**THE GEORGE WASHINGTON UNIVERSITY**

***CYBERSECURITY BOOTCAMP***

**Project 1: ELK Stack Project**

***February 2022***

**NGAZWA ANDRE-JAY BABU**

1. **Project introduction**

We are aimed to build an Elk server environment where we will be sitting a Kibana environment for the purpose of Dashboard monitoring. Through Kibana we should be able to track all the metrics and examine the logs for all our systems performance and security. In our case we deemed to be within an Azure cloud environment where we will be deploying a number of virtual environments together with some security groups. Within those virtual environments, we should be able to run ansible for docker containerization to automate the process within our chosen infrastructure.

1. **Project Layout**

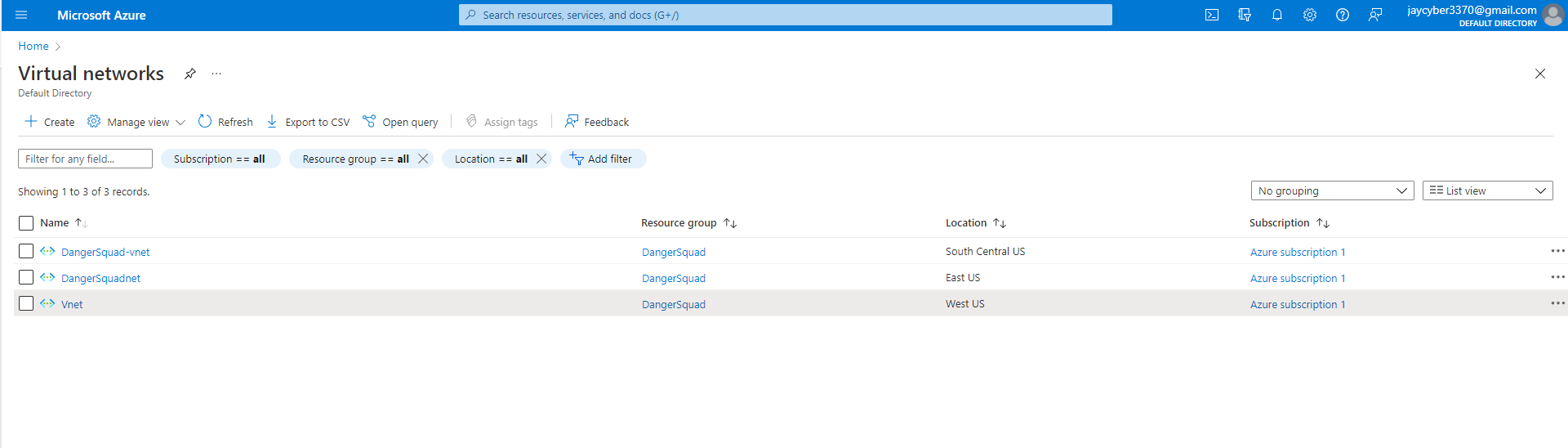
The project will consist of three phases from which we will respectively accomplish the following tasks:

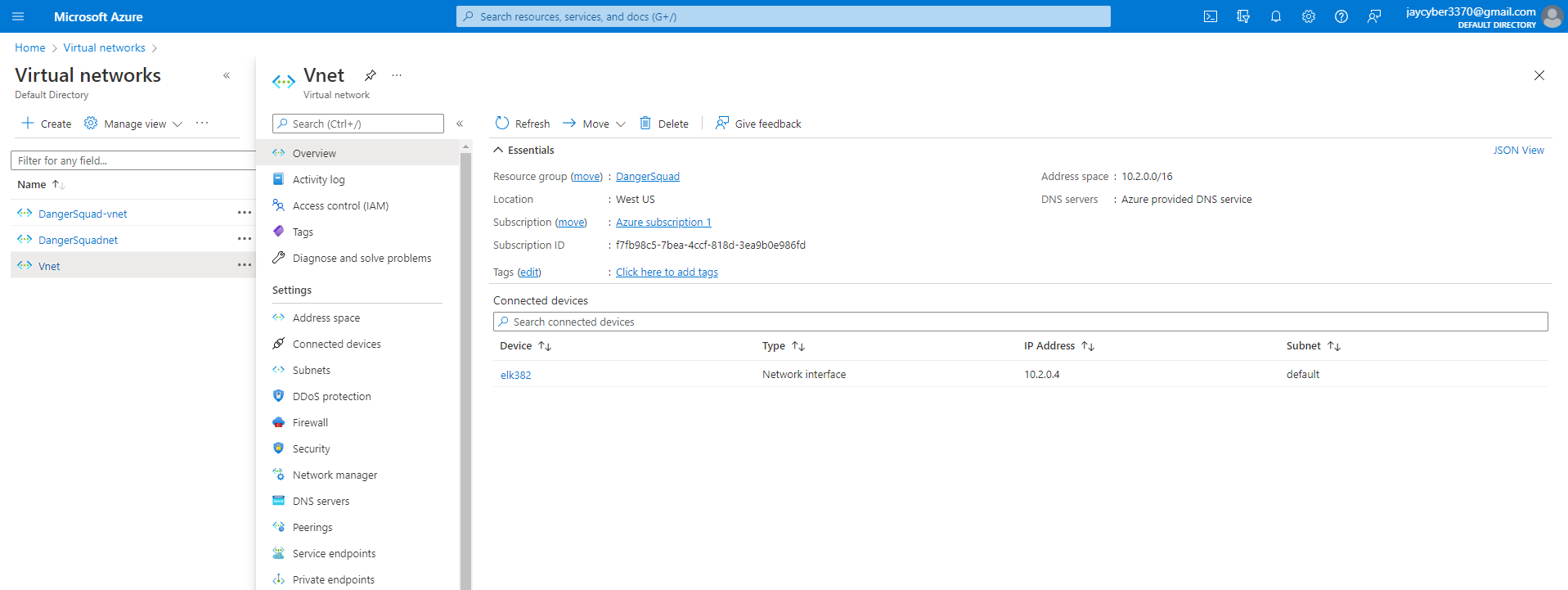
* Installing and configuring the ELK server within our set up Virtual Network.
* Installing the Filebeat and Metricbeat tools within our set up ELK monitoring server environment.
* Setting up Metrics and Logs orientation.

**II.1. Installing and configuring ELK**

1. *We will create a new vNet environment in a new region within the previously created resource group*
2. *We will then create a Peer-to-Peer Network connection between the vNets*

After running all the required parameters, we will be looking at the following vNet environment peering with our previously created virtual network

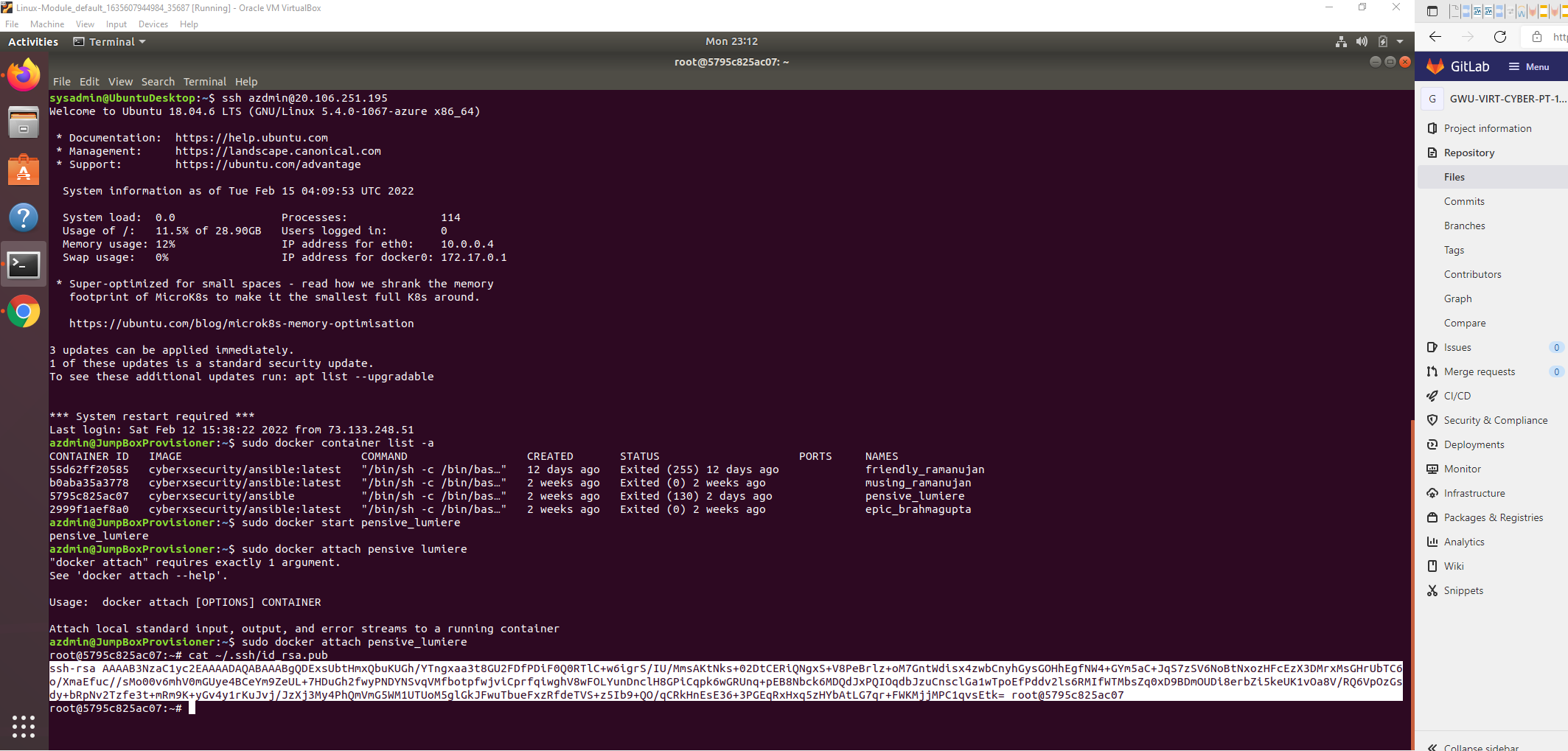




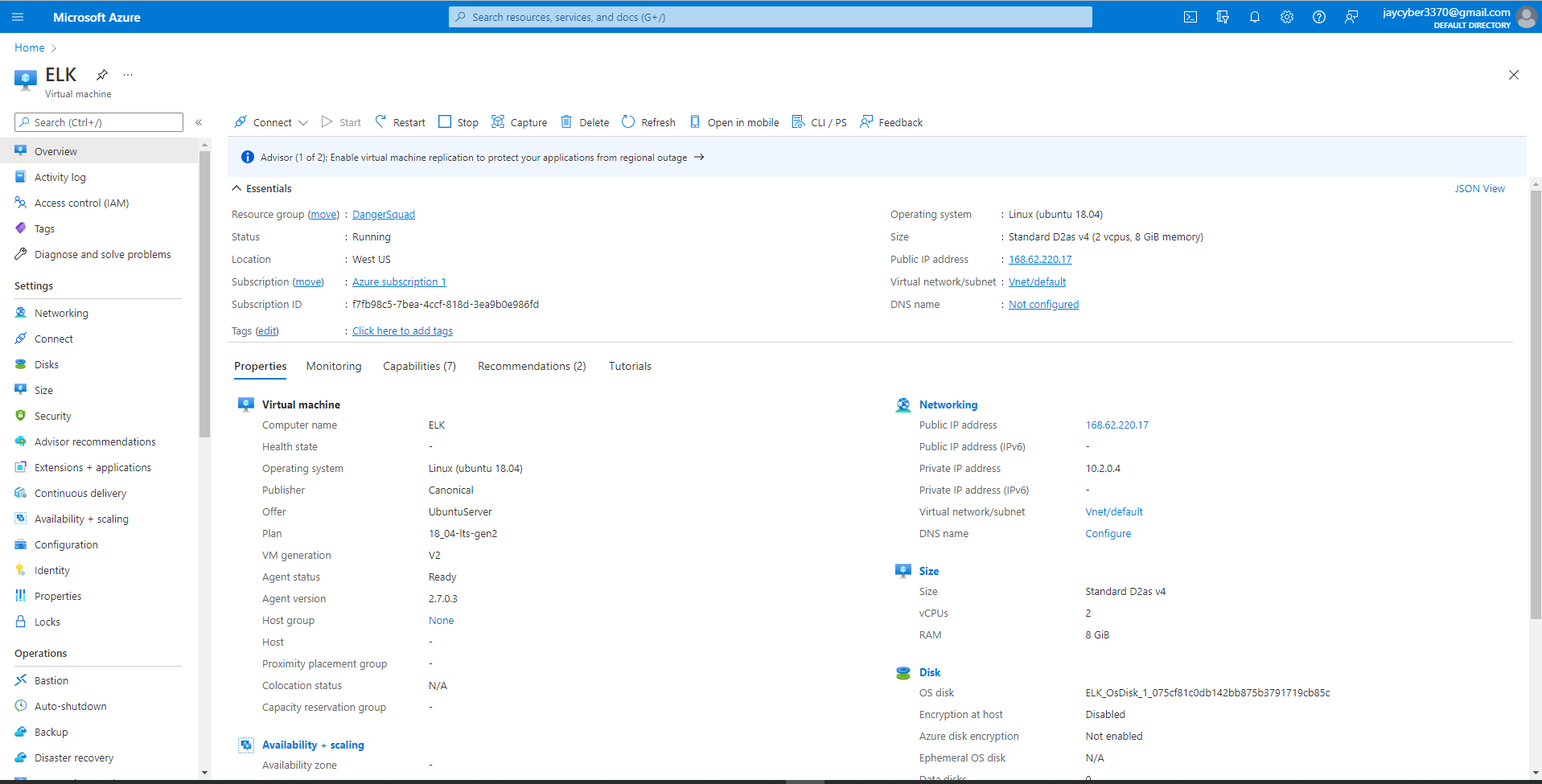
1. *We will then deploy a new VM into the new vNet with it`s own Security Group that will host the ELK server*

