Project #1

Franco Chirichella
Franco.Chirichella@Innovapost.com
fpchirichella@gmail.com

GitHub Fundamentals and Project 13 Submission

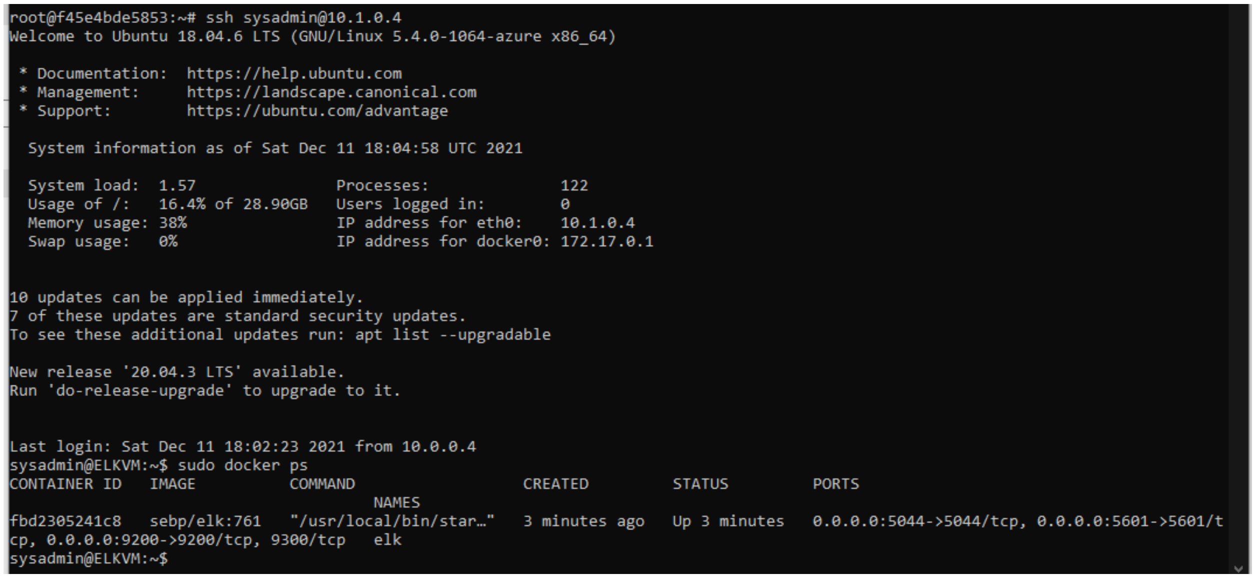
December 19, 2021

Day 1 Activity File: ELK Installation

Part 4: Launching and Exposing the Container

Check your playbook for typos and other errors, then run it.

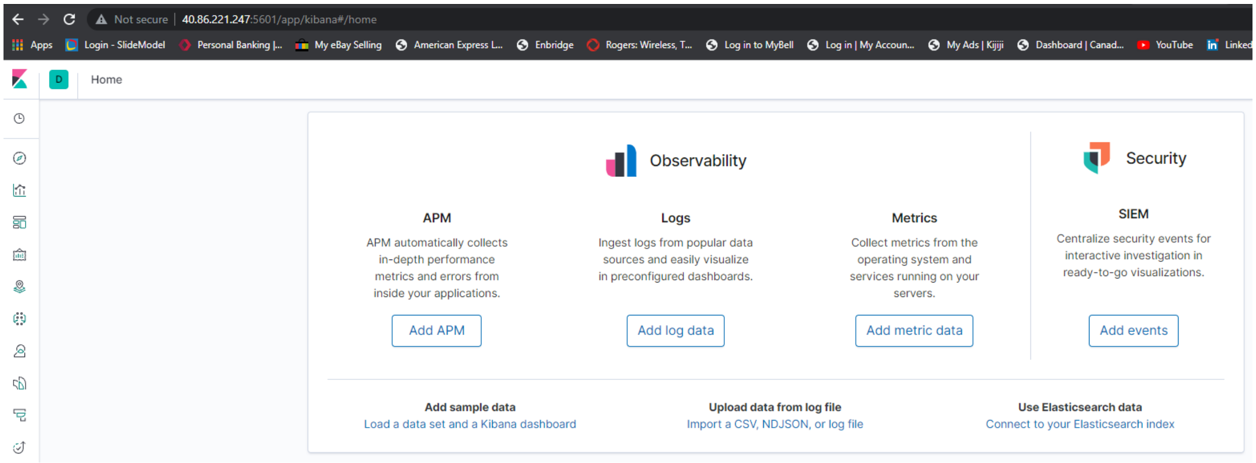
After the playbook completes, you should still be in the Ansible container. From there, use the command line to SSH into the ELK server and ensure that the sebp/elk:761 container is running by running: docker ps.



```
root@f45e4bde5853:~# ssh sysadmin@10.1.0.4
Welcome to Ubuntu 18.04.6 LTS (GNU/Linux 5.4.0-1064-azure x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

  System information as of Sat Dec 11 18:04:58 UTC 2021

  System load:  1.57               Processes:              122
  Usage of /:   16.4% of 28.90GB   Users logged in:        0
  Memory usage: 38%                IP address for eth0:    10.1.0.4
  Swap usage:   0%                 IP address for docker0: 172.17.0.1


10 updates can be applied immediately.
7 of these updates are standard security updates.
To see these additional updates run: apt list --upgradable

New release '20.04.3 LTS' available.
Run 'do-release-upgrade' to upgrade to it.


Last login: Sat Dec 11 18:02:23 2021 from 10.0.0.4
sysadmin@ELKVM:~$ sudo docker ps
CONTAINER ID   IMAGE          COMMAND                  CREATED         STATUS         PORTS
                                        NAMES
fbd2305241c8   sebp/elk:761   "/usr/local/bin/star…"   3 minutes ago   Up 3 minutes   0.0.0.0:5044->5044/tcp, 0.0.0.0:5601->5601/t
cp, 0.0.0.0:9200->9200/tcp, 9300/tcp   elk
sysadmin@ELKVM:~$
```

