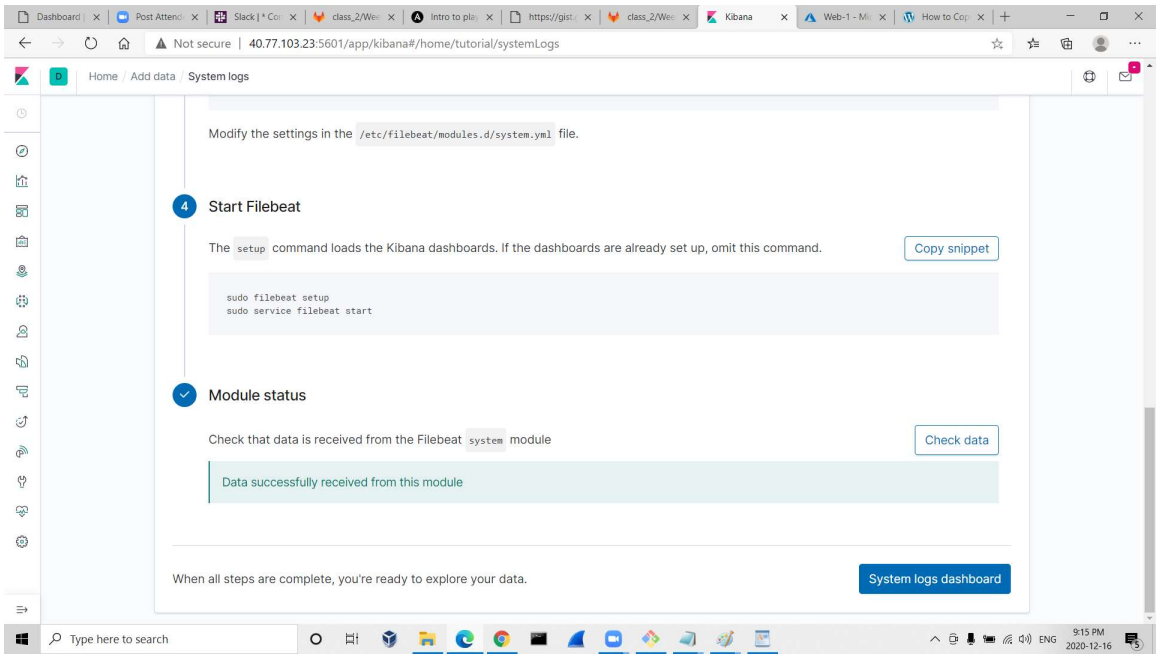
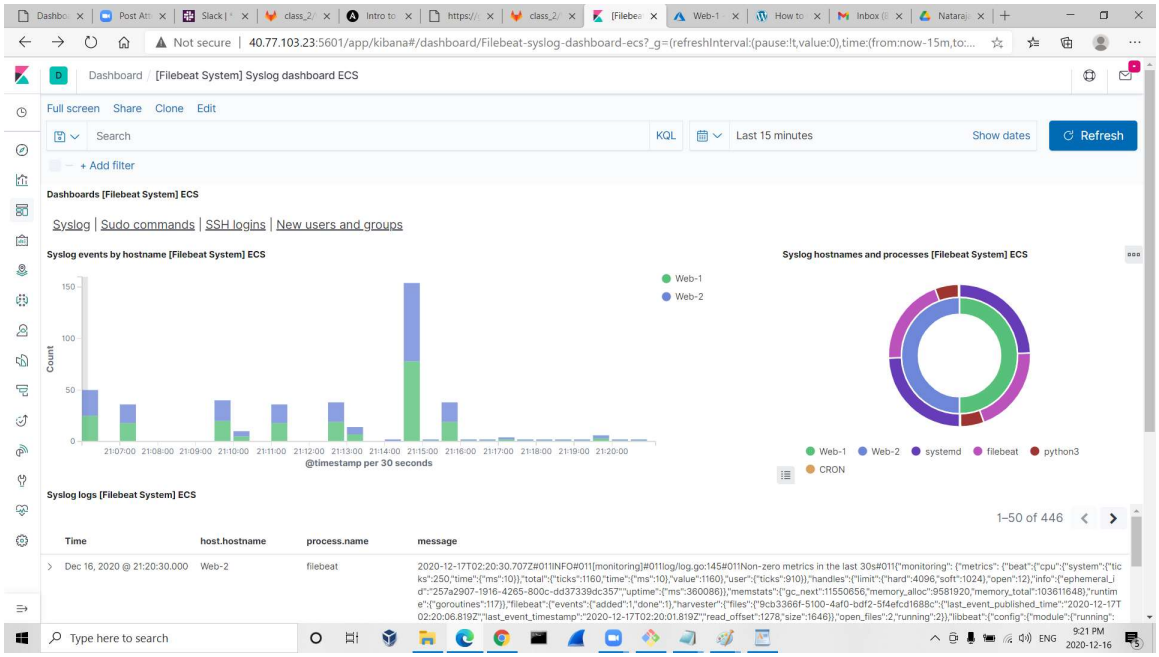
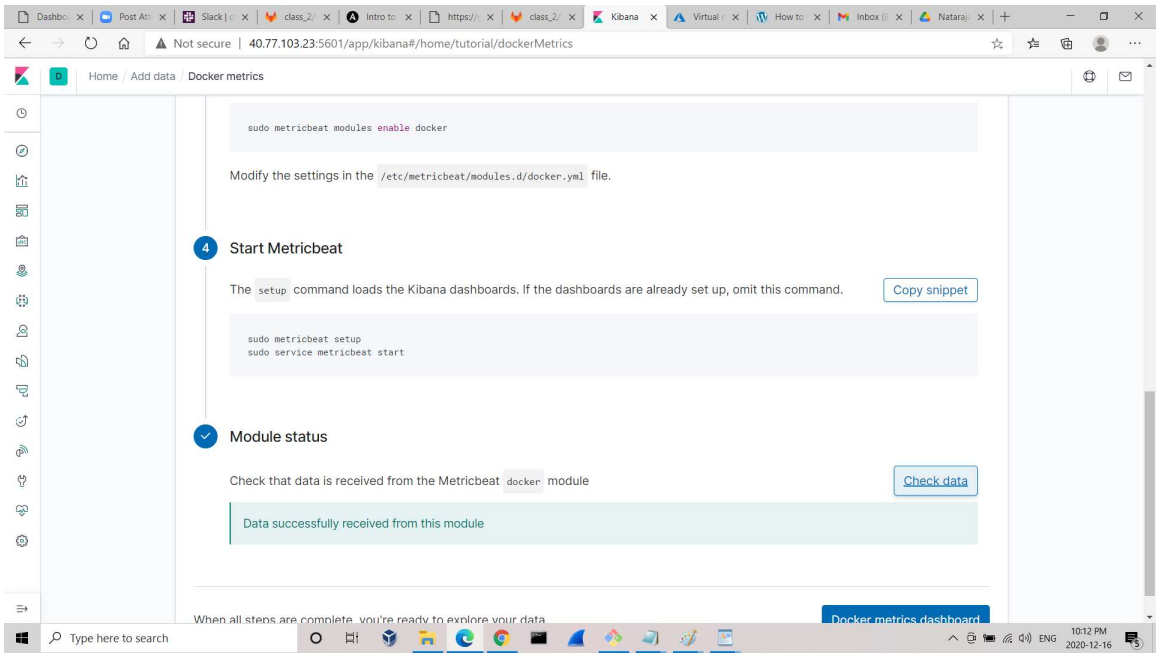
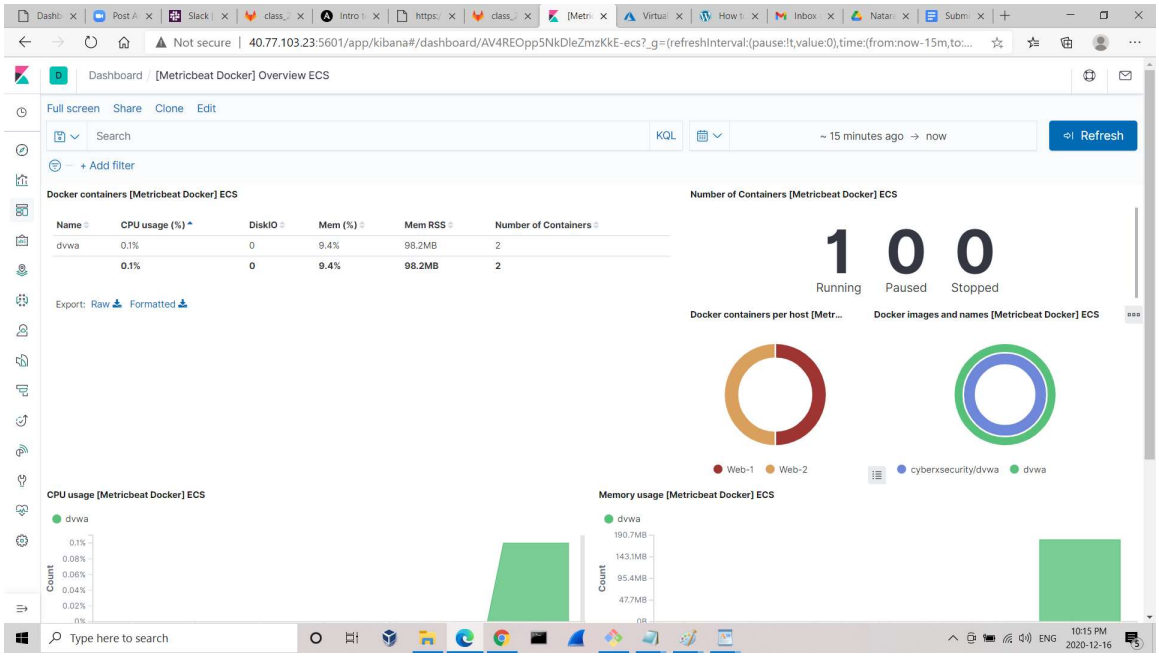

Not secure | 40.77.103.23:5601/app/kibana#/home/tutorial/systemLogs
Home / Add data / System logs
Modify the settings in the /etc/filebeat/modules.d/system.yml file.
4 Start Filebeat
The setup command loads the Kibana dashboards. If the dashboards are already set up, omit this command.
Copy snippet
sudo filebeat setup
sudo service filebeat start
Module status
Check that data is received from the Filebeat system module
Check data
Data successfully received from this module
When all steps are complete, you're ready to explore your data.
System logs dashboard
Type here to search
9:15 PM
2020-12-16


Not secure | 40.77.103.23:5601/app/kibana#/dashboard/Filebeat-syslog-dashboard-ecs?_g=(refreshInterval:(pause:!t,value:0),time:(from:now-15m,to:...
Dashboard / [Filebeat System] Syslog dashboard ECS