For that, we will also need to long in to the Jump box environment in order to generate a public key that will be used for the purpose of creating an access to that new VM via the SSH connection

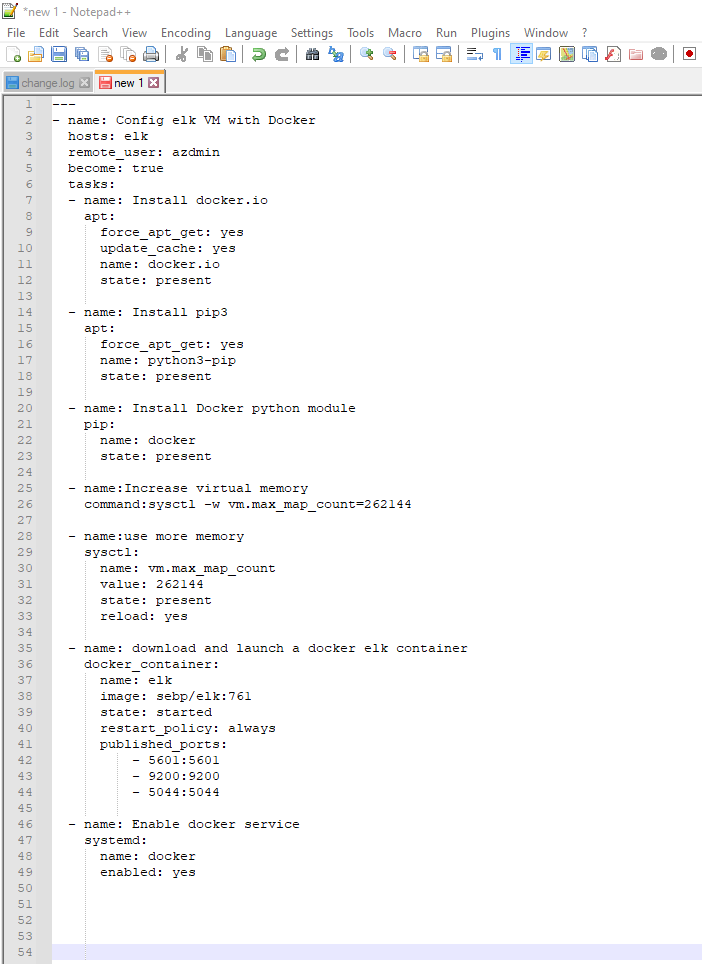
We will run the following steps appearing in the terminal to obtain the highlighted public key:



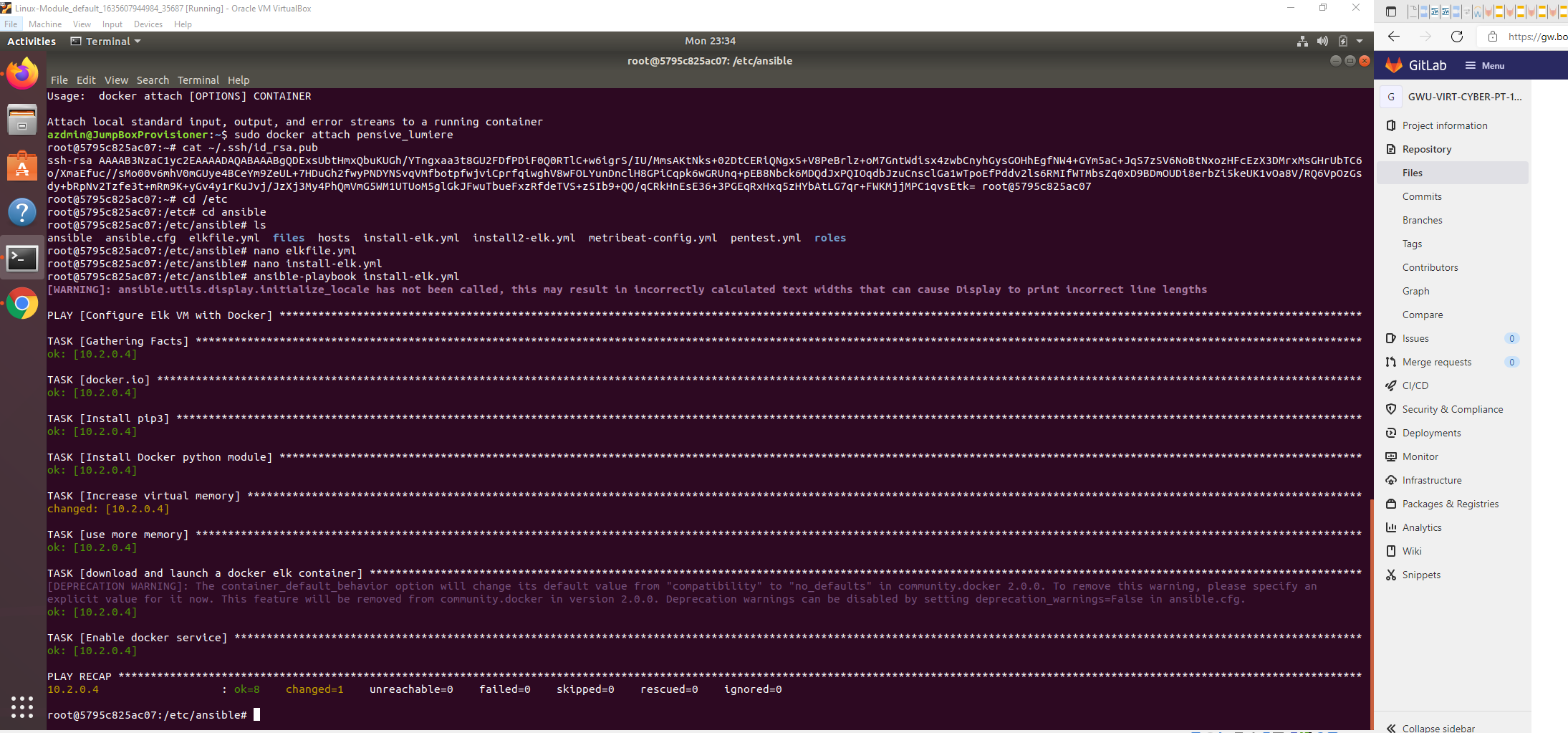
After running all the required parameters, we will end up with the following ELK server environment:



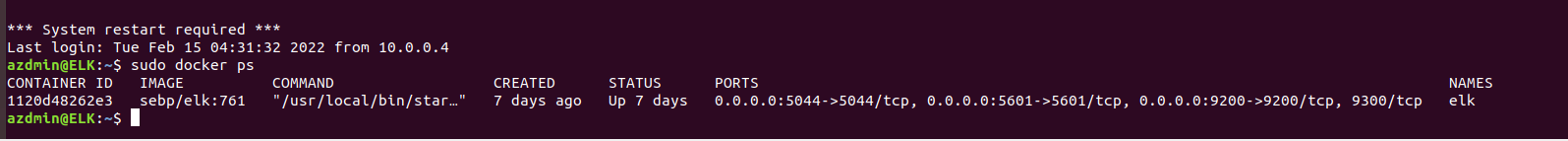
1. *We will then download and configure the container by running the following playbook with the listed details:*



1. *We will then launch and expose the container to read the following results:*

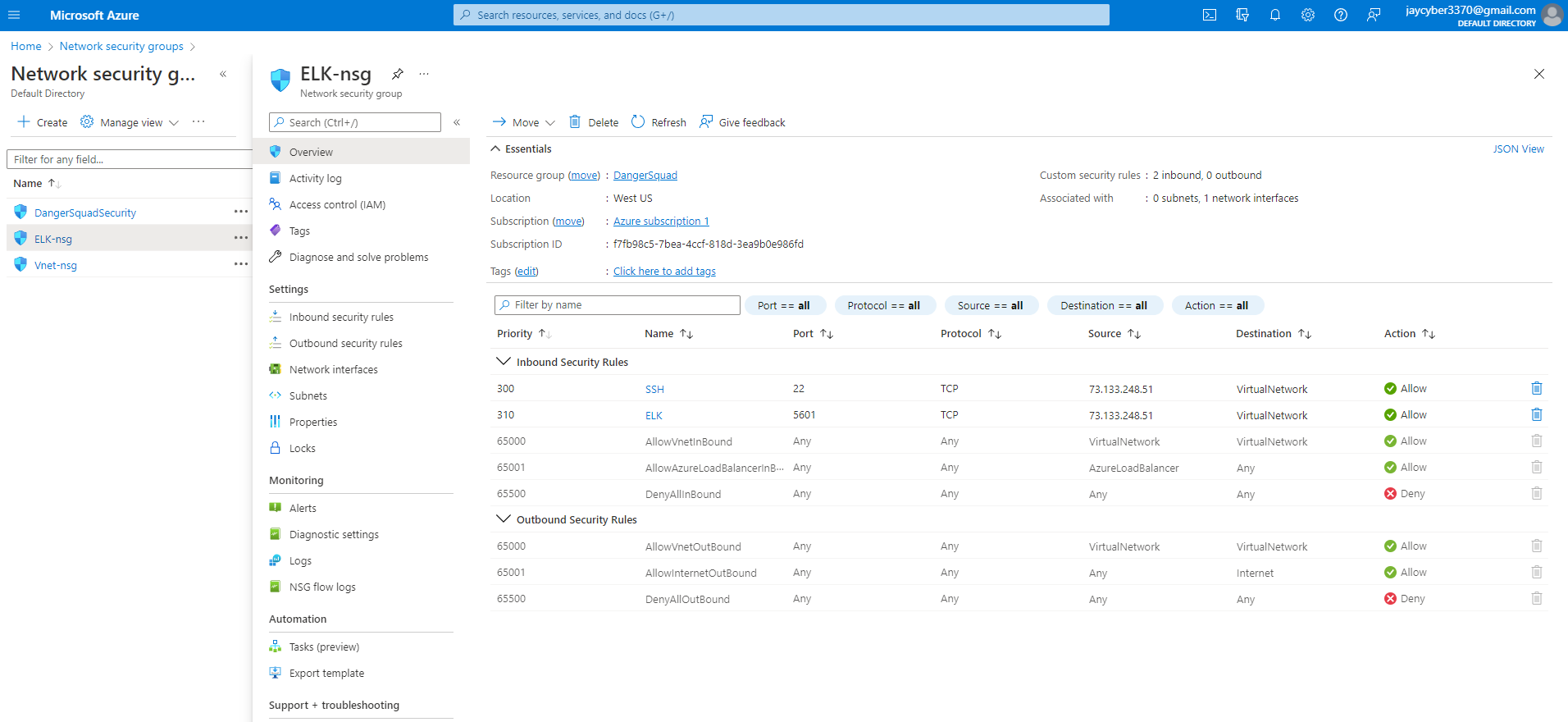


Then we will make sure that our ELK container is installed and that the elk-docker container is running

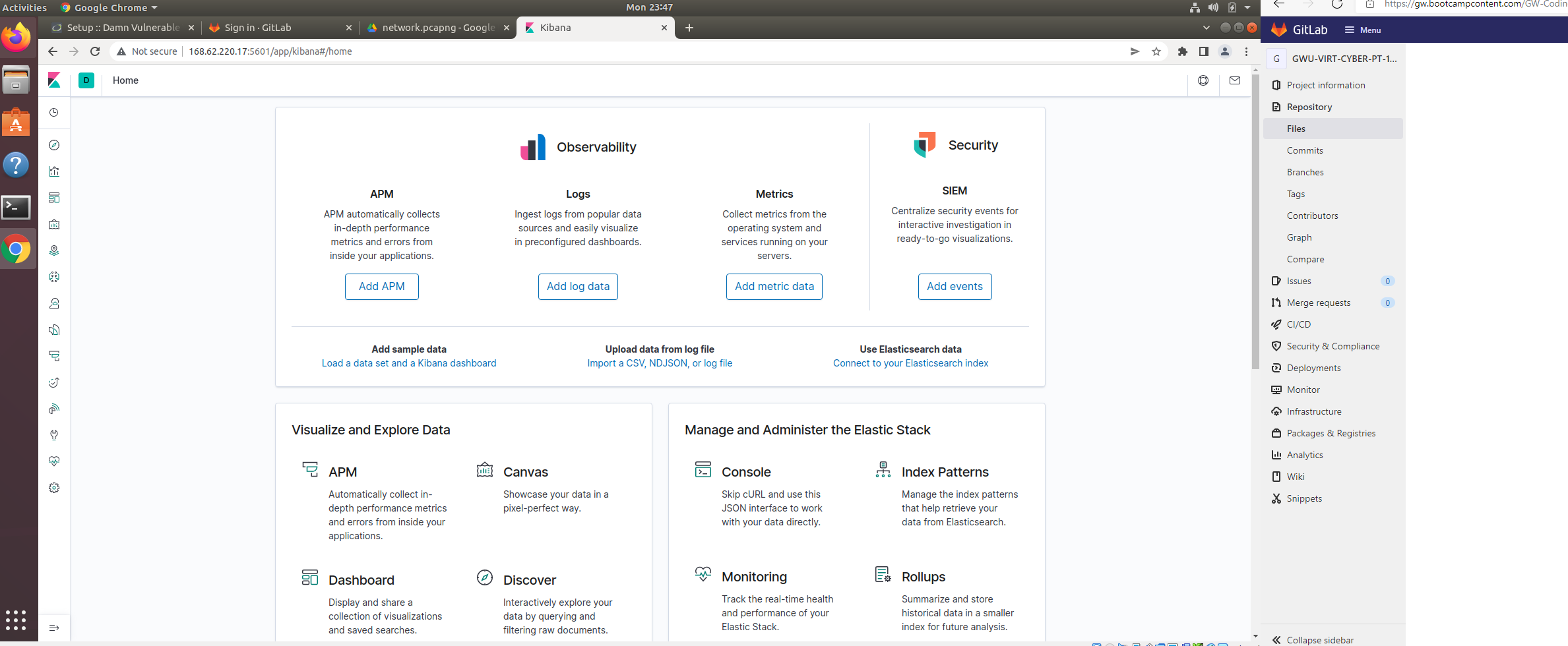


1. *We will establish identity and Access Management for our ELK web server*

We will make sure that our ELK server is running on port 5601 and we will create an incoming rule for our security group to allow TCP traffic over port 5601 from our IP address.



