**## Automated ELK Stack Deployment**

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

[**Darryl Owens Chapter 13 project**](https://drive.google.com/file/d/1ro9F0sIQtMsU4vDFNolWU4SN4CpT92Js/view?usp=sharing)

**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 Install-elk.yml file may be used to install only certain pieces of it, such as Filebeat.**

**- \_TODO: Enter the playbook file. Metricbeat-playbook.yml screenshot** 

**Filebeat-playbook.yml screenshot**



**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 and restricts traffic to the network. What aspect of security do load balancers protect? What is the advantage of a jump box? 1. Load Balancing plays a critical role in security for the cloud it covers against DDOS attacks. It also manages traffic spikes and restricts and prevents spikes on a traffic server good load balancer also ensures performance and reliability of computing resources. 2. The advantage of having a jump box is the same as having a physical one for your car. It starts up everything you see in the diagram from web one to elk server. The jump box in this project was able to carry containers to which we can use to install playbooks to browse through the elastic search or to try and infiltrate the DVWA server that we will use later.**

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

**What does Filebeat watch for? Filebeat monitors the log files or locations that you specify collects log events and forwards them to** [**Elasticsearch**](https://www.bing.com/search?q=Elasticsearch&filters=sid%3ac6dfffe9-4554-9765-c6bb-447fa6736e31&form=ENTLNK) **or Logstash for indexing.**

**What does Metricbeat record? Metricbeat is a lightweight shipper that you can install on your servers to periodically collect metrics from the operating system and services running on the server. Metricbeat takes the metrics and statistics 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](http://www.tablesgenerator.com/markdown\_tables) to add/remove values from the table\_.**

**| Name | Function | Ip Address | operating system |**

**|----------|------------|------------|------------------|**

**| Jump Box | Gateway | 10.0.0.4 | 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 |**

**| Elkvm | Web Server | 10.1.0.4 | linux |**

**### Access Policies**

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

**Only the Jump BOX machine can accept connections from the Internet. Access to this machine is only allowed from the following IP addresses: 20.120.81.193**

**Machines within the network can only be accessed by SSH Protocol to the jump box provisioner; then, you can choose to ssh to web-1,web-2,web-3, and ELKVM.**

**- \_TODO: Which machine did you allow to access your ELK VM? What was its IP address? The device that was allowed access was the jump box provisioner the IP address 10.0.0.4**

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

**| Name | | Publicly Accessible | Allowed IP Address |**

**|---|---|---|---|**

**| Jump Box | | yes | 20.120.81.93 |**

**| Web-1 | | no | N/A |**

**| Web-2 | | no | N/A |**

**| Web-3 | | no | N/A |**

**| Elkvm | | yes | 20.120.81.93 |**

**### Elk Configuration**

**Ansible was used to automate configuration of the ELK machine. No configuration was performed manually, which is advantageous because It saves time when you can execute the same ansible command, prevents your tasks from being tedious makes your system very reliable.**

**What is the main advantage of automating configuration with Ansible? You can run anything within that container with an ansible file available with a playbook.**

**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.**

**1. Install docker.io**

**2. Install Python3-pip**

**3. Install Docker Module**

**4. Increase Virtual Memory**

**5. Download and launch a docker elk container**

**6. Published ports**

**7. Enable service docker on boot**

**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:**

**1.Web-1 10.0.0.5**

**2.Web-2 10.0.0.6**

**3.Web-3 10.0.0.7**

**We have installed the following Beats on these machines:**

**- \_TODO: Specify which Beats you successfully installed**

* **We were able to install filebeats and metricbeats successfully**

**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.**

* Filebeats: Filebeat plays the role of the logging agent—installed on the machine generating the log files, tailing them, and forwarding the data to either Logstash for more advanced processing or directly into Elasticsearch for indexing filebeats ships log files
* Metricbeats: Metricbeat is a lightweight shipper that you can install on your servers to periodically collect metrics from the operating system and services running on the server. Metricbeat takes the metrics and statistics that it collects and ships them to the output that you specify, such as Elasticsearch or Logstash

**### 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 YAML playbook file to ansible machine located on etc/ansible**

**- Update the config file to include the IP address of machines we are employing, adding the ports we are using and also username as well**

**- Run the playbook, and navigate to \_\_\_\_ to check that the installation worked as expected.**

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

**- \_Which file is the playbook? Where do you copy it?**

**The paybook.YAML files are the playbooks files as seen in this screenshot** 

**You copy the files inside the yml playbook on the ansible container located in the etc/ansible.**

**- \_Which file do you update to make Ansible run the playbook on a specific machine? How do I specify which machine to install the ELK server versus which to install Filebeat on? You will update the config file of each playbook you are trying to run or download. For instance, if I want to make changes to metricbeat, I will use the metricbeat-config.yml. The description I gave before is the answer to the second question. You will use the config.yml of the information you are trying to install to determine if you will use elk or filebeat.**

**- \_Which URL do you navigate to in order to check that the ELK server is running?** [**Kibana**](http://52.173.104.43:5601/app/kibana#/home) **52.173.104.43.:5601.app/kibana#/home**

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