

Please read this:

NOTE: The instructions below are what will be used for real quizzes. The questions on this sample quiz may not be indicative of material being tested on the real quizzes but are intended to demonstrate the format of the questions and the style of answers expected. This sample quiz is NOT for a grade.

This is a **closed book, closed notes** quiz. Use a dark ink (or pencil) and print answers on the test paper following the questions. Please answer the questions **as briefly as possible!** Write your answers legibly. Unreadable answers will be counted wrong.

Please - no talking! You may write on back. Please turn in quiz promptly, when asked. If you need more paper: raise your hand, put your name and 4 digit # on top right. Please turn off and put your phones (and any connected devices including smart watches) away. Thank You.

1. What is password salting and how does it improve security?

Notional Answer: Password salting enhances the security of stored passwords by combining the plaintext with a random string prior to hashing, thus ensuring that if more than one account uses the same password, the resulting hash will be unique. It helps defeat the use of rainbow tables which would otherwise speed up offline attacks against hashed passwords.

2. Alice runs a Set-UID program that is owned by Bob. The program tries to read from /tmp/x, which is readable to Alice, but not to anybody else. Can this program successfully read from the file? Why or why not? Explain your answer.

Notional Answer: No. When the program runs, the effective user ID is Bob, which is what is used by the system to check whether the process is able to read from /tmp/x. Although the real user ID Alice can read from the file, the effective user ID does not have permission. Therefore, the read access will be denied.

3. What are some of the data concerns that must be addressed in the disposal phase of a system lifecycle?

Notional Answer: Data residing on the system must be dispositioned in accordance with any applicable laws or regulations. It may be required to retain or archive the data for some specific period of time or destroy the data in accordance with established practices, typically through sanitization of media or destruction of non-volatile storage devices.