Then we will obtain the following Kibana environment after launching the traffic to the ELK server by changing the Virtual Network to the IP of our ELK server:

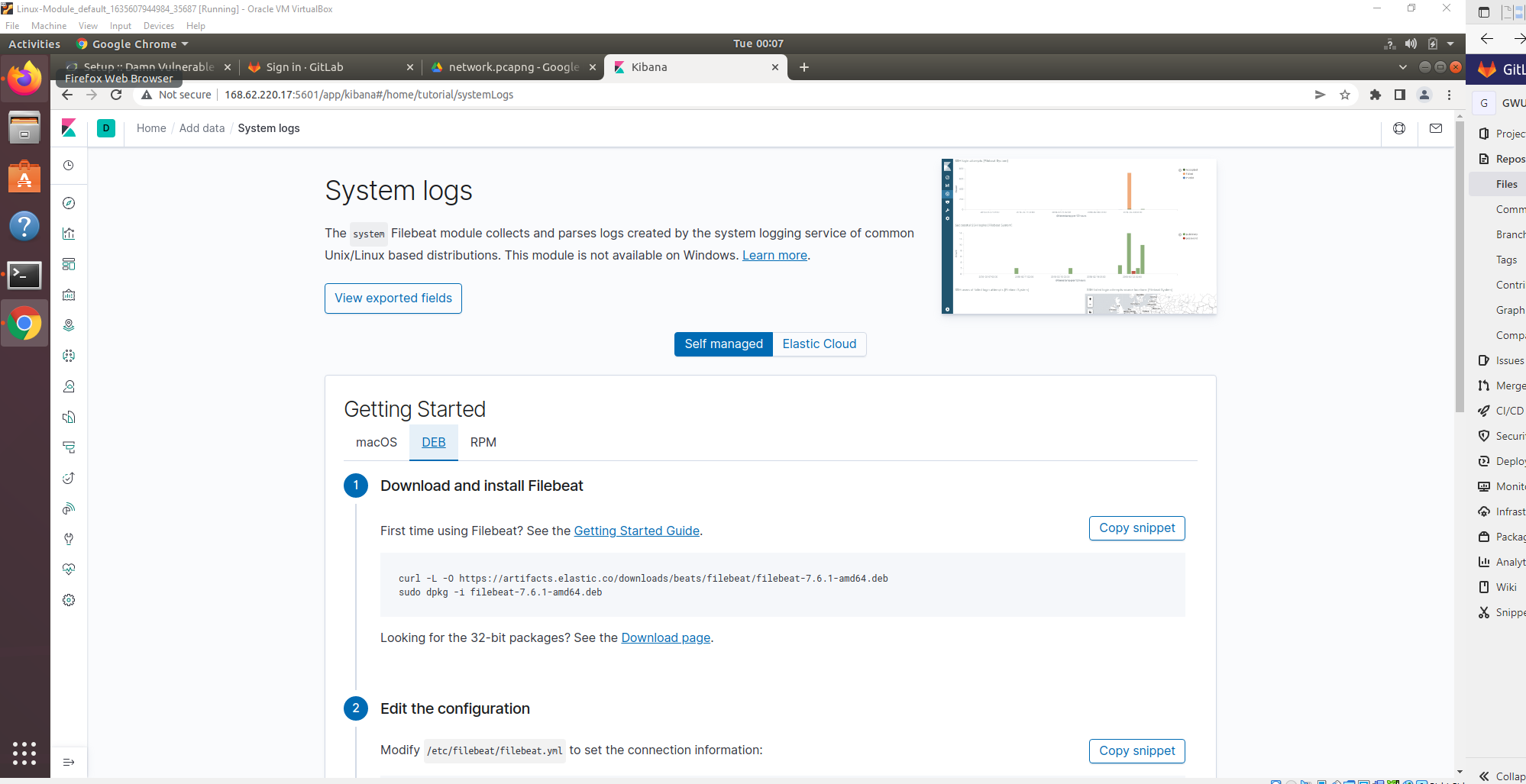


**II.2. Installing Filebeat and Metricbeat in our new ELK monitoring server**

**II.2.1 Installing Filebeat**

1. *We will install filebeat on the DVWA container*

After successfully installing the ELK monitoring server environment, we will check on the status of the filebeat configuration log download file:

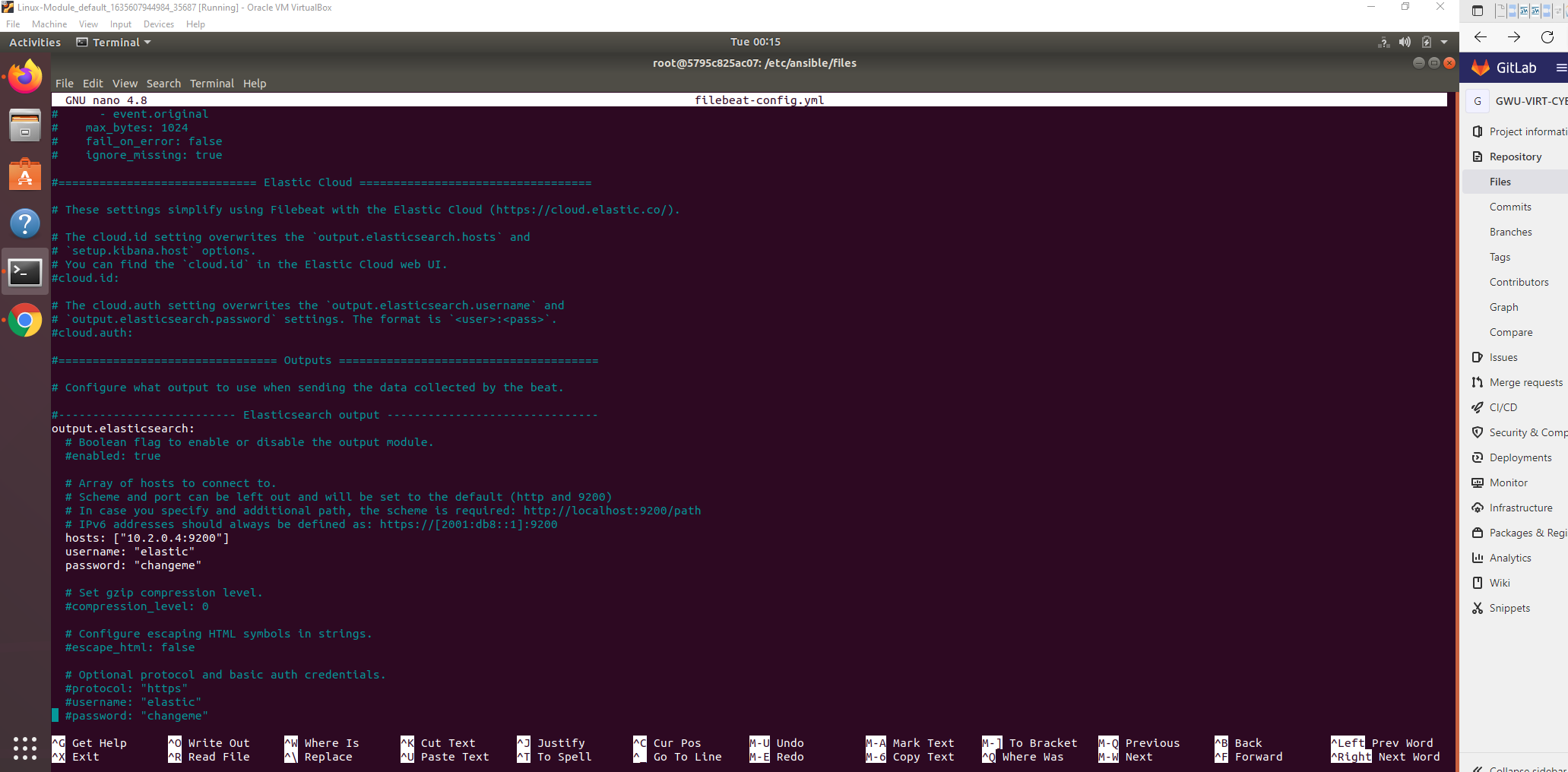


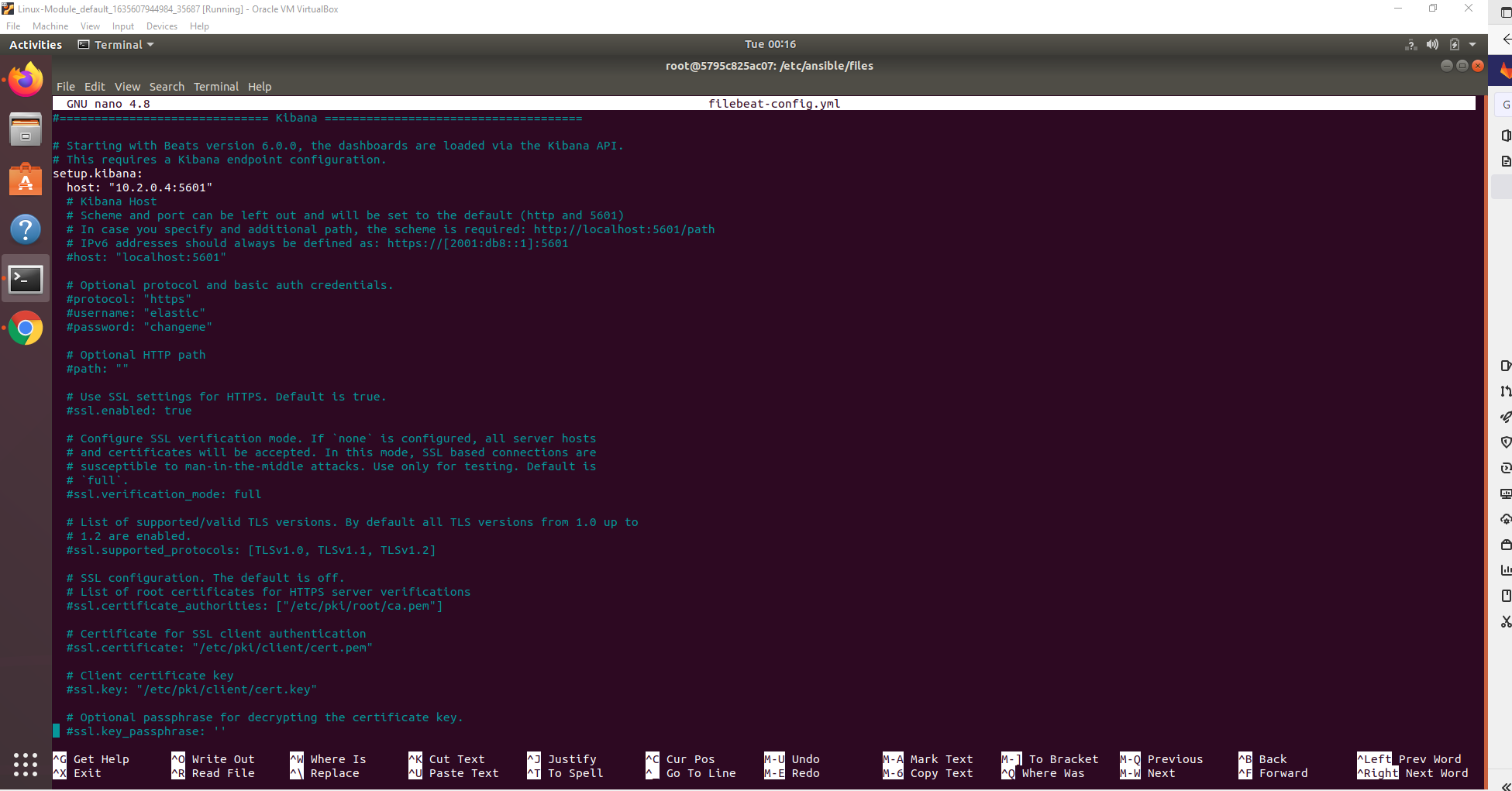
1. *We will create the Filebeat configuration File*

We will then run the following curl command to download the configuration file in our ansible container:

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

We will then update the obtained Filebeat configuration file to look like this:



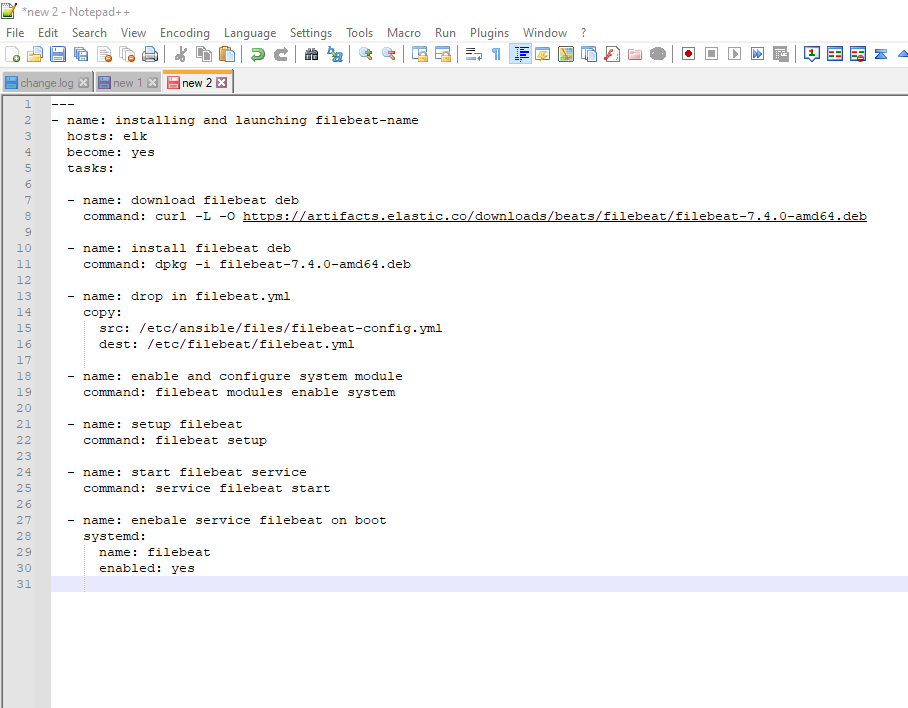


Then we will save that new configuration file under the following path:

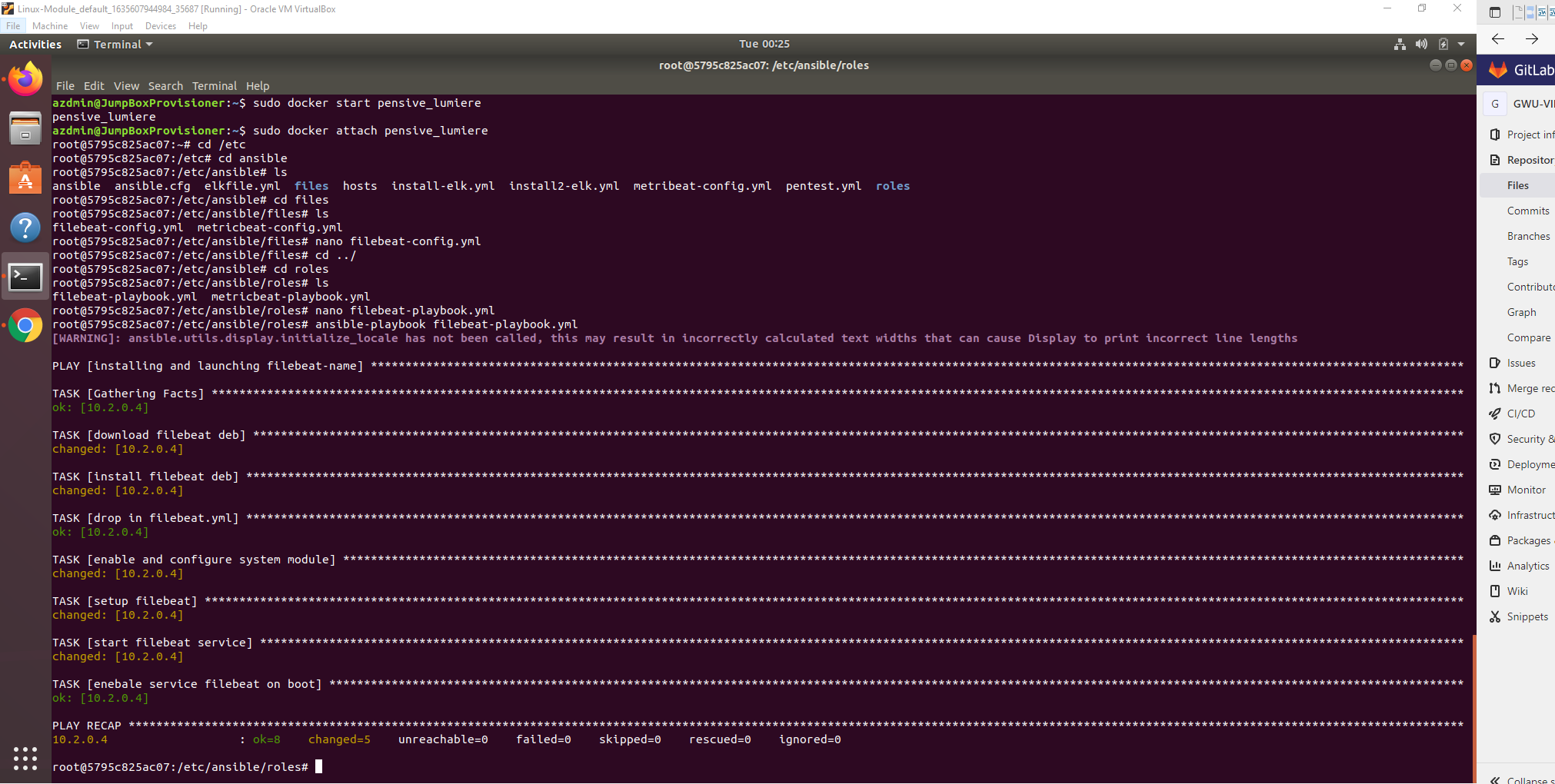
/etc/ansible/files/filebeat-config.yml.

1. *We will create the Filebeat installation playbook*

Our Installation playbook will look like this:

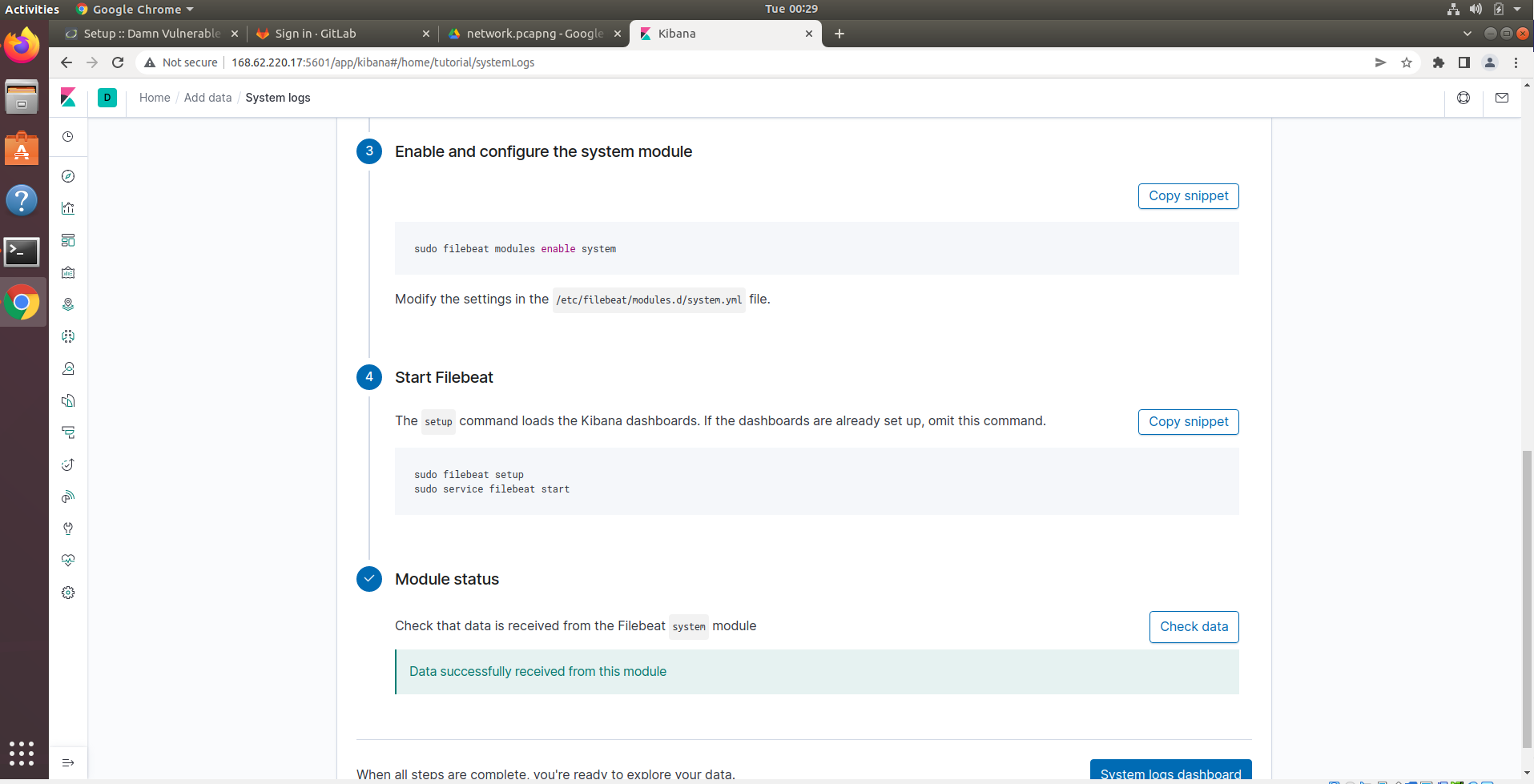


As we successfully run our playbook, we will come to the following results:



1. *We will then verify the successful installation of our Filebeat inside the ELK server monitoring environment*

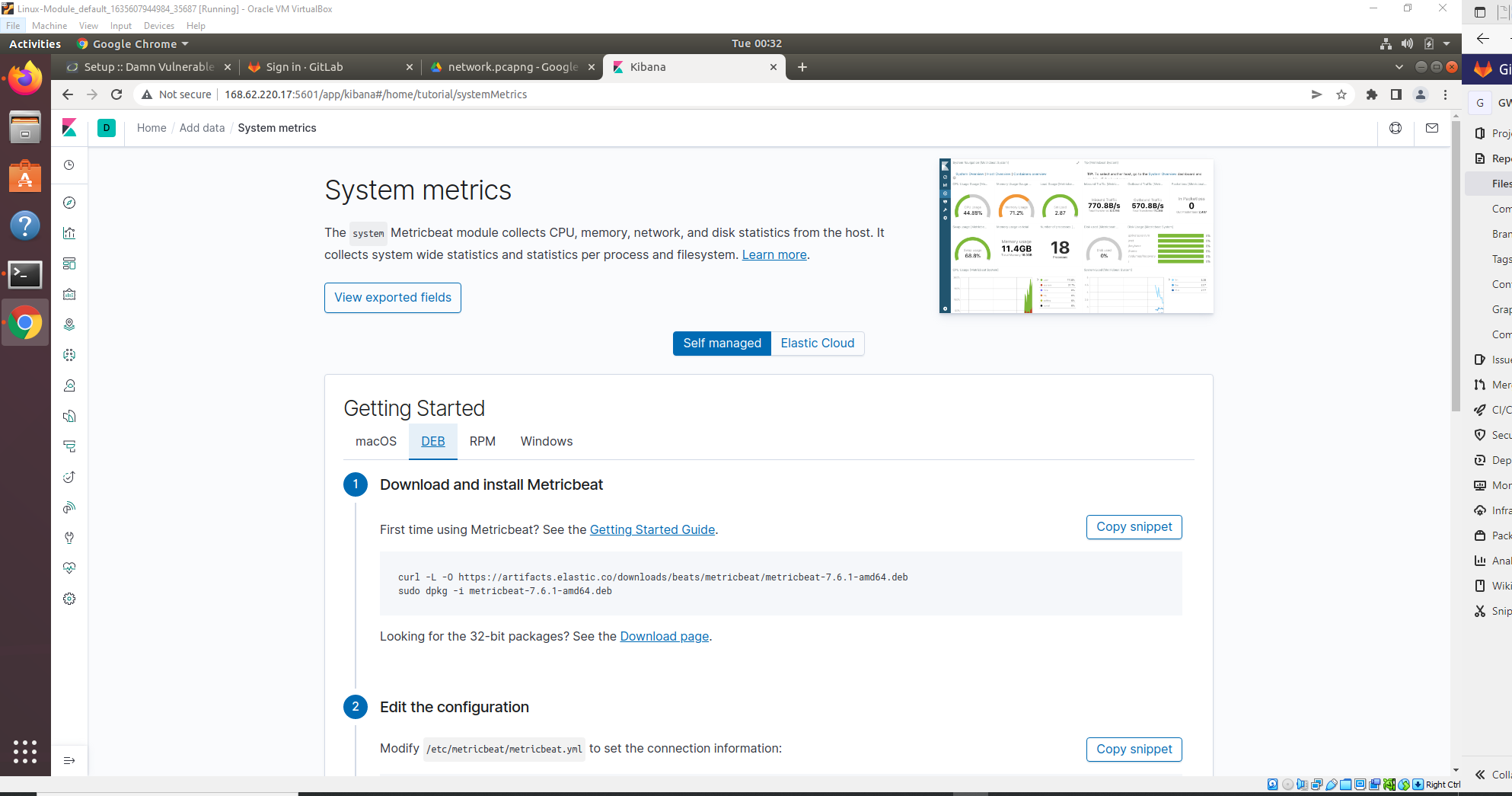
*We* will verify by checking that the logs are successfully received



**II.2.2 Installing Metricbeat**

*a) We will install Metricbeat on the DVWA container*

After successfully installing the ELK monitoring server environment, we will check on the status of the Metricbeat configuration log download file:



