## Automated ELK Stack Deployment  
  
The files in this repository were used to configure the network depicted below.  
  
![TODO: Update the path with the name of your diagram](Images/diagram\_filename.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 \_\_\_\_\_ file may be used to install only certain pieces of it, such as Filebeat.  
  
  - \_TODO: <https://github.com/dwmamone/Daniel-s-Repository.git>

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 **(availabilty**), in addition to restricting (**traffic**) to the network.  
- \_TODO: What aspect of security do load balancers protect? (**DOS attacks**) What is the advantage of a jump box?\_(**creates a secure central point that all admins can connect to**)  
  
Integrating an ELK server allows users to easily monitor the vulnerable VMs for changes to the \_\_(**Logs**)\_\_\_ and system \_\_(**Traffic**)\_\_\_.  
- \_TODO: What does Filebeat watch for?\_ **Log Data**  
- \_TODO: What does Metricbeat record?\_ **Metric Data**  
  
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            |  
| DVWA 1   |Web Server| 10.0.0.5   | Linux            |  
| DVWA 2   |Web Server| 10.0.0.6   | Linux**            |  
**| Elk      |Monitoring| 10.1.0.4   | 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\_ **(23.96.116.12)**  
Machines within the network can only be accessed by \_\_\_**machines in the network**\_\_.  
- \_TODO: Which machine did you allow to access your ELK VM? (**Jumpbox**) What was its IP address? (**Jumpbox:23.96.116.12**)  
  
A summary of the access policies in place can be found in the table below.  
  
| Name     | Publicly Accessible | Allowed IP Addresses |  
|----------|---------------------|----------------------|  
**| Jump Box |     Yes             | 23.96.116.12     |  
|  Web-1   |     No              | 10.0.0.6-254         |  
|  Web-2   |     No              | 10.0.0.5-254         |  
|  ELK     |     No              | 10.1.0.4-254         |**  
### 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?\_ **Frees up time for the administrator to focus on other tasks**  
The playbook implements the following tasks:  
**- Create an Ansible playbook that installs docker to the ELK container  
- creates the playbook**

**-Adds ELK to the host file**  
  
The following screenshot displays the result of running `docker ps` after successfully configuring the ELK instance.  
  
![TODO: Update the path with the name of your screenshot of docker ps output]

**~/Daniel’s Repository/Ansible/screenshots/PS Screenshot.PNG**

  
  
### Target Machines & Beats  
This ELK server is configured to monitor the following machines:  
**- DVWA1 10.0.0.5  
- DVWA2 10.0.0.6**

We have installed the following Beats on these machines:  
**- Filebeat  
- Metricbeat**  
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.\_  
**-Filebeat: Detects changes in the system (apache logs)  
-Metricbeat: Detects changes in metrics (CPU usage)**  
  
### 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 \_\_**yml**\_\_\_ file to \_\_**playbook**\_\_\_.  
- Update the \_\_**Host**\_\_\_ file to include...  
- Run the playbook, and navigate to \_\_\_**VM**\_ to check that the installation worked as expected.  
  
\_TODO: Answer the following questions to fill in the blanks:\_  
- \_Which file is the playbook? **Yml file** Where do you copy it? **Playbook directory**  
- \_Which file do you update to make Ansible run the playbook on a specific machine? **Host file** How do I specify which machine to install the ELK server on versus which to install Filebeat on? **Create a group and then add the IPs to the group**  
- \_Which URL do you navigate to in order to check that the ELK server is running? **13.83.88.244:5601/app/kibana**  
  
\_As a \*\*Bonus\*\*, provide the specific commands the user will need to run to download the playbook, update the files, etc.\_