**Automated Elk Stack Deployment**

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

<https://github.com/yohannesr2/cybersecurity-project-1/blob/main/Diagram%22/Diagram.jpg>

All the files have been tested and they can be 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 Project 1 Red-Team Network Diagram file may be used to install only certain pieces of it, such as Filebeat or metricbeat.

<https://github.com/yohannesr2/cybersecurity-project-1/blob/main/Ansible%22/filebeat%20installation>

<https://github.com/yohannesr2/cybersecurity-project-1/blob/main/Ansible%22/metricbeat.txt>

This readme.md 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 Dmn Vulnerable Web Application.

* Load balancing ensures that the application will be highly functional, in addition to restricting high-traffic to the network.
* What aspect of security do load balancers protect?
* It helps prevent overloading servers as well as optimizes productivity and maximizes uptime.
* It also adds resiliency by rerouting live traffic from one server to another causing it to eliminate single points of failure from attacks such as DDoS attack.
* What is the advantage of a jump box?  
  -Jump-box are highly secured computers that are never used for non-admin tasks. Jump-box has improved into an even more comprehensive/lock-down secure admin workstation to decrease the chances of hackers/malware infection.

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

* What does Filebeat watch for?
* It monitors the log files/locations that you specify and forwards them to Elasticsearch/Logstash for indexing.
* What does Metricbeat record?
* Metricbeat will records metrics from the server and OS

The configuration details of each machine can be found below

|  |  |  |  |
| --- | --- | --- | --- |
| Name | Function | IP Address | Operating System |
| Jump Box | Gateway | 10.0.0.4 | Linux |
| Web 1 | web server | 10.0.0.5 | Linux |
| Web 2 | Web server | 10.0.0.6 | Linux |
| Web 3 | Web server | 10.0.0.7 | Linux |
| Elk | Elk server | 10.1.0.4 | Linux |

**Access Policies**

All the machines on the internal network are not exposed to the public internet. The only machine that is accepting connection from the internet is the jump-box-provisioner. Access to the jump-box-provisioner is only allowed from the local host IP address. The other machines within the network can only be accessed by the jump-box-provisioner.

The Elk VM can be accessed using the jump-box-provisioner, which has 10.0.0.4 private IP address.

**Elk Configuration**

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

* We are using YAML playbook which is the best alternative for configuration management/automation.
* It will eliminate human errors and we can configure multiple machines at once.

The playbook implements the following tasks: -

* Increase the memory of the machine
* Install pip
* Install docker python module
* Download and launch docker web container

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

<https://github.com/yohannesr2/cybersecurity-project-1/blob/main/ScreenShots%22/docker%20ps.PNG>

**Target Machines and Beats**

The 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

We have also installed the following Beats on these machine: -

* Filebeat
* Metricbeat

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

* **Filebeat: -** it generates and organizes log files to send to elasticsearch on the Elk server. The logs contain information about the file system. Examples of Filebeat can be files generated by Apache, Microsoft Azure tool, and MySQl databases.
* **Metricbeat: -** collects machine metrics. It is simply a measurement that tells analysts how healthy a machine is. Examples include CPU usage, memory, disk IO, and Network IO statistics.

**Using the Playbook**

In order to use the playbook, you will need to have the Ansible control node already configured. Assuming you have such a control node provisioned:

SSH into the control node and follow the steps below:

**For Filebeat**

* Copy the filebeat-configuration.yml file to /etc/ansible/files.
* Update the filebeat-configuration.yml file to include the Elk private IP address.
* Run the playbook, and navigate to <http://52.137.127.147:5601/> (Elk-VM) to check that the installation worked as expected.

For Metricbeat

* Copy the metricbeat-configuration.yml file to /etc/ansible/files.
* Update the metricbeat-configuration.yml file to include the ELK private IP address.
* We run the playbook and navigate to <http://52.137.127.147:5601/> 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?
* We copy it to the Elk VM
* Which file do you update to make Ansible run the playbook on a specific machine?
* The filebeat config file
* How do I specify which machine to install the ELK server on versus which to install Filebeat on?
* We add the private IP under “servers”
* \_Which URL do you navigate to in order to check that the ELK server is running?
* <http://52.137.127.147:5601/>