIC BY BEING THE POINT OF ENTRY VIA REMOTE DESKTOP PROTOCOL. }\*

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 WATCHES FOR LOG FILES AND/OR LOCATIONS THAT THE USER SPECIFIES. FILEBEAT COLLECTS LOG EVENT AND FORWARDS THEM TO TOOLS IN KIBANA TO VIEW. }\*

- \_TODO: What does Metricbeat record?\_

--- \*{ METRICBEAT RECORDS AND COLLECTS METRICS FROM THE OS AND SERVICES RUNNING ON THE SERVER. IT TAKES THOSE METRICS AND STATS AND FORWARDS IT TO THE PLACE THAT THE USER SPECIFIES. WE USE TOOLS IN KIBANA FOR THIS. }\*

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 |

| WEB-1 | SERVER | 10.0.0.5 | Linux |

| WEB-2 | SERVER | 10.0.0.6 | Linux |

| ELK-VM |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:

- \_TODO: Add whitelisted IP addresses\_

--- \*{ 5601, KIBANA PORT }\*

Machines within the network can only be accessed by JUMP-BOX.

- \_TODO:

- Which machine did you allow to access your ELK VM?

--- \*{ JUMP-BOX }\*

- What was its IP address?\_

--- \*{ 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 | Yes | 40.83.11.21 |

| Web-1 | NO | 10.0.0.4 |

| Web-2 | NO | 10.0.0.4 |

### 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?\_

--- \*{ ANSIBLE IS AN OPEN SOURCE TOOL, SO IT'S FREE. NOTHING BETTER THAN THAT! }\*

--- \*{ IT IS VERY SIMPLE TO SET UP AND A POWERFUL TOOL. }\*

--- \*{ ANSIBLE DOES NOT REQUIRE A MASTER CLIENT MODEL. }\*

--- \*{ ANSIBLE USES SIMPLE SYNTAX WRITTEN IN YAML. }\*

--- \*{ ANSIBLE PROVIDES A GUI PLATFORM CALLED THE ANSIBLE TOWER. }\*

--- \*{ IT CAN MANAGE THE INFRASTRUCTURE, NETWORKS, OPERATING SYSTEMS, AND SERVICES THAT YOU ARE ALREADY USING. }\*

--- \*{ NO EXTRA SOFTWARE ON YOUR SERVERS ARE NEEDED, THEREFORE YOU HAVE MORE RESOURCES. }\*

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 }\*

--- \*{ INSTALL PIP3 }\*

--- \*{ INSTALL DOCKER PYTHON MODULE }\*

--- \*{ INCREASE VIRTUAL MEMORY }\*

--- \*{ DOWNLOAD AND LAUNCH DOCKER }\*

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](Images/docker\_ps\_output.png)

\README\Images \Day\_1\sebp\_elk\_761.png

### Target Machines & Beats

This ELK server is configured to monitor the following machines:

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

--- \*{ WEB-1 : 10.0.0.5 }\*

--- \*{ WEB-2 : 10.0.0.6 }\*

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 FILES ON THE SYSTEM AND THEIR LOG EVENTS. IT SENDS THEM TO KIBANA FOR MONITORING AND ANALYZING. }\*

--- \*{ METRICBEAT: COLLECTS METRICS AND STATS AND SENDS THEM TO A SPECIFIED OUTPUT, LIKE KIBANA TOOLS. }\*

### 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 \*{PLAYBOOK }\* file to \*{ ANSIBLE }\*.

- Update the \*{ HOST }\* file to include \*{ ELK AND WEBSERVERS }\*

- Run the playbook, and navigate to \*{ KIBANA }\* to check that the installation worked as expected.

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

- \_Which file is the playbook?

--- \*{ INSTALL-ELK.YML }\*

- Where do you copy it?\_

--- \*{ /ETC/ANSIBLE }\*

- \_Which file do you update to make Ansible run the playbook on a specific machine?

--- \*{ ANSIBLE.CFG or HOSTS }\* \*\*\*\*\*\*\*\*\*\* ASK ABOUT THIS ONE \*\*\*\*\*\*\*\*\*\*

- How do I specify which machine to install the ELK server on versus which to install Filebeat on?\_

--- \*{ \*\*\*\*\*\*\*\*\*\* ASK ABOUT THIS ONE \*\*\*\*\*\*\*\*\*\*

- \_Which URL do you navigate to in order to check that the ELK server is running?

--- \*{ HTTP://ELK\_MACHINE\_IP:5601 }\*

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