Automated ELK Stack Deployment

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

RedTeam Network Diagram.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 yml and config file may be used to install only certain pieces of it, such as Filebeat.

Ansible Playbook
Ansible Hosts
Ansible Configuration
Ansible ELK installation and VM Configuration
Ansible Filebeat Playbook
Ansible Filebeat Configuration File
Ansible Metricbeat Playbook
Ansible Metric Configuration File

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 available, in addition to restricting traffic to the network.

What aspect of security do load balancers protect?

Availability, Web Traffic,Web Security

What is the advantage of a jump box?

Automation, Security, Network Segmentation, Access Control

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

What does Filebeat watch for?

Monitors the log files or locations that you specify collects log events, and forwards them either to Elasticsearch or Logstash for indexing.

What does Metricbeat record?

Metricbeat takes the metrics and statics 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 to add/remove values from the table.*

Name	Function	IP Address	Operating System
Jump Box	Gateway	10.0.0.4	Linux-Ubuntu
Web-1	Server	10.0.0.5	Linux-ubuntu
Web-2	Server	10.0.0.6	Linux- Ubuntu
Web-3	Server	10.0.0.7	Linux-Ubuntu

Access Policies

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

Only the **ELK Server** machine can accept connections from the Internet. Access to this machine is only allowed from the following IP addresses: -
Via Workstation Public IP - TCP 5601

Machines within the network can only be accessed by **Workstation and Jumpbox provisioner.**-

Which machine did you allow to access your ELK VM? ***JUMPBOX***

What was its IP address?

Jumpbox ip: 10.0.0.4 via SSH 22
Workstation public ip via TCP 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/No	Workstation public Ip on SSH 22
Web-1	No	10.0.0.4
Web-2	No	10.0.0.4
Web-3	No	10.0.0.4
ELK	No	10.0.0.4

Elk Configuration

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

Ansible lets you quickly and easily deploy multi tier applications. You wont need to write custom code to automate your system, you will only list the tasks required to be done by simply writing a playbook, and Andible will figure out how to get your system to the state you want them to be in.

What is the main advantage of automating configuration with Ansible? ***To Allow IT administrators to automate away the drudgery from their daily task.***

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. - ... - …

- **Install: docker.io**
- **Install: python-pip**
- **Install: docker**
- **Command: sysctl -w vm.max_map_count=262144**
- **Launch docker container: elk**

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: -
Web-1 10.0.0.5
Web-2 10.0.0.6
Web-3 10.0.0.7

List the IP addresses of the machines you are monitoring: ***DVWA-VM1 10.0.0.5 DVWA-VM2 10.0.0.6***

We have installed the following Beats on these machines: -

ELK Server, Web-1, Web-2,

The ELK Stack installed: Filebeat and Metricbeat

These Beats allow us to collect the following information from each machine: -
Filebeat: Log Events
Metricbeat: Metrics and system statics
Using Filebeat allows you to monitor the log files or locations that you specify.
Using Metricbeat allows you to monitor your servers by collecting system metrics and services running on the server.

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 Ansible ELK Installation and VM Config file to **/etc/ansible/roles/files**. -
Update the **/etc/ansible/files/filebeat-config.yml** file to include the **ELK private IP in lines 1106 and 1806 /etc/filebeat/filbeat-config.yml**
Run the playbook (**ansible-playbook filebeat-playbook.yml**), and navigate to **Kibana-Logs: Add log data-System Logs-Module status-Check data** to check that the installation worked as expected

Answer the following questions to fill in the blanks:

Which file is the playbook? ***filebeat-playbook.yml***

Where do you copy it? **/etc/ansible/roles**

Which file do you update to make Ansible run the playbook on a specific machine? ***/etc/ansible/hosts file (IP of the virtual machine)***

How do I specify which machine to install the ELK server on versus which to install Filebeat on? **In 2 separate groups in the /etc/ansible/hosts file. One of the groups will be Webservers which have the IPs of the VMs where Filebeat was installed to. The other group is named The-ELK-Server-VM which contains the IPs of the VM ELK will be installed to.**

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

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

-------Filebeat---------

- To create the filebeat-configuration.yml file: nano filebeat-configuration.yml. For this, I used the filebeat configuration file template.

- To create the playbook: nano filebeat-playbook.yml

```
  ---
 - name: installing and launching filebeat
         hosts: webservers
       become: true
       tasks:

          - name: download filebeat deb
            command: curl -L -O
https://artifacts.elastic.co/downloads/beats/filebeat/filebeat-7.7.1-amd64.deb

          - name: install filebeat deb
            command: dpkg -i filebeat-7.7.1-amd64.deb

          - name: drop in filebeat.yml
            copy:
              src: ./files/filebeat-configuration.yml
              dest: /etc/filebeat/filebeat.yml

          - name: enable and configure system module
            command: filebeat modules enable system

          - name: setup filebeat
            command: filebeat setup

          - name: start filebeat service
           command: service filebeat start
---
```

-To run the playbook: ansible-playbook filebeat-playbook.yml

* In order to run the playbook, you have to be in the directory the playbook is at, or give the path to it (ansible-playbook /etc/ansible/roles/filebeat-playbook.yml

-------Metricbeat-------

- To create the metricbeat-configuration.yml file: nano metricbeat-configuration.yml. For this, I used the metricbeat configuration file template.

- To create the playbook: nano metricbeat-playbook.yml

```
---
  - name: installing and launching metricbeat
    hosts: webservers
    become: true
    tasks:

  - name: download metricbeat deb
    command: curl -L -O
https://artifacts.elastic.co/downloads/beats/metricbeat/metricbeat-7.7.1-amd64.deb

  - name: install metricbeat deb
    command: sudo dpkg -i metricbeat-7.7.1-amd64.deb

  - name: drop in metricbeat.yml
    copy:
      src: /etc/ansible/roles/files/metricbeat-configuration.yml
      dest: /etc/metricbeat/metricbeat.yml

   - name: enable and configure system module
     command: metricbeat modules enable system

   - name: setup metricbeat
     command: metricbeat setup

   - name: start metricbeat service
     command: service metricbeat start

   ---
```

- To run the playbook: ansible-playbook metricbeat-playbook.yml

* To order to run the playbook, you have to be in the directory the playbook is at, or give the path to it (ansible-playbook /etc/ansible/roles/metricbeat-playbook.yml