**## Automated ELK Stack Deployment**

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

RedTeamVM1@Jump-Box-Provisioner: ~$ sudo docker ps

Update the path with the name of your diagram] (Images/diagram\_filename.png)

/var/folders/5f/bf1\_hppj65qd8xvshfnlq0d00000gn/T/TemporaryItems/NSIRD\_screencaptureui\_XUMMXE/Screen Shot 2021-02-13 at 2.52.37 PM.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 playbook file may be used to install only certain pieces of it, such as Filebeat.

- Enter the playbook file.

root@82513afd5949:/etc/ansible# nano filebeat.yml

root@82513afd5949:/etc/ansible# ansible-playbook /etc/ansible/filebeat\_playbook.yml

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 access to the network. \*

\*https://github.com/adelfavero57/CyberxSecurity

- What aspect of security do load balancers protect?

"Load balancers defends an organization against distributed denial-of-service (DDoS) attacks. It does this by shifting attack from the corporate server to a public cloud provider." Load Balancing plays an important role in the security data stored in the cloud. \*

https://avinetworks.com/what-is-load-balancing/#:~:text=Load%20Balancing%20plays%20an%20important,to%20a%20public%20cloud%20provider.

What is the advantage of a jump box?

Jump box is usually a single operating system connected with two networks. One is the public network and the other is private network. They can be used to connect directly into the security zone that has questionable security. The example is storage area network (SAN). Jump box is used, to provide hidden benefit as a tool in place for the SAN system where is maintained on that single system. Therefore, when an update is released to the SAN management software, only a single system will requires an update.\*

\*https://www.techrepublic.com/blog/data-center/jump-boxes-vs-firewalls/

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

- What does Filebeat watch for?

Filebeat is watching for log files/locations and collects data on log events.

- What does Metricbeat record?

This is a lightweight shipper that can be installed on the server. It will periodically collect data from the operating system and from services running on the server and sends into specific output like Elasticsearch or Lodstash. It will help monitor servers. \*

\*https://www.elastic.co/guide/en/beats/metricbeat/current/metricbeat-overview.html#:~:text=Metricbeat%20is%20a%20lightweight%20shippersuch%20as%20Elasticsearch%20or%20Logstash.

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-Provisioner|Gateway| 10.0.0.4 |

|Linux|

|RedTeamVM1 |Web Server| 10.0.0.6| |Linux|

|RedTeamVM2 |Web Server| 10.0.0.5|

|Linux|

|DVWA-VM3 |Web Server| 10.0.0.7|

|Linux|

|ELK-SERVERVM|Web Server| 10.2.0.4|

|Linux|

**### Access Policies**

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

Only the Jump-Box-Provisioner machine can accept connections from the Internet. Access to this machine is only allowed from the following IP addresses:

- Add whitelisted IP addresses:

52.136.125.98 (Public IP)

IP whitelist means that it is an approved list of IP addresses and/or IP domains that have permission to access your domain. It is reserved only for trusted users, and set and updated by the site administrator. \*

https://github.com/adelfavero57/CyberxSecurity

Machines within the network can only be accessed by Jump-Box-Provisioner.

-Which machine did you allow to access your ELK VM? Jump-Box-Provisioner

What was its IP address? 10.0.0.4 (Public IP 52.136.125.98)

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

| Name | Publicly Accessible | Allowed IP Addresses |

|----------|---------------------|----------------------|

| Jump Box-Provisioner | Yes | 10.0.0.5 10.0.0.6 10.0.0.7 10.2.0.4|

| Web Server | 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...

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

The main advantage of this simple automation with Ansible is that allow IT administrators automate repetitive daily tasks. This provides time to focus on more complex tasks that bring value to their business. \*

https://www.ansible.com/overview/it-automation?sc\_cid=7013a0000026PAOAA2&gclid=CjwKCAiAjp6BBhAIEiwAkO9WuszFtbXuDohwPBD7yz9kHsSrskkrv\_FbNgiUhCqknkkjpaxXt1bJKhoCF5QQAvD\_BwE&gclsrc=aw.ds

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

- Install pip3

- Install Docker-Python Module

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

/var/folders/5f/bf1\_hppj65qd8xvshfnlq0d00000gn/T/TemporaryItems/NSIRD\_screencaptureui\_XUMMXE/Screen Shot 2021-02-13 at 2.52.37 PM.png

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:

- List the IP addresses of the machines you are monitoring: ELK-Server VM 10.2.0.4

We have installed the following Beats on these machines:

- Specify which Beats you successfully installed: Filebeat

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 collecting log files from the system it is monitoring and sends them into Elastic search for analysis.

**### 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 filebeat\_playbook.yml file to the host machine.

- Update the hosts file to include the IP addresses of the computers to run this on

- Run the playbook, and navigate to http://10.2.0.4/app/kibana to check that the installation worked as expected.

Answer the following questions to fill in the blanks:

- Which file is the playbook?

/etc/ansible/

/etc/ansible/filebeat\_playbook.yml

- Where do you copy it?

Host machine

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

Ansible file

- How do I specify which machine to install the ELK server on versus which to install Filebeat on? Filebeats goes into containers where you have ELK server, ELK server goes onto Virtual Machine.

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

https://portal.azure.com/#blade/HubsExtension/BrowseResource/resourceType/Microsoft.Compute%2FVirtualMachines

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

Commends:

ssh RedTeamVM1@52.136.125.98

RedTeamVM1@Jump-Box-Provisioner: ~$

sudo docker ps

sudo docker container list -a

sudo docker rm amazing\_payne

sudo docker start optimistic\_ellis

sudo docker attach optimistic\_ellis

ssh -keygen

cat .ssh/id\_rsa.pub

ansible all -m ping

container root@82513afd5949

ls /etc/ansible

nano /etc/ansible/hosts

/etc/ansible# ansible -i hosts -m ping webserver

mkdir playbooks

cd playbooks

~/playbooks# ansible-playbook /etc/ansible/pentest.yml

~/playbooks# ansible-platbook /etc/ansible/filebeat\_playbook.yml

~/playbooks# nano /etc/ansible filebeat.yml

nano /etc/ansible/install-elk.yml