Full screen Share Clone Edit
Search KQL Last 15 minutes Show dates Refresh
+ Add filter
Dashboards [Filebeat System] ECS
Syslog | Sudo commands | SSH logins | New users and groups
Syslog events by hostname [Filebeat System] ECS
Web-1
Web-2
Count
@timestamp per 30 seconds
Syslog hostnames and processes [Filebeat System] ECS
Web-1 Web-2 systemd filebeat python3
CRON
Syslog logs [Filebeat System] ECS
1–50 of 446
Time host.hostname process.name message
Dec 16, 2020 @ 21:20:30.000 Web-2 filebeat
Type here to search
9:21 PM
2020-12-16


Not secure | 40.77.103.23:5601/app/kibana#/home/tutorial/dockerMetrics
Home / Add data / Docker metrics
sudo metricbeat modules enable docker
Modify the settings in the /etc/metricbeat/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
sudo metricbeat setup
sudo service metricbeat start
Module status
Check that data is received from the Metricbeat docker module
Check data
Data successfully received from this module
When all steps are complete, you're ready to explore your data.
Docker metrics dashboard
Type here to search
ENG
10:12 PM
2020-12-16


Not secure | 40.77.103.23:5601/app/kibana#/dashboard/AV4REOpp5NkDleZmzKkE-ecs?_g=(refreshInterval:(pause:!t,value:0),time:(from:now-15m,to:...
Dashboard / [Metricbeat Docker] Overview ECS
Full screen Share Clone Edit
Search
KQL
~ 15 minutes ago → now
Refresh
+ Add filter
Docker containers [Metricbeat Docker] ECS
Name CPU usage (%) DiskIO Mem (%) Mem RSS Number of Containers
dvwa 0.1% 0 9.4% 98.2MB 2
0.1% 0 9.4% 98.2MB 2
Export: Raw Formatted
Number of Containers [Metricbeat Docker] ECS
1 Running
0 Paused
0 Stopped
Docker containers per host [Metr...
Web-1 Web-2
Docker images and names [Metricbeat Docker] ECS
cyberxsecurity/dvwa dvwa
CPU usage [Metricbeat Docker] ECS
dvwa
Count
Memory usage [Metricbeat Docker] ECS
dvwa
190.7MB
143.1MB
95.4MB
47.7MB
Count
Type here to search
ENG
10:15 PM
2020-12-16