Automated ELK Stack Deployment

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

Red Team Security Network(Images/diagram_filename.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 files may be used to install only certain pieces of it, such as Filebeat, Metricbeat etc

All Playbook Files are located in the playbook directory

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 reliable and available, in addition to restricting unwanted traffic to the network.
There is a jump--box deployed to ensure that high level of security is maintained, restricting unauthorised access to the webservers through means of Symmetric Key SSH encrypted connection.

Integrating an ELK server allows users to easily monitor the vulnerable VMs for changes to the data and system logs.
Filebeat works by looking into logs that have been specified and forwards any new log data through to Elasticsearch
Metricbeat focuses on operating system data and services running on the server, also collecting and sending on the ElasticSearch.

The configuration details of each machine may be found below.

Name	Function	IP address	OS
JumpBox	Gateway	10.0.0.9 / 13.86.154.77	Linux (ubuntu 18.04)
Web-1	Webserver	10.0.0.10	Linux (ubuntu 18.04)
Web-2	Webserver	10.0.0.11	Linux (ubuntu 18.04)
Web-3	Webserver	10.0.0.12	Linux (ubuntu 18.04)
ELK-VM	Webserver	10.1.0.4 / 20.120.100.35	

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:
124.177.235.128 - My Workstation

Machines within the network can only be accessed by SSH. The Red Team Security Group on Azure has rules in place allowing the JumpBox VM to connect to the Webservers via the ansible container through SSH using Private key symmetric encryption. These rules are put in place to limit the attack surface for the virtual network.

Name	Publicly Accessible	Allowed IP Addresses
JumpBox	Yes	124.177.235.128
Web-1	No	10.0.0.9
Web-2	No	10.0.0.9
Web-3	No	10.0.0.9
ELK-VM	No	124.177.235.128:5601

Elk Configuration

Ansible was used to automate configuration of the ELK machine. No configuration was performed manually, which is advantageous because deploying machines becomes a simple process not only to initially deploy but also in the event of one or even all machines needing to come offline, replacements or reconfiguration can happen in a matter of minutes, furthermore it can take human error out of the equation.

The playbook implements the following tasks:

1. Looks at the host config file under ELK and carry out the following commands on the internal IP addresses that are listed.
2. Install docker.io
3. Install Python-pip
4. Increase Virtual Memory to support applications
5. Download Docker container image sep:elk and restart always
6. Ports 5044, 5601, 9200 made available for ElasticSearch

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

```
root@ElkVM:~# docker ps
CONTAINER ID   IMAGE          COMMAND                  CREATED      STATUS         PORTS
                                                                    NAMES
c43e7f47a3be   sebp/elk:761   "/usr/local/bin/star…"   8 days ago   Up 3 minutes   0.0.0.0:5044-
>5044/tcp, 0.0.0.0:5601->5601/tcp, 0.0.0.0:9200->9200/tcp, 9300/tcp   elk
root@ElkVM:~#
```

Target Machines & Beats
This ELK server is configured to monitor the following machines:

Web-1: 10.0.0.10
Web-2: 10.0.0.11
Web-3: 10.0.0.12

We have installed the following Beats on these machines:
1.Filebeat
2.Metricbeat

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

Filebeat is used to collect system logs regarding web servers, MySQL databases and Apache etc. Filebeat can gives us insight into things like sudo commands that have been executed on the system and also logs about successful and failed SSH connections including information about what credentials were used.

MetricBeat is focused more about the performance of our machines in regards to CPU usage, Memory usage and more valuable data along those lines. These tools can be very useful for monitoring suspicious behaviour that leads to preventing and investigating attacks along with monitoring how the system is performing.

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 .yml file to the ansible directory.
- Update the config file to include the IP address of your VM/VM's that is set up to host ELK server
- Run the playbook, and navigate to (ELK-VM public ip:5601) to check that the installation worked as expected.

- Which file is the playbook?
Ansible - myfirst-playbook.yml
Filebeat - filebeat-playbook.yml
Metricbeat - metricbeat-playbook.yml
ELKserver - 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?
/etc/ansible/hosts - add the IP of VM's you intend to install on.

- How do I specify which machine to install the ELK server on versus which to install Filebeat on?
When running the playbook's you will notice at the top of the playbook there is a section that reads hosts: webservers or hosts: elk. This is telling the playbook to look at the host file in mention and then look under the section webservers for instance and install on the IP addresses that are listed. The same would be said if the playbook had hosts: elk but it would look under the hosts file for the section reading elk and install on those specific VM's. This is why it is critical to have the hosts file updated before you run a playbook.

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

You will need to check what the public IP address is of your ELKVM, for example mine is 20.120.100.35, so I would navigate to http://20.120.100.35:5601
5601 being the port we set up cabana on.

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

Depending how the user has set up security on SSH connection will vary so im going to leave that section up to the user, the following is provided the user has access to Virtual Network. Also note that some of the names of your docker containers will vary.

TERMINAL COMMANDS	DESCRIPTION
ssh RedAdmin@10.0.0.9	SSH into jumpbox VM
sudo docker container list -a	Show previously running containers (-a all)
sudo docker start nifty_hershal	Start selected container
sudo docker attach nifty_hershal	Connecting to nifty_hershal container
cd /etc/ansible	Change directory
nano hosts	update hosts file for webservers IP
nano ansible.cfg	update ansible config file
cd playbooks	change to playbook directory
nano myfirst-playbook.yml	update yamal playbook
ansible-playbook myfirst-playbook.yml	run yamal playbook
nano /etc/ansible/playbooks/elk-playbook.yml	update elk-playbook.yml playbook
nano /etc/ansible/hosts	update host file with elk VM IP
ansible-playbook elk-playbook.yml	run elk playbook
ssh RedAdmin@10.1.0.4	SSH into elkvm
sudo docker container list -a	check if elk container is running
exit	
cd /etc/ansible	change directory
nano /etc/ansible/files/filebeat-config.yml	edit filebeat config
nano /etc/ansible/playbooks/filebeat-playbook.yml	edit filebeat playbook (if necessary)
ansible-playbook filebeat-playbook.yml	run filebeat playbook to install filebeat
nano /etc/ansible/files/metricbeat-config.yml	edit metricbeat config file
nano /etc/ansible/playbooks/metricbeat-playbook.yml	edit metricbeat playbook (if necessary)
ansible-playbook metricbeat-playbook.yml	run metricbeat playbook to install metricbeat
ssh RedAdmin@10.1.0.4	SSH into elkvm

systemctl status filebeat	check if service is runnnig
systemctl status metricbeat	check if service is runnnig
exit	