ELK- STACK-PROJECT-1

Class Project-1, ELK Stack Deployment Automated ELK Stack Deployment.

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

Diagram

Description automatically generated

`

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

etc/ansible/install-elk-playbook.yml

This document contains the following details:

#Description of the Topology

# Access Policies

#ELK Configuration

\*Beat in Use

\*Machines being monitored

#How to use the Ansible Build

ui

Description of the Topology

The main purpose of this network is to expose a load- balanced and monitored instance of DVWA, the Damn Vulnerable Web Application.

Load balancing ensures that the application will be highly efficient, in addition to restricting traffic to the network.

# What aspect of security do load balancers protect?

* Load balancers protect the system from DDoS attacks by shifting attach traffic.
* Load Balancing contributes to the availability aspect of security in regards to the CIA Triad.

What is the advantage of a Jump Box?

* The advantage of a Jump Box is to give access to the user from a single node that can be secured and monitored.
* The advantage of a JumpBox is the origination point for launching Administrative Tasks. This ultimately sets the JumpBox as a SAW (Secure Admin Workstation). All Administrators when conducting any Administrative Tasks will be required to connect to the JumpBox (SAW) before performing any task/assignment.

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

#What does FileBeat watch for?

\*FileBeat watches for any information in the file system which has been changed and when it has.

\* FileBeat watches for log files/locations and collects log events.

#What does Metricbeat record?

* Metricbeat takes the metrics and statistics that collects and ship them to the output you specify.
* Metricbeat records metric and statistical data from the operating system and from services running on the server.

The configuration details of each machine may be found below:

|  |  |  |  |
| --- | --- | --- | --- |
| NAME | FUNCTION | IP ADDRESS | OPERATING SYSTEM |
| JumpBox | Gateway | Private IP:10.0.0.8 public:20.124.251.210 | LINUX |
| Web-1 | Server | Private IP:10.0.0.5 | LINUX |
| Web-2 | Server | Private IP:10.0.0.7 | LINUX |
| ELK-VM1137.135.115.14 | ELK Server | 10.1.0.4 public:13.64.231.134 | 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: .5601 Kibana port

#Add whitelisted IP addresses:-- Public IP address which changes everytime when the VM is on/off eg of Public IP 13.64.231.134

Machines within the network can only be accessed by SSH.

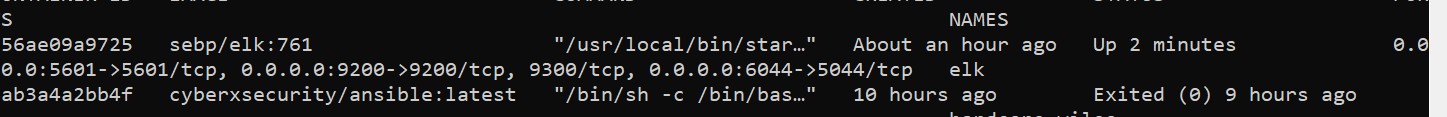
#Which machine did you allow to access your ELK VM? What was its IP address ?

Jumpbox VM, its private IP address (Vnet IP)-10.0.0.8 IP)

A SUMMARY OF THE ACCESS POLICIES IN PLACE CAN BE FOUND BELOW:

|  |  |  |
| --- | --- | --- |
| NAME | PUBLICLY ACCESSIBLE | ALLOWED IP ADDRESSES |
| JUMP BOX | YES/NO | MY PERSONAL IP ADDRESS:76.171.11.33 |
| WEB-1 | NO | 10.0.0.5 |
| WEB-2 | NO | 10.0.0.7 |
| ELK=SERVER | NO | 10.1.0.4 |

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



Target Machines & Beats.

This ELK server is configured to monitor the following machines:

# List the IP addresses of the machines you are monitoring:--Web-1(10.0.0.5) and Web-3(10.0.0.7)

We have installed the following Beats on these machines :

# Specify which Beats you successfully installed: --FileBeat and Metricbeat

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

|  |
| --- |
| *Filebeat monitors log files or locations you specify, collects log events and forwards them either to Elastic search or logstash for indexing.*  *Metricbeat collects metrics from the operating system and from services running on the server.* |

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?

\*This allows you to deploy to multiple servers using a single playbook.

The playbook implements the following tasks:

\*Install docker.io

\*Install Python3-pip

\*Install docker via pip

\*Launch docker container: elk

\*Command: sysctl –wvm.max\_map\_count=262144[webservers] (Increases virtual memory) [10.0.0.5]ansible\_python\_interpreter=/usr/bin/python3 [10.0.0.7]ansible\_python\_interpreter=/usr/bin/python3[10.1.0.11]ansible\_python\_interpreter=/usr/bin/python3

Run the playbook and SSH into the ELK VM, then run docker ps to check that the installation worked as expected. Playbook:install\_elk,yml Location:/etc/ansible/install\_elk.yml Navigate to <http://[your.ELK-VM.Externl.IP]:5601/app/kibana> to confirm ELK and kibana are running. You may need to try from multiple web browsers. Click ‘Explore On Your Own’ and you should see the following:

Answer the following question to fill in the blanks:

#Which file is the

*Operating system and from services running on the server*

Using the Playbook –install-elk.yml

*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 configuration file to include the webservers and ElkVM (Private IP address.

\*Run the playbook and navigate to ElkVM to check that the installation worked as expected. /etc/ansible/host should include

\* Create a new playbook in the /etc/ansible/roles/directory that will install, drop in the updated configuration file, enable and configure system module, run the filebeat setup, and start the Filebeat

service.

Graphical user interface, text, application, email

Description automatically generatedA picture containing text

Description automatically generated

\*Create a new playbook in the /etc/ansible/roles/directory that will install, drop in the updated configuration file, enable, and configure system module, run the metric setup and start the metric service.

\* Run the playbooks, and navigate back to the installation page on the ELK-Server GUI, click the check data on the module Status

\*Click the verify incoming Data to check and see the receiving logs from the DVWA machines.

You should see the following:

Playbook? Where do you copy it? /etc/ansible/file/filebeat-configuration.yml

\*Which file do you update to make Ansible run the playbook on a specific machine? How do I specify which machine iunstall the ElK server on versus which to unstall filebeat on?\_edit the/etc/ansible/hosts file to add webserver/elkserver IP addresses.

\*Which URL do you navigate to in order to check that the ELK server is running? <http://[your.ELK-VM.External.IP]:5601/app/kibana>

Using the Playbook-filebeat-playbook.yml

\*Copy the filebeat.yml file to the /etc/ansible/files/directory.

\*Update the configuration file to include the Private IP of the ELK-Server to the ElasticSearch and Kibana sections of the configuration file.

*The commands needed to run the Ansible configuration for the ELK server are:*

*-ssh azadmin@JumpBox (Public IP)*

*-sudo docker containerlist –a(locate your ansible container)*

*-sudo docker attach container (name of the container)*

Cd /etc/ansible/-ansible-playbook elk.yml (configures Elk-Server and starts the ELK container on the ELK-Server) wait a couple minutes for the implementation of the ELK- Server –cd /etc/ansible/roles/ -ansible-playbook.yml (installs Filebeat and Metricbeat) –open a new web browser (<http://[your.ELK-VM.external.IP]:5601/app/kibana>) This will bring up the Kibana Web Portal –check the Module status for File beat and metric beat to see their data receiving.

\*\* You will need to ensure all files are properly placed before running the ansible-playbooks.

Graphical user interface, application

Description automatically generated

*Graphical user interface

Description automatically generated*