12/11/2024 Log Analysis using ELK stack

- Download or install the required file.
  - ElasticSearch : https://www.elastic.co/downloads/elasticsearch
  - Kibana : https://www.elastic.co/downloads/kibana
  - Logstash : https://www.elastic.co/downloads/logstash

- Installation and Configuration.
  - Github Repo for this Task: https://github.com/soumilshah1995/learning-logstash-and-elastic-search-plugins/blob/main/ELKStack8.3/readme.md
  - Window : https://www.youtube.com/watch?v=BybAetckH88
  - Linux : https://www.youtube.com/watch?v=oiK0JWin7i0
  - MAC : https://www.youtube.com/watch?v=DMh92_0epO0

- Working on ELS :
  - https://www.youtube.com/watch?v=nsJar753ROc&list=PLTgwj-KL1pO2I0EQu8IDbhoH1CpLIHg9d&index=1&ab_channel=Techster

Today’s Task:

➔ Install Elasticsearch and Kibana on the student's machine.
➔ Configure Elasticsearch and Kibana to ensure they are running correctly.

For Elasticsearch:

➔ Set up the necessary configuration files.
➔ Start the Elasticsearch service and verify its status.

For Kibana:

➔ Configure Kibana to connect to Elasticsearch.
➔ Start the Kibana service and ensure it's operational.

After installation

➔ Accessing the Kibana portal using a web browser.
➔ Explain how to add datasets to Kibana for analysis:
  - ◆ Provide instructions on data ingestion methods, such as Logstash or direct indexing.
  - ◆ Demonstrate how to define index patterns to organize and search the data efficiently.

➔ Show how to create visualizations in Kibana:
  - ◆ Explain the types of visualizations available (e.g., bar charts, pie charts, maps).

- Walk through the process of selecting data, configuring visualization options, and creating visual representations of the data.