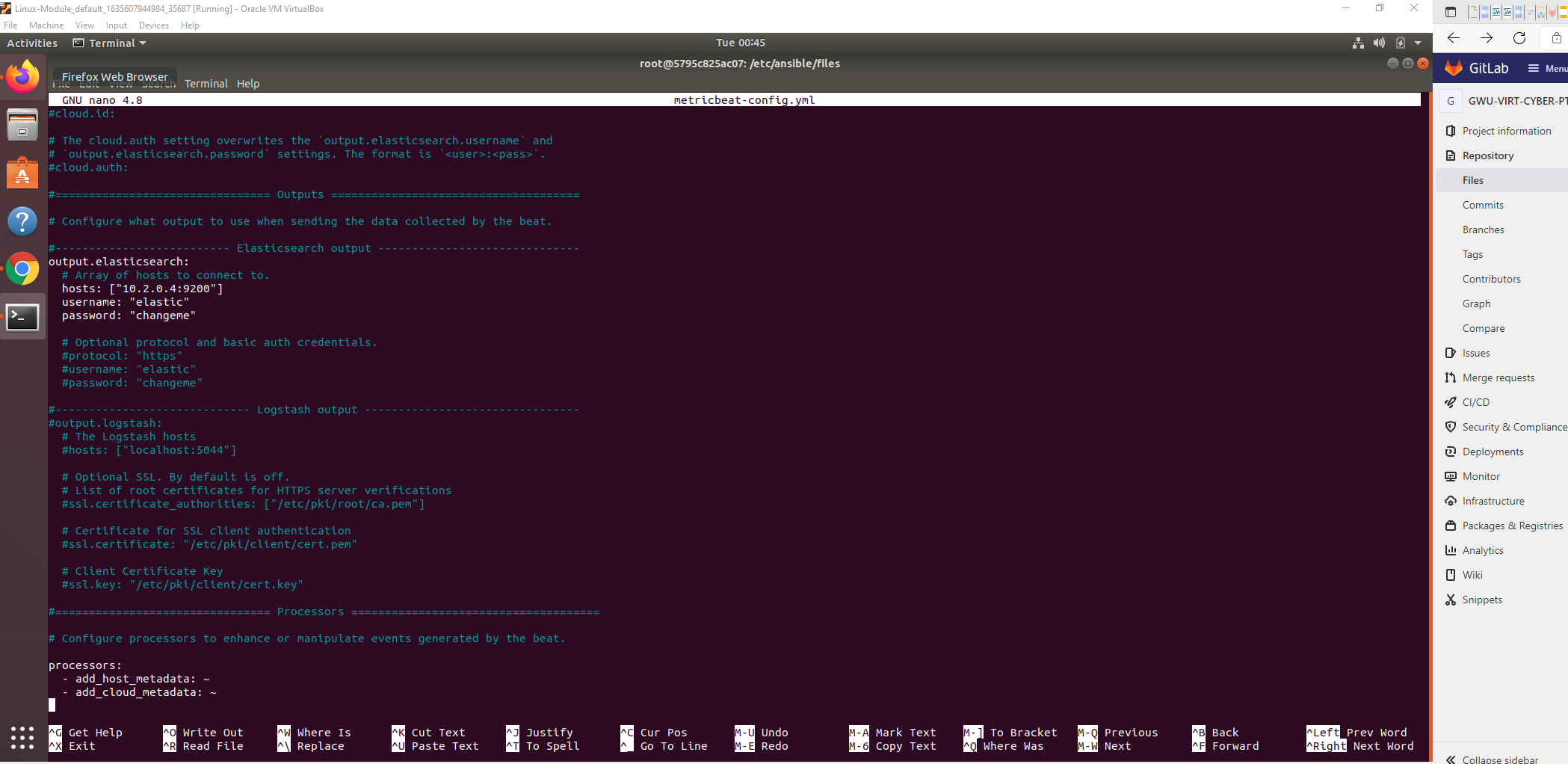
1. *We will create the Metricbeat configuration File*

We will then run the following curl command to download the configuration file in our ansible container:

Curl https://gist.githubusercontent.com/slape/58541585cc1886d2e26cd8be557ce04c/raw/0ce2c7e744c54513616966affb5e9d96f5e12f73/metricbeat>> /etc/ansible/metricbeat-config.yml

We will then update the obtained Metricbeat configuration file to look like this:



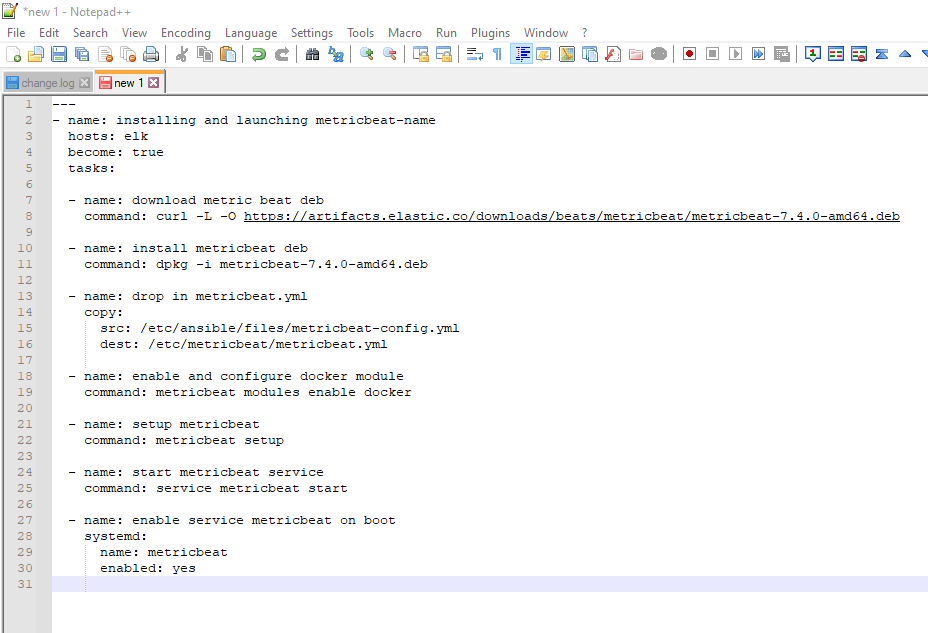


Then we will save that new configuration file under the following path:

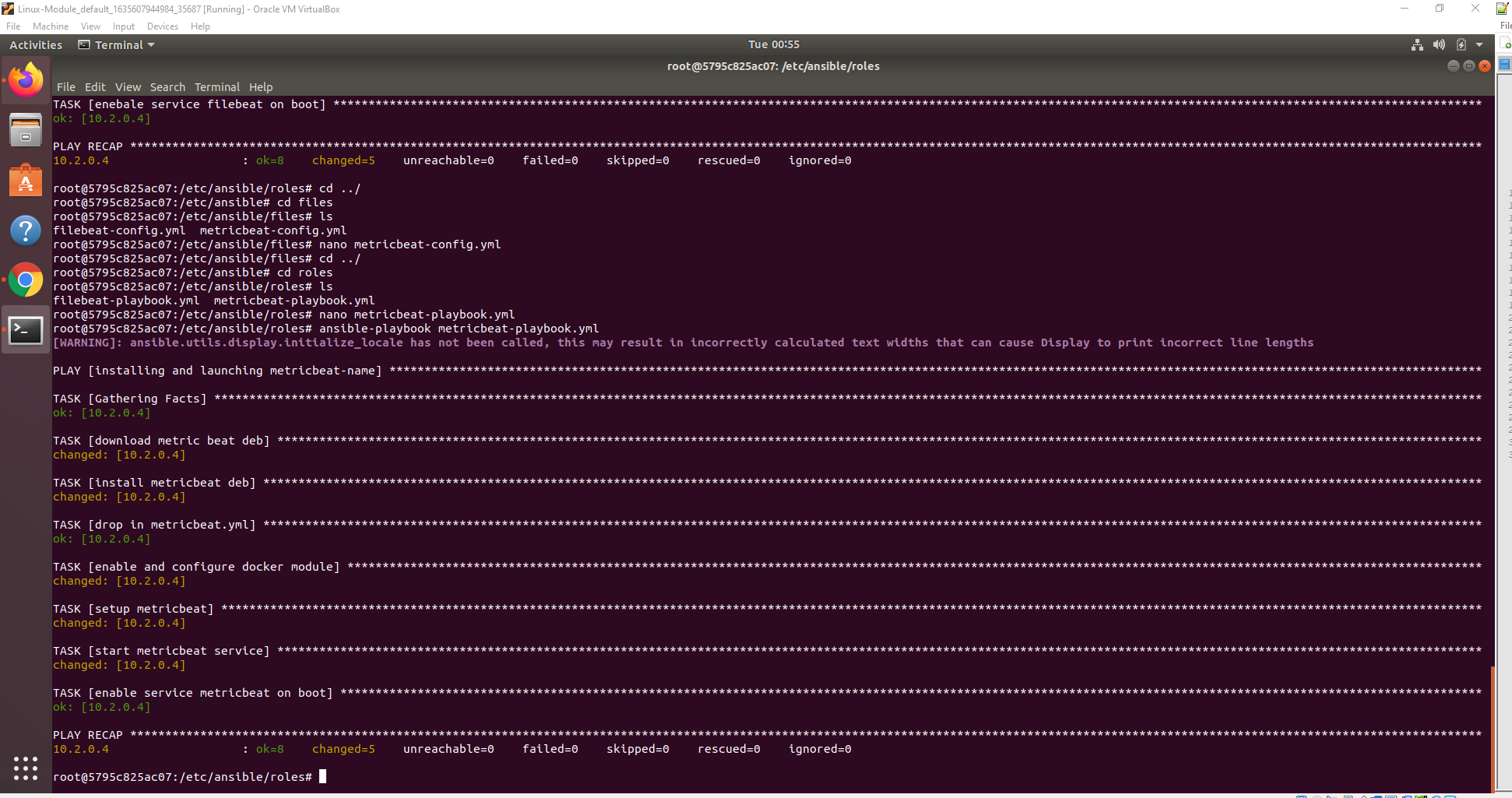
/etc/ansible/files/metricbeat-config.yml.

1. *We will create the Metricbeat installation playbook*

Our Installation playbook will look like this:

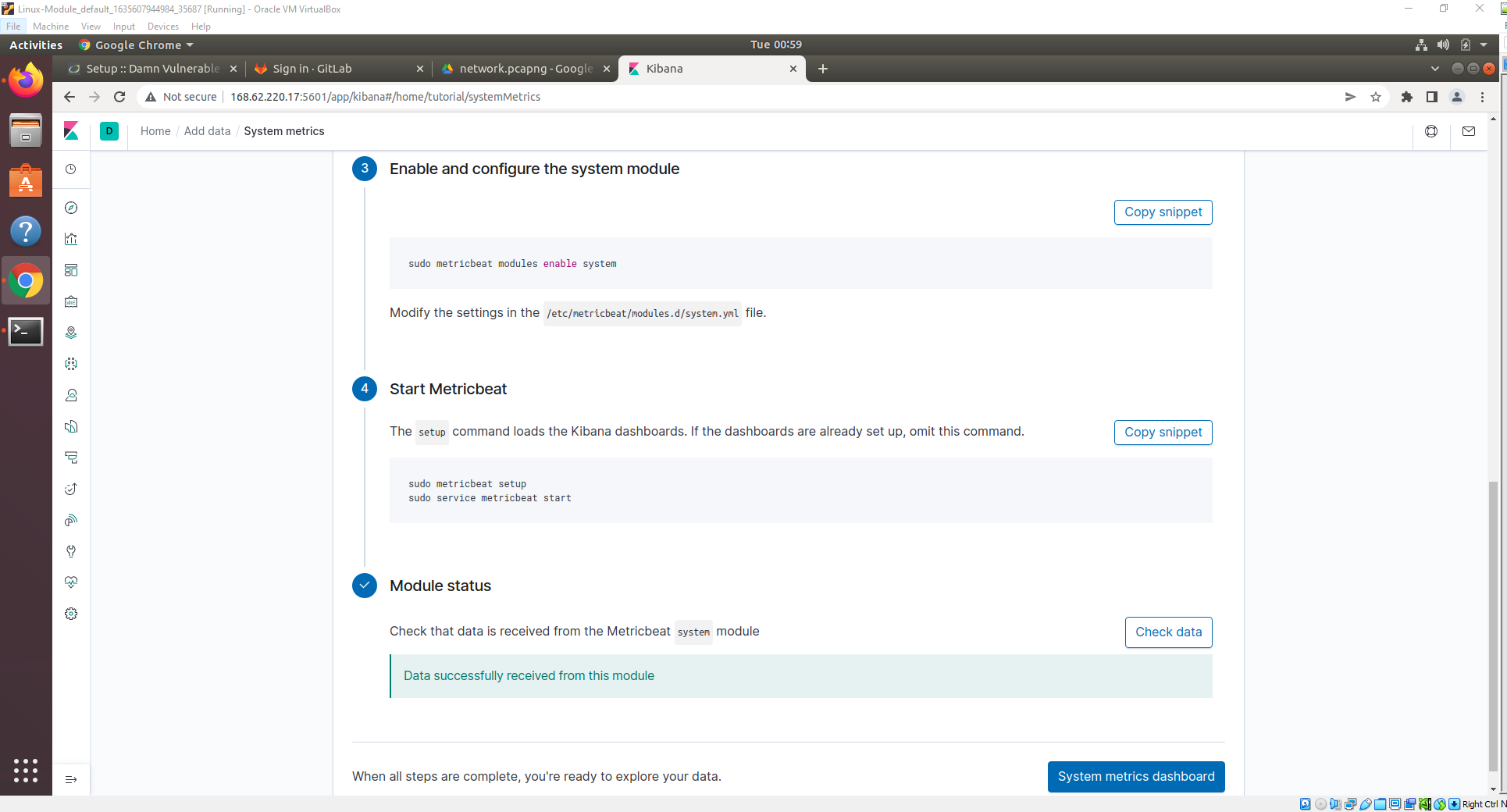


As we successfully run our playbook, we will come to the following results:



1. *We will then verify the successful installation of our Metricbeat inside the ELK server monitoring environment*

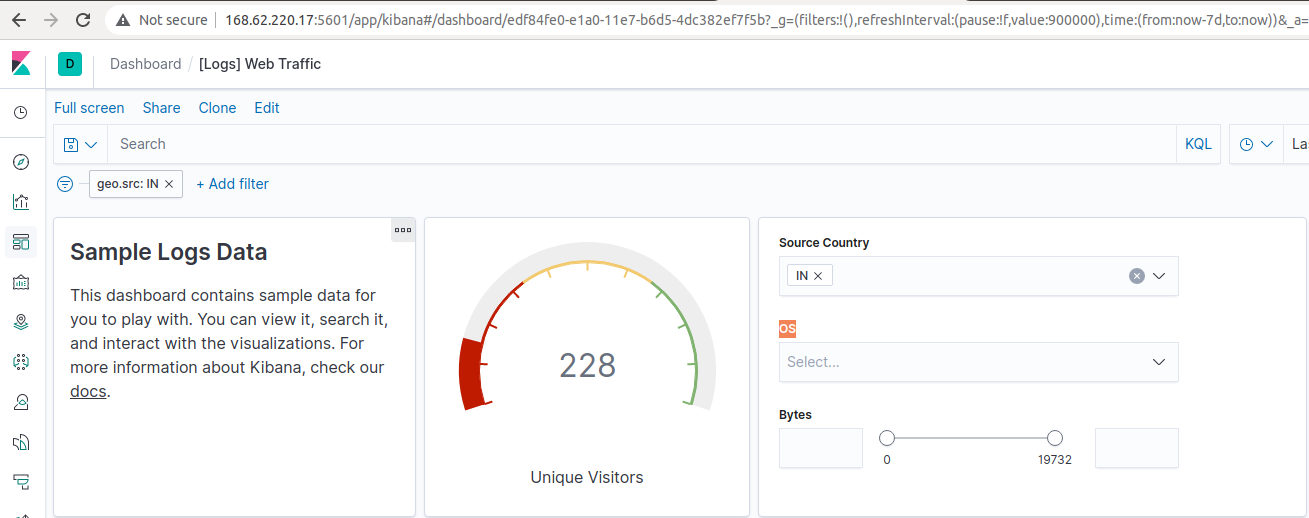
*We* will verify by checking that the logs are successfully received



