### **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.

* *TODO: What aspect of security do load balancers protect? What is the advantage of a jump box?*
* *Load balancers protect network traffic.*
* *An advantage of a jump box is that everything needed on a SAN system is all in one system so it will only require one system to update for them all too.*

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

* *TODO: What does Filebeat watch for? It monitors log files on the network to see if there is any suspicious activity*
* *TODO: What does Metricbeat record? It records metrics from the operating system and other services running on the server*

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 | Gateway | 10.0.0.1 | Linux |
| RedTeam |  | 10.0.0.5 | Linux |
| Project |  | 10.0.0.7 | Linux |
|  |  |  |  |

### **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:

* *TODO: Add whitelisted IP addresses*

Machines within the network can only be accessed by \_SSH through the jumpbox first\_.

* *TODO: Which machine did you allow to access your ELK VM? What was its IP address? The vm i allowed access to the elk vm was the Project VM ip address 10.0.0.7*

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

|  |  |  |
| --- | --- | --- |
| **Name** | **Publicly Accessible** | **Allowed IP Addresses** |
| Jump Box | No | 10.0.0.1 10.0.0.2 |
| RedTeam | no | 10.0.0.5 |
| Project | no | 10.0.0.5 |

### **Elk Configuration**

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

* *TODO: What is the main advantage of automating configuration with Ansible? The advantage of automation of these processes would allow for a cleaner and more streamlined cloud data storage and access service for those who utilize these services. If the process were to be automated, much like google drive, documents and data are far less likely to be lost or destroyed due to a lack of a save. This process would also make creating applications and softwares far easier and more streamline.*

The playbook implements the following tasks:

* *TODO: In 3-5 bullets, explain the steps of the ELK installation play. E.g., install Docker; download image; etc.*
* Sudo apt install docker.io to install docker
* Sudo docker pull sebp/elk:E1L1K4 to pull the image
* Sudo docker run -p 5601:5601 -p 9200:9200 -p 5044:5044 -it --name elk sebp/elk to run a container from the image

### **Target Machines & Beats**

This ELK server is configured to monitor the following machines:

* *TODO: List the IP addresses of the machines you are monitoring*
* 10.0.0.1
* 10.0.0.5
* 10.0.0.7

We have installed the following Beats on these machines:

* *TODO: Specify which Beats you successfully installed*

*We successfully installed a beat called filebeat which can forward logs and other file data to elasticsearch.We also installed metricbeat which overtime collects metrics from operating systems on the server.*

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

* *TODO: 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.*
* *Two examples of these beats are: the packetbeat and the filebeat.*
* *The metricbeat is used as a light weight shipper for server data.*
* *The filebeat is a shipper for logs and other file data.*

### **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 \_playbook\_ file to \_the ELK VM\_.
* Update the \_Metricbeat\_ file to include...
* Run the playbook, and navigate to \_http://[your.vm.ip]:5601\_ to check that the installation worked as expected.

*TODO: Answer the following questions to fill in the blanks:*

* *Which file is the playbook? filebeat-playbook.yml Where do you copy it? From ansible container to ELK VM*
* *Which file do you update to make Ansible run the playbook on a specific machine? Update the metricbeat config file How do I specify which machine to install the ELK server on versus which to install Filebeat on? By replacing the ip address in elasticsearch with the ip address of your ELK machine*
* \_Which URL do you navigate to in order to check that the ELK server is running? http://[your.vm.ip]:5601