BFOR519 (System Administration and Operating System Concepts)

1. Tentative title of your project:

Log Analysis & Threat Detection

2. The scope of your project (problem you plan to tackle, solution you plan to present, topic you want to research, etc):

- **Build a pipeline to collect and analyze logs for suspicious activity.**
- **Ingest logs from multiple systems (Syslog, Windows Event Viewer).**
- **Apply basic detection rules (failed logins, privilege escalation).**
- **Visualize activity with Kibana/Grafana dashboards.**

3. Name of group members (if any):

Saanvi Shah

Acero, Elijah A

Kalariparambil Abdul Rafeek, Afla Rafeek