Part 5: Identity and Access Management

Verify that you can access your server by navigating to *[http://[your.ELK-VM.External.IP]:5601/app/kibana](http://[your.ELK-VM.External.IP]:5601/app/kibana). Use the public IP address of your new VM.*



Not secure | 40.86.221.247:5601/app/kibana#/home

APM

APM automatically collects in-depth performance metrics and errors from inside your applications.

Logs

Ingest logs from popular data sources and easily visualize in preconfigured dashboards.

Metrics

Collect metrics from the operating system and services running on your servers.

SIEM

Centralize security events for interactive investigation in ready-to-go visualizations.

Add sample data
Load a data set and a Kibana dashboard

Upload data from log file
Import a CSV, NDJSON, or log file

Use Elasticsearch data
Connect to your Elasticsearch index

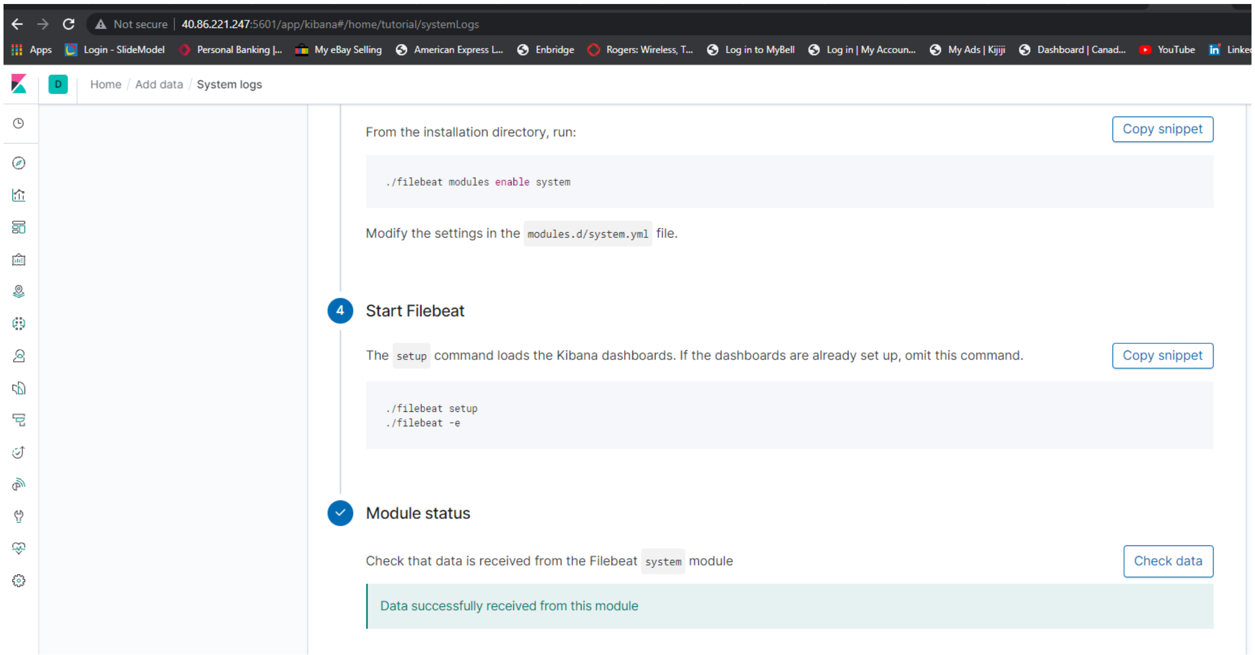
Day 2 Activity File: Filebeat and Metricbeat Installation

