**Automated ELK Stack Deployment**

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

Update the path with the name of your diagram](Images/diagram\_filename.png) **https://drive.google.com/drive/my-drive**

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

- Enter the playbook file.**install-elk.yml**

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**, in addition to restricting **unauthorized traffic** to the network.

What aspect of security do load balancers protect? What is the advantage of a jump box?

**Load balancer protects the server from being overloaded and protects against Distributed Denial of Service (DDoS) attacks.**

**JumpBox provides the advantage of enhanced security and enables greater control over sensitive files and information.**

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

What does Filebeat watch for?

**Filebeat watches for any information that has been changed and when the change occurred.**

What does Metricbeat record?

**Metricbeat monitors at a less granular level, analyzing log data at a specific moment in time.**

|  |
| --- |
| Name | Function | IP Address | Operating System |
| Jump Box | Gateway | 10.0.0.4 | Linux |
| **Web1** | **Server** 10.0.0.5 **Linux** |
| **Web2** | **Server 10.0.0.6 Linux** |
| **elkVM** | **Server 10.1.0.4 Linux** |

**Access Policies**

The machines on the internal network are not exposed to the public Internet.

Only the **JumpBoxProvisioner** machine can accept connections from the Internet. Access to this machine is only allowed from the following IP addresses:

**20.124.240.121**

Machines within the network can only be accessed by **JumpBoxProvisioner** **10.0.0.4.**

Which machine did you allow to access your ELK VM? What was its IP address?

**136.57.177.79 via port 5601.**

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

|  |
| --- |
| Name | Publicly Accessible | Allowed IP Addresses |
| Jump Box| Yes | 10.0.0.4 |
| Web1 | No | 10.0.0.5 |
| Web2 | No | 10.0.0.6 |
| elkVM | Yes | 10.1.0.4, 136.57.177.79 |
|  |

**Elk Configuration**

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

What is the main advantage of automating configuration with Ansible?

**The same configuration can be programmed and automated and deployed across multiple machines.**

The playbook implements the following tasks:

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

* **Installed docker and ansible on the Jumpboxprovisioner.**
* **ELKVM was added to host file under elk group header.**
* **Run playbook file via ansible-playbook command.**

The following screenshot displays the result of running `docker ps after successfully configuring the ELK instance. Graphical user interface, text, application

Description automatically generated

Update the path with the name of your screenshot of docker ps output](Images/docker\_ps\_output.png) **C:\Users\eloch\Documents\OneDrive\Pictures**

**Target Machines & Beats**

This ELK server is configured to monitor the following machines:

**Web1(10.0.0.5) and Web2(10.0.0.6)**

We have installed the following Beats on these machines:

**Filebeat**

**Metricbeat**

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

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 allows the ELK Server to monitor files that are accessed, either by authorized or unauthorized users. It keeps track of access, so changes are made to sensitive files, the user can figure out when the event took place. If a user altered or accessed the shadow or passwd files, this allows valuable intelligence into the time and how it was done.**

**Metricbeat allows the ELK Server to monitor valuable usage metrics like CPU usage, memory usage, and monitors what is coming in and out of the server at specific moment. This allows for a user to further configure or change assets when there may be high traffic volume or usage volume.**

**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 **/etc/ansible.**

- Update the **host** file to include the **webservers and elkVM**

- Run the playbook and navigate to **vm** to check that the installation worked as expected.

Answer the following questions to fill in the blanks:

Which file is the playbook?

**.yml are playbook files.**

Where do you copy it?

**It is copied into a container.**

Which file do you update to make Ansible run the playbook on a specific machine? **The Hosts file.**

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

**Filebeat is installed on the web servers that are accepting traffic which sends that data to the ELK server.**

Which URL do you navigate to in order to check that the ELK server is running? **http://20.69.94.191:5601/app/kibana**

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