**Deepak Shenoy – Read Me File**

## 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](Diagram/Elk-Project-Diagram-Final.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 \_\_\_\_\_ file may be used to install only certain pieces of it, such as Filebeat.

- \_TODO: Enter the playbook file.

---

- name: Config elk VM with Docker

hosts: elk

remote\_user: dshenoycbc

become: true

tasks:

# install docker.io

- name: Install docker.io

apt:

force\_apt\_get: yes

update\_cache: yes

name: docker.io

state: present

# install python3-pip

- name: Install pip

apt:

force\_apt\_get: yes

name: python3-pip

state: present

# install docker python pip module

- name: Install docker

pip:

name: docker

state: present

# increase memory

- name: Use more memory

sysctl:

name: vm.max\_map\_count

value: "262144"

state: present

reload: yes

# increase virtual memory on restart

- shell:

echo "vm.max\_map\_count=262144" >> /etc/sysctl.conf

# install sebp/elk:761 container

- name: Install and run a docker elk container

docker\_container:

name: elk

image: sebp/elk:761

state: started

restart\_policy: always

published\_ports:

- 5601:5601

- 9200:9200

- 5044:5044

# enable service docker on boot

- name: Enable service docker on boot

systemd:

name: docker

enabled: yes

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 \_\_\_\_\_, in addition to restricting \_\_\_\_\_ to the network.

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

The Load Balancers protects the system from DDoS attacks by shifting attack traffic.

The Load Balancers ensures that the VMs and Applications in them are highly available. LBs also provides a user access to a single node that can be monitored and secured.

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

- \_TODO: What does Filebeat watch for?

Filebeat is a lightweight shipper that forwards all data to a centralized log data system. Filebeat is installed as an agent on our servers and monitors log files, collects log events, and forwards them either to Elasticsearch or Logstash for indexing.

- \_TODO: What does Metricbeat record?

Metricbeat is a lightweight shipper that you can install on your servers to periodically collect metrics from the operating system and from services running on the server. Metricbeat takes the metrics and statistics that it collects and ships them to the output that you specify, such as Elasticsearch or Logstash

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 | DVWA | 10.0.0.5 | Linux |

| Web-2 | DVWA | 10.0.0.6 | Linux |

| Web-3 | DVWA | 10.0.0.7 | Linux |

### Access Policies

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

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

- \_TODO: Add whitelisted IP addresses

71.105.12.3

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

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

Jumpbox VM – Local IP: 10.0.0.4 and Public IP: 20.94.205.25

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

|  |  |  |
| --- | --- | --- |
| Name | Publicly Accessible | Allowed IP Addresses |
| Jumpbox | Yes | 10.0.0.5 to 10.0.0.7 |
| Web-1 | No | 10.0.0.4 |
| Web-2 | No | 10.0.0.4 |
| Web-3 | No | 10.0.0.4 |
| Elk-Server | Yes | None |

NOTE – I am assuming, under Allowed IP addresses, you are asking which boxes you can SSH to from the Jumpbox and other VMs. If not then Jumpbox and Elk-Server are only allowed from 71.105.12.3 and Web 1,2, and 3 aren’t publicly accessible.

### 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?\_

Automating configuration cuts down time of developers and system admins with configuring new machines thus saving money as well. This also simplifies many complex tasks thus allowing system admins and developers focus their attention to more pressing issues.

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.\_

- First it installs the Docker.io on the machine to avoid a name conflict with docker system-tray binary

- Next, python3-pip is installed which is a package management system written in Python to install and manage software packages.

- Finally, it installs an Elk container (sebp/elk:761) while allowing (opening) the ports that it requires to connect with Kibana and transfer data to the log system.

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](Diagram/ Elk\_Docker\_PS\_Snip.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

Web-3: 10.0.0.7

We have installed the following Beats on these machines:

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

Filebeat and 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 - monitors log files, collects log events, and forwards them either to Elasticsearch or Logstash for indexing.

Metricbeat - takes the metrics and statistics that it collects and ships them to the output that you specify, such as Elasticsearch or Logstash.

### 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 \_\_\_\_\_ file to \_\_\_\_\_.

- Update the \_\_\_\_\_ file to include...

- Run the playbook and navigate to \_\_\_\_ 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?\_ First create the ansible-config file and run the pentest.yml file which creates an ansible folder under the /etc/ folder.

- \_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?\_ We have to update the hosts file under the ansible folder and add the local IPs of Web-1, Web-2, and Web-3 under the uncommented “Webservers” section.

In the same hosts file, you can create another uncommented “elk” section which you can use to specify where to install the Filebeat on.

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

And in my case, the link is: http://104.208.159.120:5601/app/kibana

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

ssh username@ip\_of\_jumpbox

sudo su

docker container ls -a

docker start <container name>

docker attach <container name>

cd /etc/ansible

nano <hosts file> # to add IPs of the webservers and elk server

nano <name of config file> # and make the necessary changes in it.

nano <name of files>.yml

ansible-playbook <name of the file>.yml

# To test if the ansible have been installed on each webserver, you should SSH into a webserver from the ansible container of the Jumpbox server. Then run the following commands:

sudo su

docker container ls -a

docker start <container name>