Week 2 Quiz

1. Which of the principles does having an all-powerful system administration account violate? Pick the best one.
    - Principle of economy of mechanism
    - Principle of open design
    - Principle of least privilege
    - Principle of complete mediation

Correct The all-powerful system administrator can perform any function; that user should be limited to specific tasks, so an error in one will not damage the system. This is least privilege.

2. Which of the following reflects the principle of complete mediation?
    - Access permissions for a file are checked when the file is opened, and are periodically rechecked until the file is closed.
    - Access permissions for a file are checked whenever the file is accessed.
    - Access permissions for a file are checked when a process that will access the file starts.
    - Access permissions for a file are checked when the file is opened.

Correct Complete mediation requires that each access be checked. It's not a matter of checks based on time or permissions once.

3. Which of the following underlie software security design principles?
    - Secrecy of controls
    - Simplicity of controls
    - Complexity of controls
    - Minimizing cost of controls

Correct The simpler a design or implementation is, the less that can go wrong, the fewer inconsistencies are possible, and the easier it is to understand.

4. Which of the following underlie software security design principles?
   - Restrictiveness of controls
   - Inclusivity of controls
   - Incomprehensibility of controls
   - Validation of controls

Correct The controls are designed to limit access, not expand it.

5. A virtual machine isolates its operating system and processes from the host it runs Which principle best reflects this?
   - Principle of fail-safe defaults
   - Principle of least common mechanism
   - Principle of psychological acceptability
   - Principle of separation of privilege

Correct Isolation minimizes (or, ideally, eliminates sharing, which is the principle of least common mechanism.

6. Considering the basic file access controls of Windows and Linux systems (called "systems" here), which of the following is true?
   - The file access mechanisms enforce least privilege because users can control access on a per-user basis.
   - The file access mechanisms do not enforce least privilege.
   - The file access mechanisms enforce least privilege because the permission can be on a per-group basis.
   - The file access mechanisms enforce least privilege because the permissions are checked on each access.

Correct The basic file access mechanisms do not allow per-user control or per-group control; access is given to exactly 1 user and 1 group, and then everyone else is lumped together.

7. To change to the root user, the su(1) program in FreeBSD requires that the user know the root password and that the user be a member of group 0. Which principle does this reflect? Pick the best one.
   - Principle of separation of privilege
   - Principle of least privilege
   - Principle of complete mediation
   - Principle of least astonishment

   Correct The user must satisfy 2 conditions to change to the root user, which is separation of privilege.