Part 4: Verifying Installation and Playbook

After the playbook completes, follow the steps below to confirm that the ELK stack is receiving logs from your DVWA machines:

6. Navigate back to the Filebeat installation page on the ELK server GUI.
7. On the same page, scroll to **Step 5: Module Status** and click **Check Data**.
8. Scroll to the bottom of the page and click **Verify Incoming Data**.

If your installation was successful, take a screenshot of what you see before proceeding.



From the installation directory, run:

```
./filebeat modules enable system
```

Modify the settings in the `modules.d/system.yml` file.

4 Start Filebeat

The `setup` command loads the Kibana dashboards. If the dashboards are already set up, omit this command.

```
./filebeat setup
./filebeat -e
```

✓ Module status

Check that data is received from the Filebeat `system` module

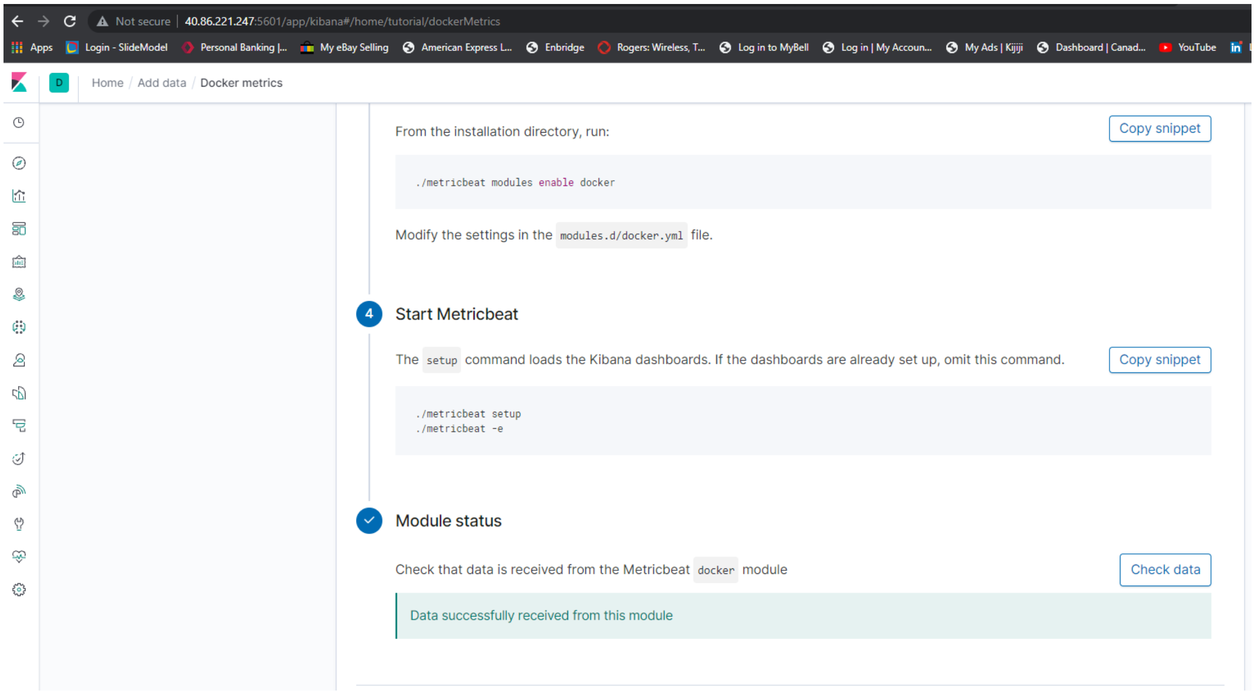
Data successfully received from this module

Part 5: Creating a Play to Install Metricbeat

Verify that your play works as expected:

- On the Metricbeat Installation Page in the ELK server GUI, scroll to **Step 5: Module Status** and click **Check Data**.

If your installation was successful, take a screenshot of what you see before proceeding.



From the installation directory, run:

Copy snippet

```
./metricbeat modules enable docker
```

Modify the settings in the `modules.d/docker.yml` file.

4 Start Metricbeat

The `setup` command loads the Kibana dashboards. If the dashboards are already set up, omit this command.

Copy snippet

```
./metricbeat setup
./metricbeat -e
```

✓ Module status

Check that data is received from the Metricbeat `docker` module

Check data

Data successfully received from this module