Automated ELK Stack Deployment:

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 Playbook (.yml) file may be used to install only certain pieces of it, such as Filebeat.

Red-Team-Project Diagram

These following files has been used to create and install DVWA on web server and Kibana on Elk server.

1. Pentest.yml (playbook) – it run on ansible container to install DVWA on both web server (Web-1 and Web-2)
2. Elk.yml – (playbook) – it run on ansible container to install ELK server
3. Filebeat-playbook.yml – install and configure filebeat on Elk server and Web server
4. Metricbeat-playbook.yml – install and configure metricbeat on Elk server and Web server

The document contains the following details:

1. Description of topology
2. Access policy
3. ELK server

* Beats in use
* Machine being monitored

1. How to use the ansible build

XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX

1. **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 available, in addition to restricting access to the network. Load balancing help ensures availability through distribution of incoming data to the webservers.

Advantage: Reduce server workload, increase performance, reduce single point of failure, improve scalability

* What is the advantage of a jump box?

Jump box allow for more easy administration of multiple systems and provide an additional security layer between the outside and internal assets. It works as secure admin workstation.

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

* What does Filebeat watch for?

Filebeat monitors the log files or location that you specify, collects log events, and forwards them to either to Elasticsearch or Logstash for Indexing

* What does Metricbeat record?

Metricbeat collect metrics and statistics from the operating system and from the services running on the server.

The configuration details of each machine may be found below (Red-Team Resource Group).

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Name | Function | OS | Location | Private - IP | Public - IP |
| Jump Box | Gateway | Linux Ubuntu VM | US East | 10.1.0.4 | 13.90.94.255 |
| Web Server – 1 | Server | Linux VM | US East | 10.1.0.5 |  |
| Web Server - 2 | Server | Linux VM | US Ease | 10.1.0.7 |  |
| Elk Server | Server | Linux VM | US West | 10.0.0.4 | 104.210.51.88 |

XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX

1. **Access Policies**

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

Only the Jump box (13.90.94.255)machine can accept connections from the Internet. Access to this machine is only allowed from the following IP addresses:

* Personal IP addresses (Private – Local Machine where we provide the public key to access)
* Local Host IP range: 107.790.0.0/16

Machines within the network can only be accessed by Jump box (10.1.0.4).

* Web server -1 (10.1.0.5)
* Web Server -3 (10.1.0.7)
* Elk Server (10.0.0.4)

Which machine did you allow to access your ELK VM?

* ELK VM can connect through Jump Box

What was its IP address?

* Jump Box IP 10.1.0.4 (Private IP)

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

|  |  |  |
| --- | --- | --- |
| Name | Publicly Accessible | Allowed IP address |
| Jump Box | No (SSH-public key authorization) | Personal IP address [(107.190.0.0/16) to (13.90.94.255)] |
| Web Server -1 | Yes, through Load Balancer | 137.135.127.119 LB Public IP, 10.1.0.4 (from jump box) |
| Web Server - 3 | Yes, through Load Balancer | 137.135.127.119 LB Public IP, 10.1.0.4 (from jump box) |
| ELK Server | yes | SSH 10.1.0.4 (jump Box), 104.210.51.88 (http with 5601 port |

XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX

1. **Elk Configuration**

Ansible was used to automate configuration of the ELK machine. No configuration was performed manually, which is advantageous because services running can be limited, system installation and update can be streamlined, and process become more replicable.

* What is the main advantage of automating configuration with Ansible?

One of the main advantages of .YML playbook, it is the best alternative for configuration management/automation.

It is also able to automate complex multi-tier IT application environment

It can deploy multiple servers easily and quickly without having to physically touch each server.

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.

1. Connect to jump box form local pc. (# ssh [azureuser@13.90.94.255](mailto:azureuser@13.90.94.255))
2. Install the docker on jump box. (# sudo apt install docker.io)
3. Pull the cyberxsecurity/ansible container inside docker. (# sudo docker pull cyberxsecurity/ansible)
4. Find out the Container list on docker (# sudo docker container list -a / ps)
5. Start / attach the ansible container. (# sudo docker start/attach container elated\_blackwell)
6. Went to /etc/ansible/roles directory and created the ELK playbook (Elk\_Playbook.yml)
7. Ran the Elk\_Playbook.yml in that same directory (ansible-playbook Elk\_Playbook.yml)
8. Lastly, I SSH into the ELK-VM to verify the server is up and running.

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

**Attached** the screen shot with step by step for ELK server

XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX

1. Update the path with the name of your screenshot of docker ps output] (Images/docker\_ps\_output.png)

Target Machines & Beats

This ELK server is configured to monitor the following machines:

* Web Server – 1 10.1.0.5
* Web Server – 3 10.1.0.7

We have installed the following Beats on these machines:

* Filebeat configuration and playbook
* Metricbeat configuration and playbook

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

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 is a log data shipper for local files. Installed as an agent on your servers, Filebeat monitors the log directories or specific log files, tails the files, and forwards them either to Elasticsearch or Logstash for indexing. An example of such are the logs produced from the MySQL database supporting our application.
* Metricbeat collects metrics and statistics on the system. An example of such is CPU usage, which can be used to monitor the system health. Metricbeat records metrics and statistical data from the operating system and from services running on the server (Metricbeat: Lightweight Shipper for Metrics)

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 configuration file from ansible container to web vm’s. (/etc/ansible/)
* Update the /etc/ansible/hosts file to include the ip address of ELK server and webservers (/etc/ansible/hosts) and ([Elkserver 1] and 10.0.0.4 ansible\_python\_interpreter=/usr/bin/python3)

Run the playbook and navigate to <http://104.210.51.88:5601/app.kibana> to check that the installation worked as expected.

XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX

Answer the following questions to fill in the blanks: \_

* Which file is the playbook and Where do you copy it?

Pentest.yml (Ansible-Playbook) – Location: /etc/ansible/pentest.yml

Elk-yml (elk-playbook.yml) – Location: /etc/ansible/elk.yml

Filebeat-Playbook.yml – Location: /etc/ansible/roles/filebeat-playbook.yml

Metricbeat-Playbook.yml – Location: /etc/ansible/roles/metricbeat-playbook.yml

* Which file do you update to make Ansible run the playbook on a specific machine?

Hosts file (Location: /etc/ansible/hosts)

Changes: [webserver]

10.1.0.5 ansible\_python\_interpreter=/usr/bin/python3 (IP address of VM web)

10.1.0.7 ansible\_python\_interpreter=/usr/bin/python3

[Elk server]

10.0.0.4 ansible\_python\_interpreter=/usr/bin/python3

How do I specify which machine to install the ELK server on versus which to install Filebeat on?\_

There is two separate groups in side the Hosts file(/etc/ansible/hosts).one group for the WEBServer and has IP address of web machine, where I will install filebeat and metricbeat too

Another group for ELK server and it has own separate ip addtess. Where I can install ELK.

- \_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.

<http://104.210.51.88:5601/app/kibana>

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