Automated ELK Stack Deployment

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

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

Image will be provided on a separate file in GitHub and google drive folder.

These files have been tested and used to generate a live ELK deployment on Azure. They can be used t o 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.

The two files to help setup not just ELK but also Filebeat are:

install_elk.yml and filebeat-playbook.yml thse two files are used to create elk and configure filebeat.

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 ____, in addition to restricting _____ to the network.

-What aspect of security do load balancers protect? What is the advantage of a jump box?

Load balancers help with making sure that the amount of data web servers is obtaining are controlled so you don't have a shutdown of servers, so it maintains its availability.

The advantages of a jump box that it becomes the centralized organizational unit for all other servers and services connected to it. In a security aspect it provides protection for the internal resources by be coming the connection point to all other internal processes within the cloud environment. and from a functional aspect it makes modifying and configuring services within a system easier and more manag eable since the jumpbox acts as the service center for the cloud environment.

Integrating an ELK server allows users to easily monitor the vulnerable VMs for changes to the ____ a nd system _____.

- What does Filebeat watch for?

Filebeat monitors system logs, event logs and log files.

- What does Metricbeat record?

Metricbeat records system usage from CPU usage to system memory from operating systems and serv ers it is monitoring.

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
RedTeamJB	Gateway	10.0.0.10	Ubuntu Linux
RedTeamWeb1	Web server	10.0.0.11	Ubuntu Linux/DVWA
RedTeamWeb2	Web server	10.0.0.12	Ubuntu Linux/DVWA
RedTeamWeb3	Web server	10.0.0.13	Ubuntu Linux/DVWA
ELKVM	Monitoring system	10.1.0.4	Ubuntu Linux/DVWA

Access Policies

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

Only the _____ machine can accept connections from the Internet. Access to this machine is only allo wed from the following IP addresses:

The only machine that accepts connection from the internet is RedTeamJB and the ip address allowed is your personal device IP Address which right now is: 73.122.219.135.

Machines within the network can only be accessed by _____.

Which machine did you allow to access your ELK VM? What was its IP address?

The only machine that is allowed connection and that can access the ELKVM is the RedTeamJB Which has an IP of : 10.0.0.10

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

Name	Publicly Accessible	Allowed IP Addresses
RedTeamJB	YES	Personal PublicIP Only
RedTeamWeb1	NO	RedTeamJB 10.0.0.10
RedTeamWeb2	NO	RedTeamJB 10.0.0.10
RedTeamWeb3	NO	RedTeamJB 10.0.0.10
ELKVM	NO	RedTeamJB 10.0.0.10/Personal PublicIP

Elk Configuration

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

What is the main advantage of automating configuration with Ansible?

The advantages are the extreme ease of managing multiple servers or systems at once. You are able to configure multiple machines at once by simply applying the correct configurations to a file and specifying a host set to direct these configurations too by simply running : ansible-playbook 'The path in which the playbook.yml file is located.'

The playbook implements the following tasks:

- 5 bullets, explain the steps of the ELK installation play. E.g., install Docker; download image; etc._

- **Download docker.io:**
  The first step in the installation playbook is to install docker onto the new ELKVM we created. This will allow us to use docker to create a container for this VM to manage and configure within the ELKVM.

- **Use apt/pip Module:**
  In this step we want to install the pip3 and python module, this enables the ELKVM to be able to use the python module to parse specific data like filebeat that monitors system logs and metricbeat that monitors system data usage. This is an important step because python comes with an easy-to-use logging module and pip3 is basically a management system for python module software.

- **Use systemctl Module:**
  In this step we configure the systemctl module to configure a max memory usage count. This is important so we make sure the system is running enough memory cap to support the system and at the same time control system overload which will cause processes to run inefficiently.

- **Use docker_container Module:**
  In this step we download and launch the docker container specified for the ELKVM. This creates a container with a name that you desire and also downloads the image on which the elk server will run on. More so, we are able to configure the state of the container and restart policy as well as what ports we want this container to be published on.

- **Use systemd Module:**
  In this step we enable the docker service on boot. This is also important because restarting a machine after adding new configurations will lower the chances of docker service throwing back errors and will ensure that docker is enabled by default after every system reboot.

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

Update the path with the name of your screenshot of docker ps output](Images/docker_ps_output.png)

Image will be provided on a separate file in GitHub and google drive folder.

Target Machines & Beats

This ELK server is configured to monitor the following machines:

-List the IP addresses of the machines you are monitoring

RedTeamWeb1 – 10.0.0.11

RedTeamWeb2 – 10.0.0.12

RedTeamWeb3 – 10.0.0.13

We have installed the following Beats on these machines:

Specify which Beats you successfully installed.

Filebeat and Metricbeat have been successfully installed.

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

2 sentences, explain what kind of data each beat collects, and provide 1 example of what you expect t o see. E.g., `Winlogbeat` collects Windows logs, which we use to track user logon events, etc.

Filebeat: collects data such as system and event logs. It monitors log information from specific machines that are set and continues to forward that information into Elasticsearch.

Metricbeat: Collects system usage and metrics data. It collects operating system and services running information combined with CPU and memory usage from the machines that have been specified for metric analysis.

Using the Playbook

In order to use the playbook, you will need to have an Ansible control node already configured. Assum ing you have such a control node provisioned:

SSH into the control node and follow the steps below:

- Copy the ____ file to _____.

- Update the _____ file to include...

- Run the playbook and navigate to ____ to check that the installation worked as expected.

Answer the following questions to fill in the blanks:

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

The playbook file is named: filebeat-playbook.yml it can be found in the /etc/ansible/roles directory.

- _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 on versus which to install Filebeat on?

You want to create a new ELK group in the ansible hosts file and add the ELKVM private IP to it. Then you want to update the filebeat-configure.yml file with the ELKVM Private IP address and username and password. And to specify which machines to install filebeat on in the filebeat-playbook.yml in the top of the script file you want to specify the host variable to the machines you are trying to configure filebeat on in this case it was all the hosts in the webserver group (RedTeamWeb1, RedTeamWeb2, RedTeamWeb3)

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

http://168.61.149.11:5601/app/kibana