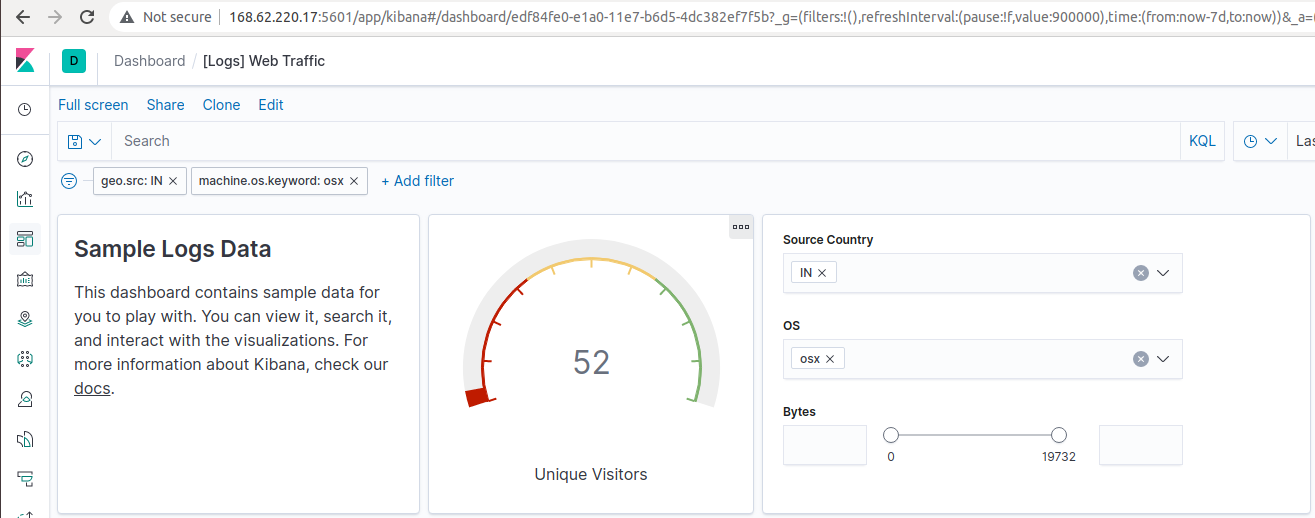
**II.3. Setting up Metrics and Logs orientation**

**II.3.1 Exploring Kibana**

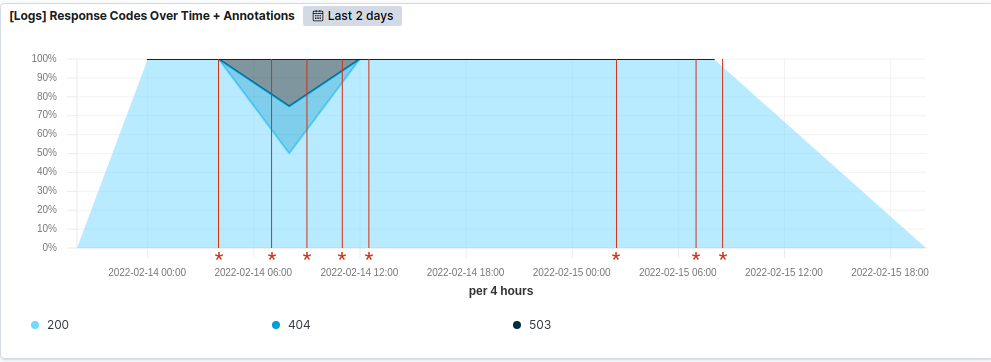
1. Unique visitors located in India: 228



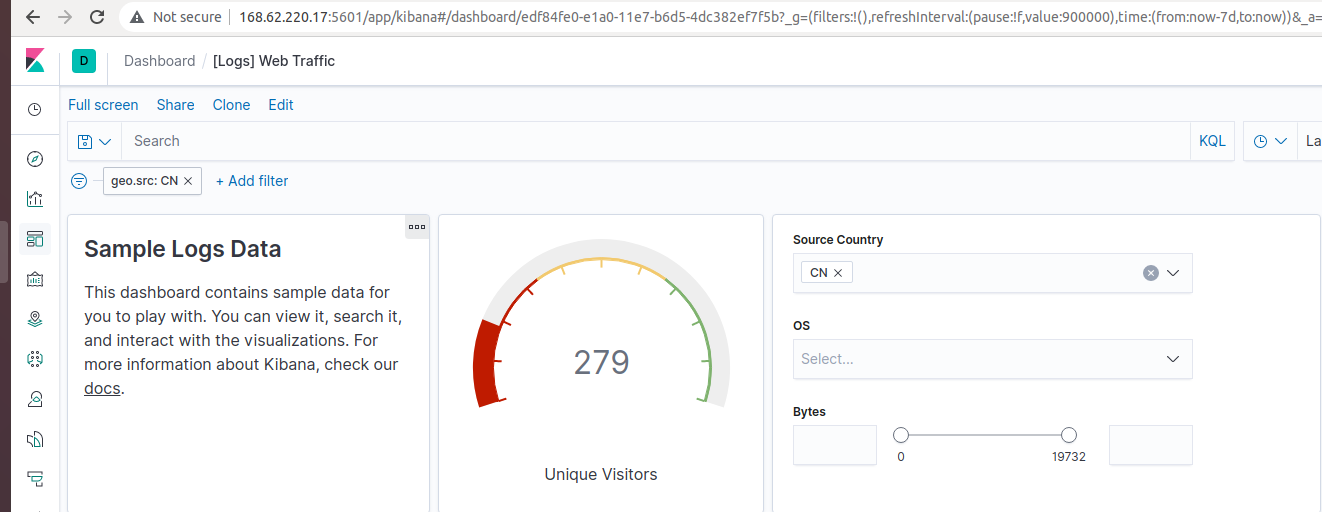
1. In the last 24 hours of the visitors in China, 52 were using Mac OSX



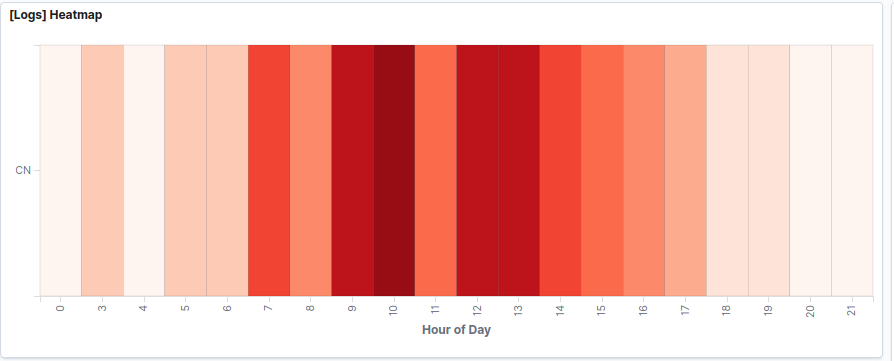
1. In the last 2 days, what percentage of visitors received 404 errors? 25% How about 503 errors? 25%



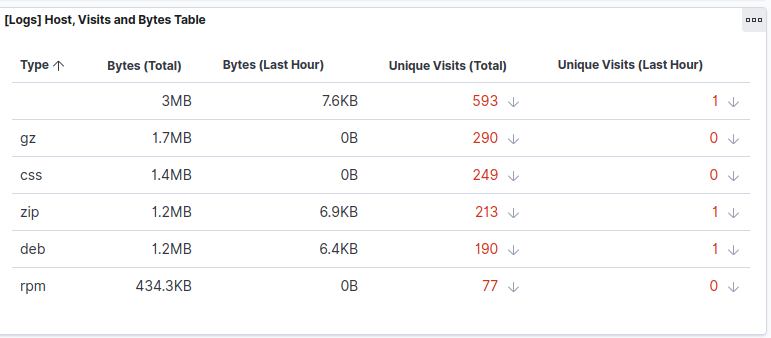
d. In the last 7 days, what country produced the majority of the traffic on the website? China: 279

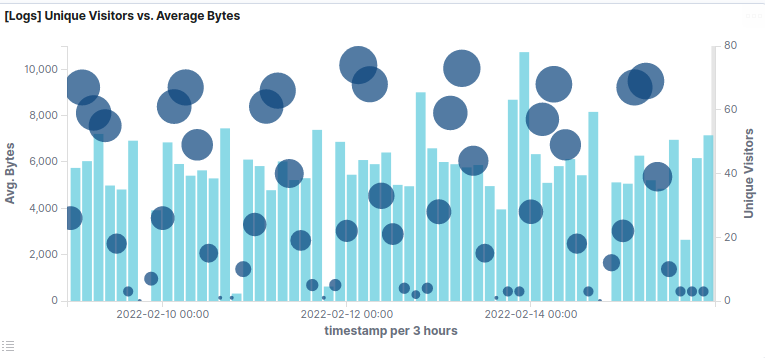


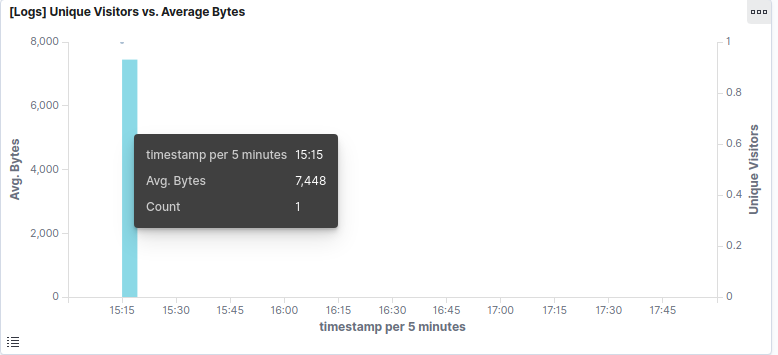
e. Of the traffic that's coming from that country, what time of day had the highest amount of activity? 12pm and 1pm China: 34

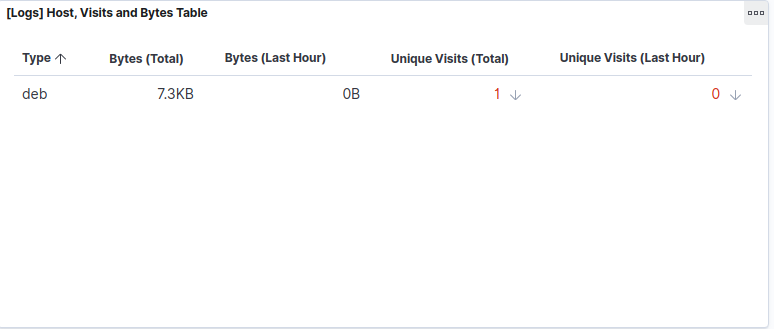


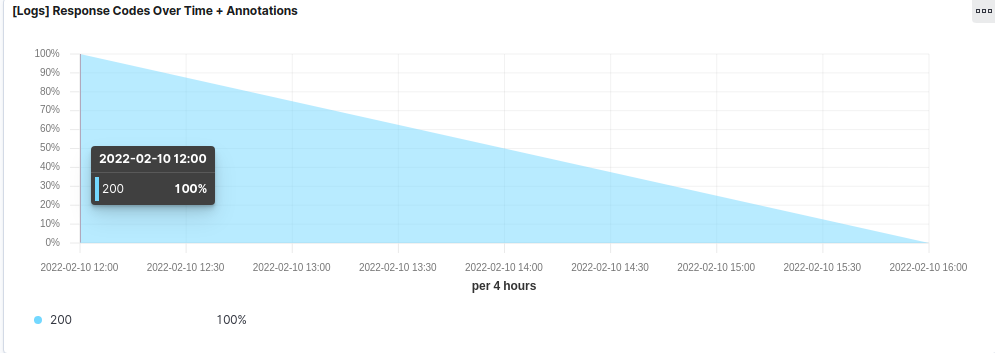
f. List all the types of downloaded files that have been identified for the last 7 days, along with a short description of each file type (use Google if you aren't sure about a particular file type).

