# Design Principles

**Instructor: Khaled Diab**

# Least Privilege

Every program/user should operate using **the least privileges** necessary to complete their job.

# Privilege Separation

- Division of a program into smaller parts, such that each part is limited to a specific set of privileges.

Example?

# Fail-Safe Defaults

- The default case is lack of access, and the policy identifies conditions under which access is permitted.

Example?

# Open Design

- Avoid security via obscurity. The design should be open.

Example?

# Complete Mediation

- Every access to every object must be checked for authority.

Example?

# Next Lecture

- Network Refresher

```
() { :; }; echo “Quiz”;
```

Good Luck ☺