SENG2250/6250 System and Network Security
Self-Quiz Week 6, Semester 2, 2020

True/False Questions.

1. The security kernel is responsible for enforcing the security mechanisms, so a security kernel equals to a reference monitor.
   False. A security kernel also contains mechanisms for identification, authentication, auditing, etc.

2. Security kernel can be either combined with an operating system (kernel) or as a separate security kernel.
   True.

3. In a Unix system, the “nobody” user can own files.
   False. “nobody” user cannot own files. It is used as a default user for unprivileged operations.

4. In Unix, if a file’s access permission is “rwx-w-r--”, then it means that any user can read this file.
   False. Members of the group, which the file belongs to, can read the file.

5. In Unix, a user must have the write permission on a file to delete it.
   False. If a user has the write permission on the directory that contains the target file, then he can delete it without having the write permission on the file itself.

Short-Answer Questions

6. In Unix, **/etc/shadow** (that stores passwords) is owned by the root. Other users do not have write permission on the file. Why can you change your password by using **passwd** utility?
   Because **setuid** is enabled to /bin/passwd, when a user runs **passwd**, the user will be given the effective user identifier (EUID) as root. With the (root) EUID, the user will have the privilege to run the program as the root.