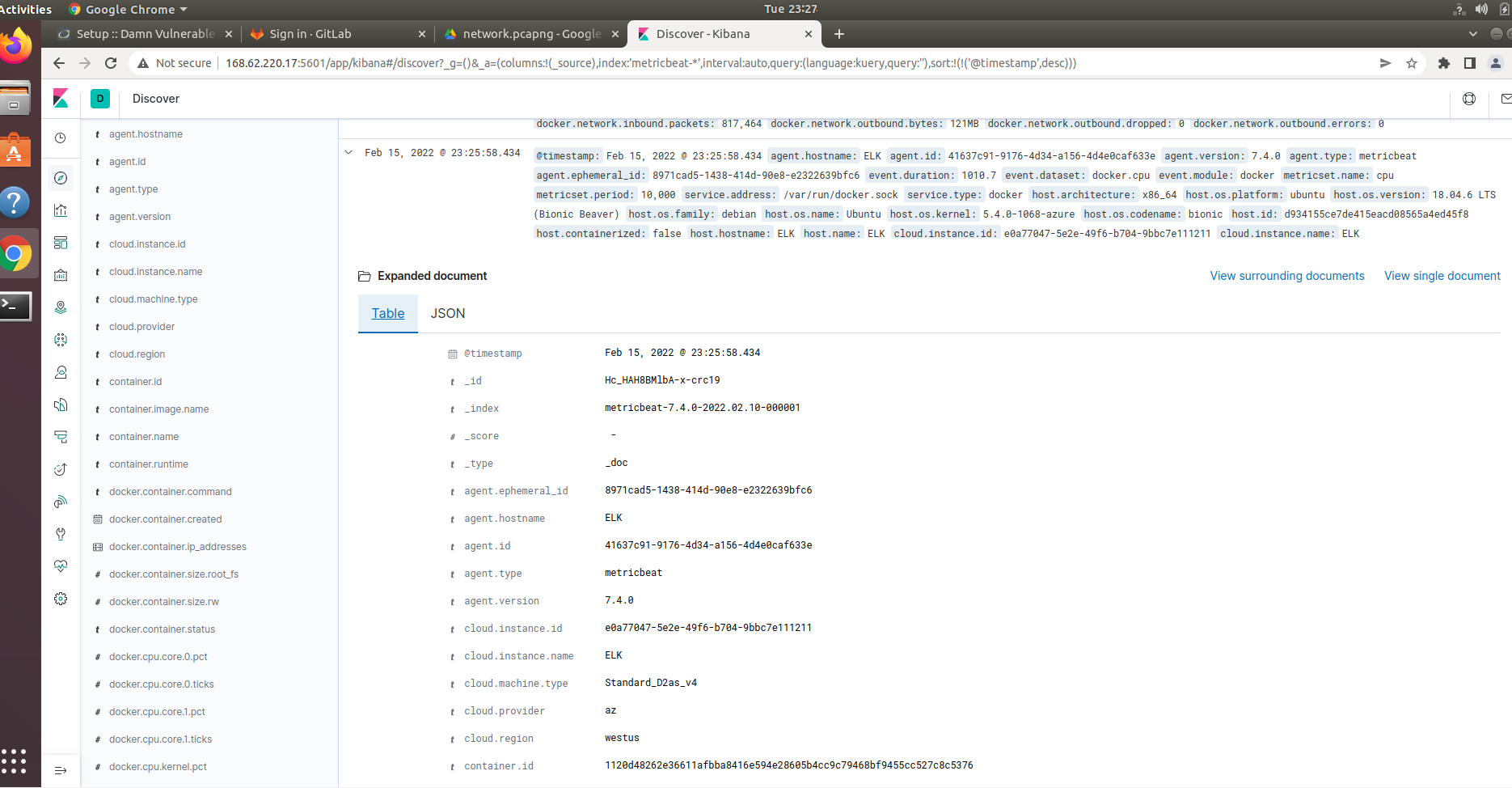






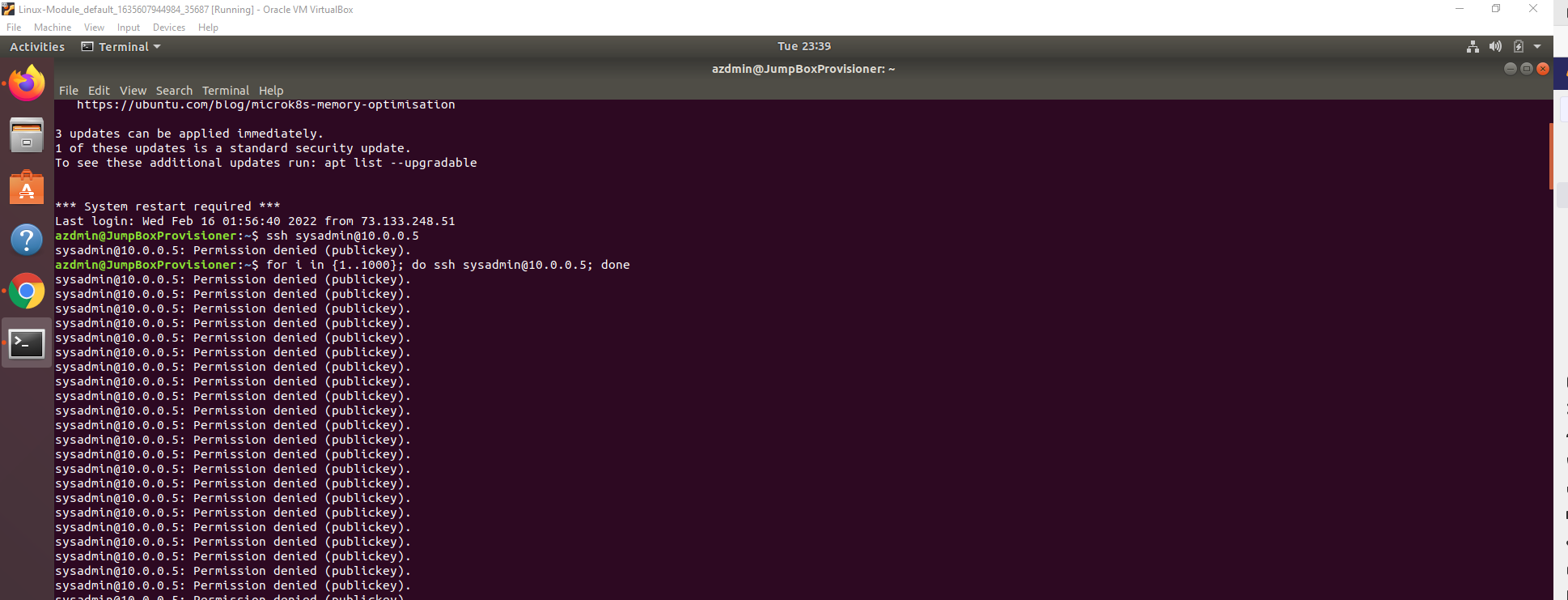


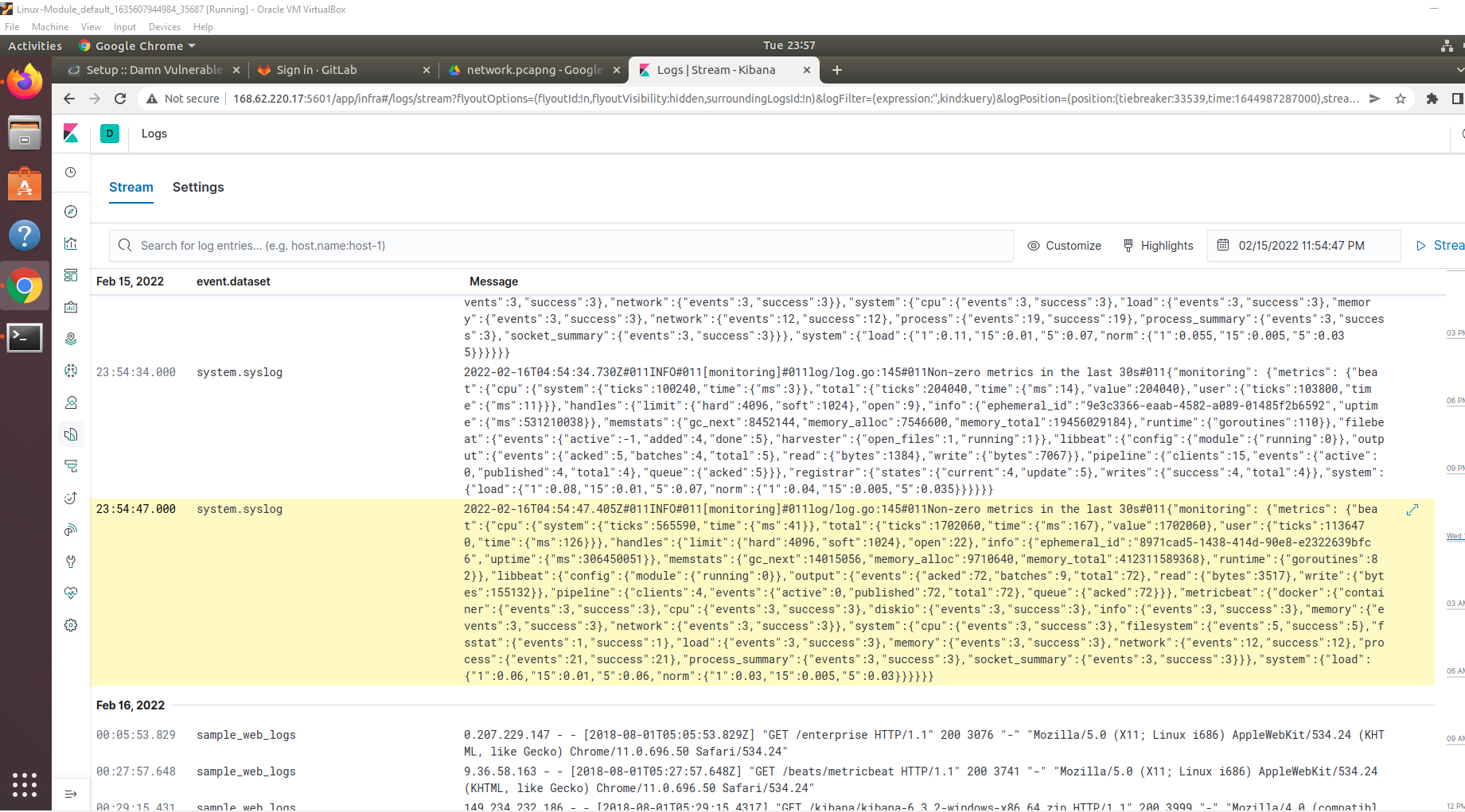




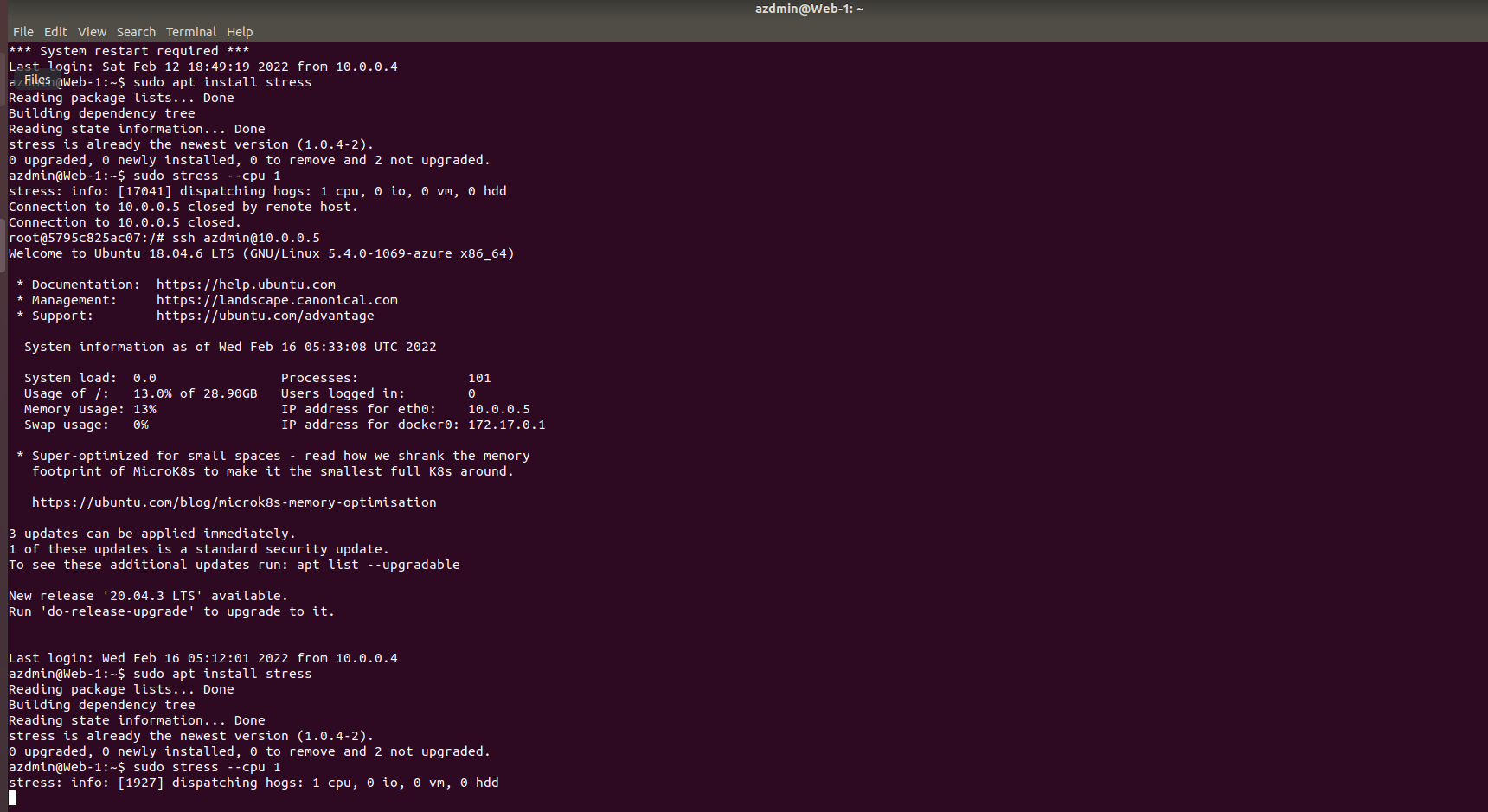
**II.3.2 Kibana Continued**

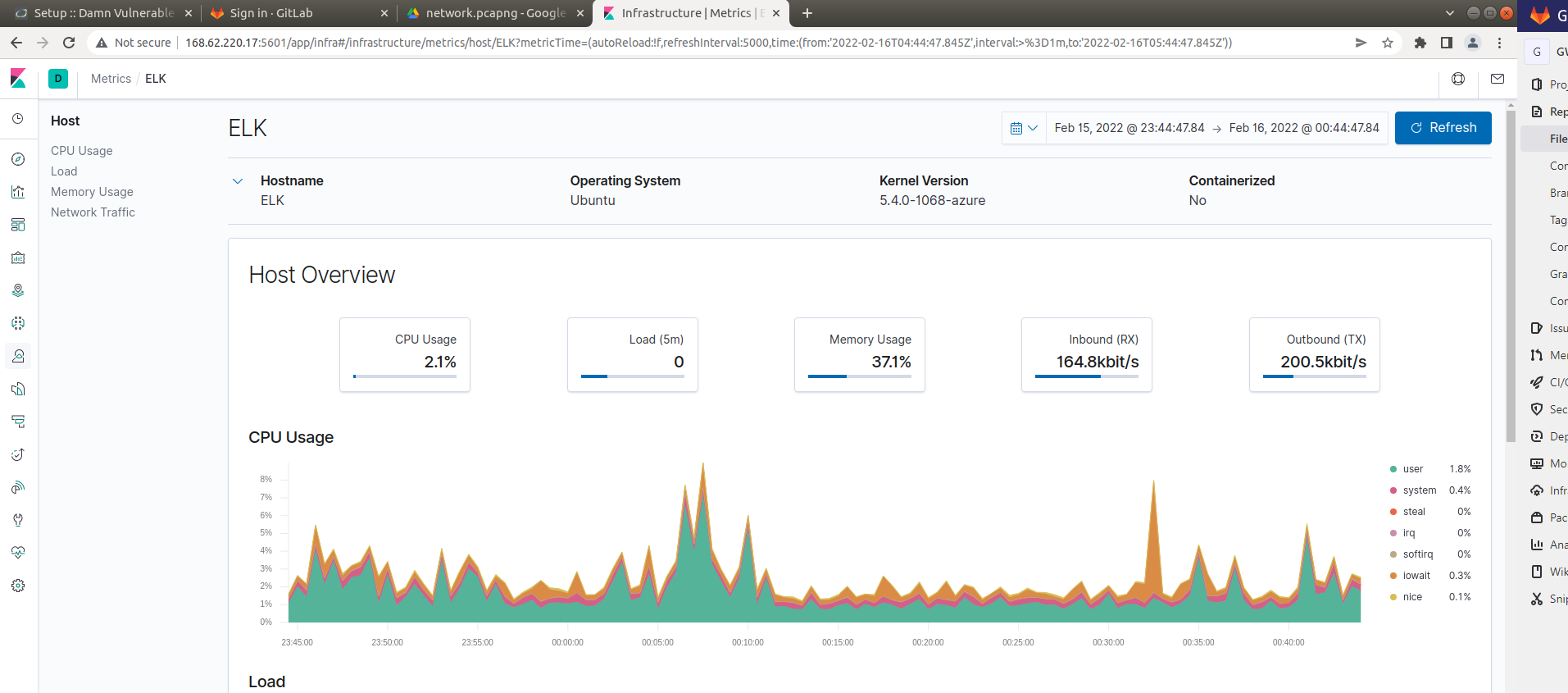
1. Generate a high amount of failed SSH login attempts and verify that Kibana is picking up this activity

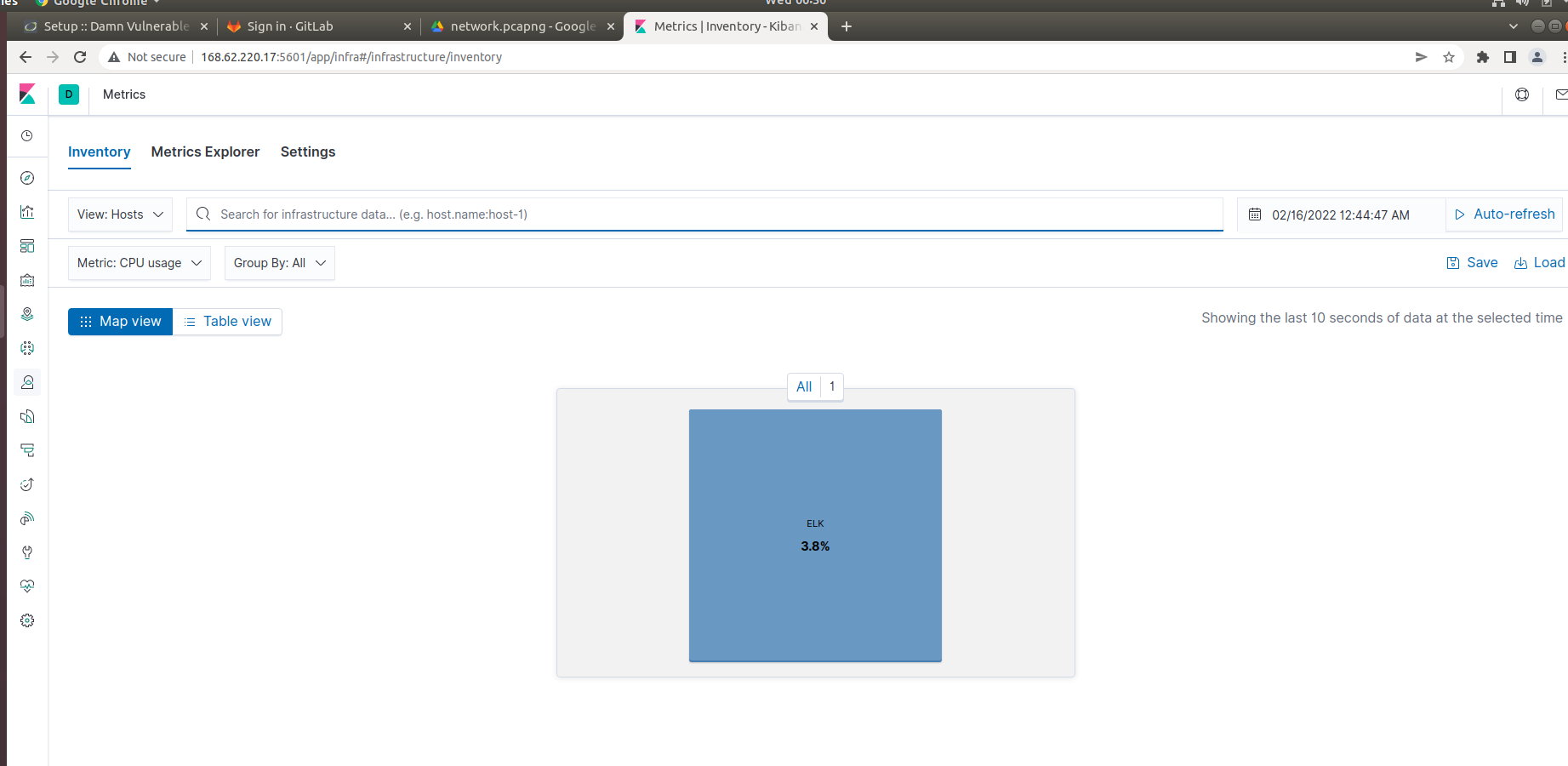




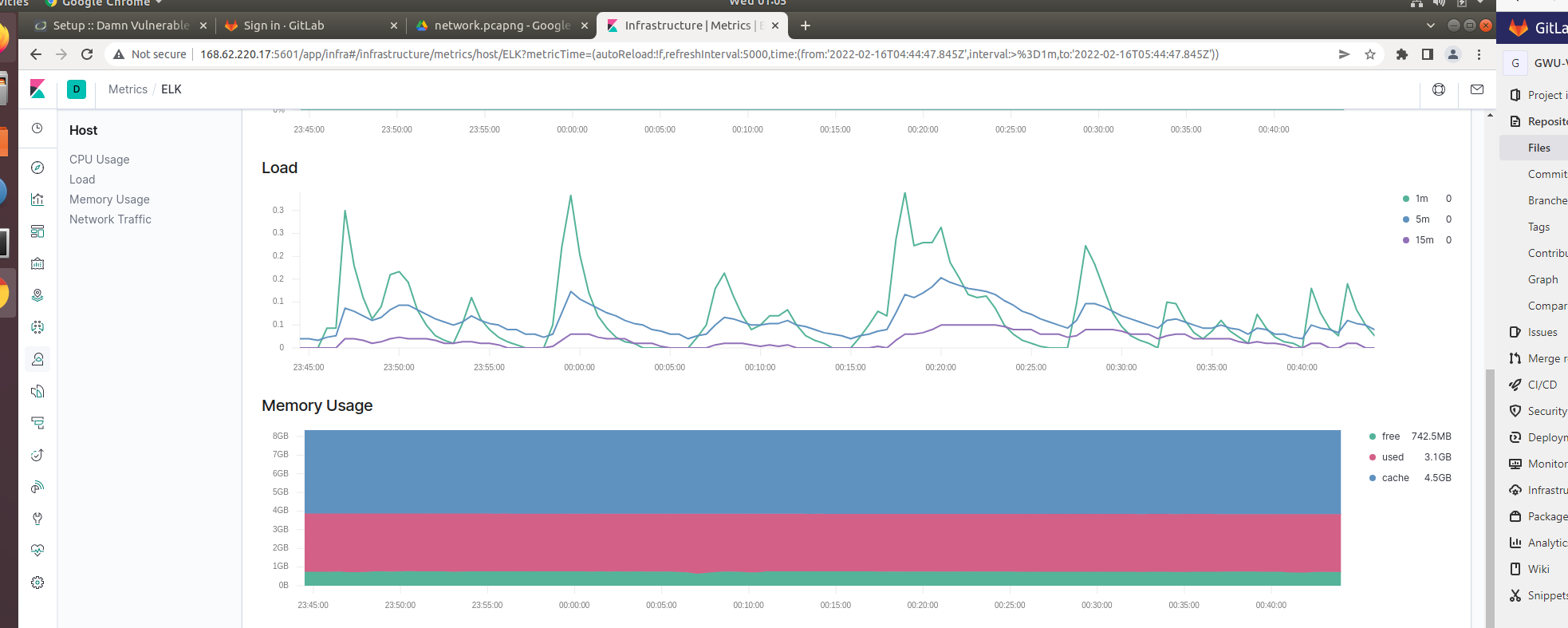
1. Generate a high amount of CPU usage on the pen-testing machines and verify that Kibana picks up this data

