## 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)

<https://drive.google.com/drive/folders/1Jyd-bcuN7izcI5ysrDAI5sH2CHJtpiz2?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.\_

**pentest.yml(dvwa-vm1 & dvwa-vm2) installing docker on both dvwa-vm**

**install-playbook.yml**

**filebeat-playbook.yml**

**metricbeat-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 \_\_**availability**\_\_\_, in addition to restricting \_\_**traffic**\_\_\_ to the network.

- \_TODO: What aspect of security do load balancers protect? What is the advantage of a jump box?\_

**load balancer protect: eliminate single point failure and reduce attack surface.**

**advantage of jump box: prevent all the vms inside the container to expose to public**

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

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

**Filebeat: watch for log files and log events**

- \_TODO: What does Metricbeat record?\_

**Metricbeat: monitor servers by collecting metrics from the system and services running on the server**

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 | 10.0.0.1 | Linux |**

**| Elk VM | monitor | 10.0.0.11 | Ubuntu |**

**| DVWA-VM1 | docker host vm | 10.0.0.8 | Ubuntu |**

**| DVWA-VM2 | docker host vm | 10.0.0.9 | Ubuntu |**

### 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:

- \_TODO: Add whitelisted IP addresses\_

**Elk Vm : 10.0.0.11**

**dvwa-vm1 : 10.0.0.8**

**dvwa-vm2 : 10.0.0.9**

Machines within the network can only be accessed by \_ElK VM\_ **jumbox**.

- \_TODO: Which machine did you allow to access your ELK VM? What was its IP address?\_

**jumpbox 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/No -- No | 10.0.0.1 10.0.0.2 |**

**| | correct one | 10.0.0.0/24(IP Range)|**

**| | | |**

### 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?\_

**playbooks are written in YAML code because YAML is a better alternative for configuration management and automation.**

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.\_

**write ELK installation playbook yaml code**

**- use apt to install docker.io**

**- use apt to install python-pip**

**- use pip to install docker python module**

**- use command to increase virutal memory**

**- use docker container to download and lauch a docker elk conainter**

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)

**I can’t log back in to the Azure personal account virtual machine because the Azure subscription was disable. I don’t know what happen. I also mentioned this problem to Branden. That’s the reason why I can’t take my screenshot.**

### Target Machines & Beats

This ELK server is configured to monitor the following machines:

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

**dvwa-vm1: 10.0.0.8 & dvwa-vm2: 10.0.0.9**

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: filebeat look in the locations that specified for log data, for each log that filebeat locates, filebeat starts a harvester which reads a single log for new content and sends the new log data to libbeat, which aggregates the events and sends the aggregated data to output. for example, systemlog, wifi.log.**

**metricbeat: metricbat defines the basic logic for collecting data from a specific service, such as MySQL, Apache, Redis.**

### 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 \_\_**YAML**\_\_\_ file to \_**directory**\_\_\_\_.

- Update the \_**hosts & ansible.cfg**\_\_ file to include **webserver updating, adding remote\_user**

- Run the **playbook**, and navigate to \_**vm**\_\_ 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?\_

**pentest.yml, install-playbook.yml, filebeat-playbook.yml & metricbeat-playbook.yml**

**all the yml instruction provide by the instruction team in the resouces directory on the day 2 activities.**

- \_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?\_

**hosts file & ansible.cfg /etc/ansible in the ansible.**

**modify hosts file to add the elkserver section for specifying elk vm ip and on yaml file of elk machine which specify the webserver(which includes two vms ip ) to install the docker host on both vms for open connection to install filebeat.**

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

**elk machine public ip: port #**

**132.12.167.1:5601**

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

**command: ansible-playbook \*.yml**