Project Day two

Installing File beat and metric beat

<http://20.124.8.117:5601/app/kibana#/home>

Once we are at our home page using our ELK Servers IP address, we want to select the ***Add Log Data***

Graphical user interface

Description automatically generated

We want to proceed to the system logs

Graphical user interface, application

Description automatically generated

We want to ensure we are selecting the Debian software version of the installation and since it will be our first time using Filebeat we can select the ***Getting started Guide***  so that we may install the ELK stack

**Graphical user interface, text, application

Description automatically generated**

**Graphical user interface, text, application

Description automatically generated**

We want to start and attach to our docker container. Then we want to create a configuration yml for our Filebeat file. So we want to ensure that its in ansible so we do so by

🡪cd /etc/ansible/

🡪ls

🡪nano Filebeat-config.yml

A screenshot of a computer

Description automatically generated

We then curl the configuration file into our Filebeat file to avoid errors

🡪 curl https://gist.githubusercontent.com/slape/5cc350109583af6cbe577bbcc0710c93/raw/eca603b72586fbe148c11f9c87bf96a63cb25760/Filebeat >> /etc/ansible/filebeat-config.yml

🡪ls

🡪nano Filebeat-config.yml

Text

Description automatically generated

Text

Description automatically generated

Since I will be changing the configuration file I took an additional step to create an original version of the file.

🡪 curl https://gist.githubusercontent.com/slape/5cc350109583a/ansible/preconfigured-filebeat.yml

Text

Description automatically generated

So, we now want to configure the file to add our webserver IP address to the Elk server that is on line 1106 of the file.

Text

Description automatically generated

Our IP for the Elk Server is 10.0.0.4 the 9200 is the host Elasicsearch so we must also make the change for the Kibana host on line 1806.

Text

Description automatically generated

We repeat the change of Ip to 10.0.0.4 for the Kibana host at port 5601

Text

Description automatically generated

Our next objective is to create a playbook to run the filebeat and its modules we begin by

🡪***nano filebeat-playbook.yml***

Text

Description automatically generated

Text

Description automatically generated

Text

Description automatically generated

So now we must check our data

Graphical user interface, text, application, email

Description automatically generated

So now we must add metric data

Graphical user interface, text, application, email

Description automatically generated

We want to select the Docker Metrics

Graphical user interface

Description automatically generated

Text

Description automatically generated

Text

Description automatically generated with medium confidence

Timeline

Description automatically generated

Graphical user interface, text, application

Description automatically generated

Graphical user interface, text, application

Description automatically generated

Text

Description automatically generated

Text

Description automatically generated

Text

Description automatically generated

Graphical user interface, text

Description automatically generated

Graphical user interface, text, application

Description automatically generated

such a great tool very resourceful