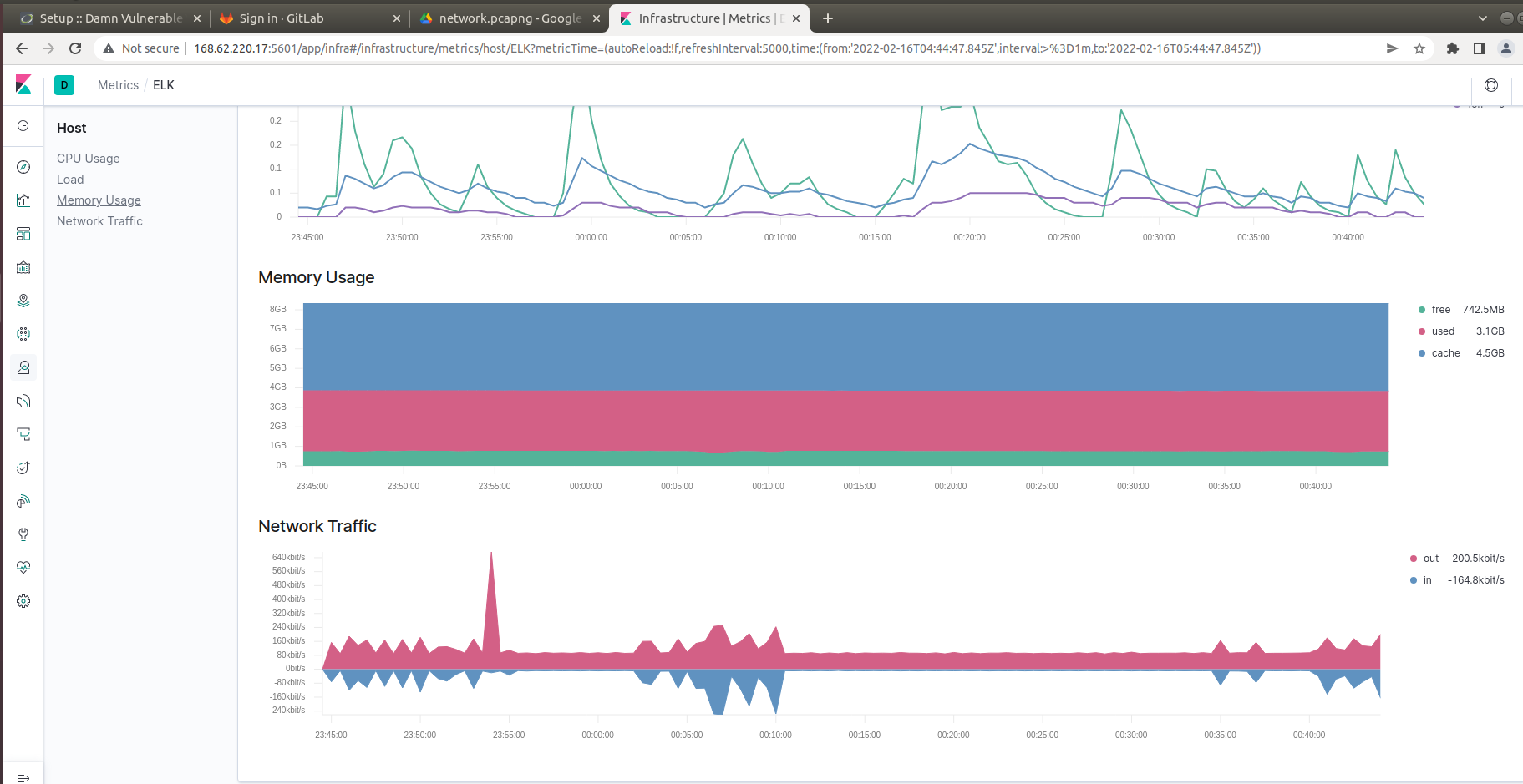






1. Generate a high amount of web requests to your pen-testing servers and make sure that Kibana is picking them up.





1. **Project Closure**

We were able to successfully deploy our elk server monitoring environment within the Azure cloud infrastructure using Ansible and docker containers that automated the entire system. Therefore, we are able to all the monitoring and tacking operations within the Kibana front end systems. The network topology and diagram below will illustrate the blueprint of our environment

