15

Answers to Even-numbered Exercises

2. What is an administrator? What makes an administrator different from an ordinary user?

   An administrator keeps one or more systems in a useful and convenient state for users. An administrator is permitted to run programs with **root** privileges.

4. Use the terms *encryption algorithm*, *plaintext*, and *ciphertext* in a sentence. What is another term for *encryption algorithm*?

   An **encryption algorithm** transforms **plaintext** into **ciphertext**. An encryption algorithm is also called a *cipher*.

6. What is an MITM (man-in-the-middle) attack?

   A MITM attack is a setup in which the attacker sits on the network between two people attempting to exchange messages securely. The attacker intercepts the public keys the two people exchange and substitutes his own keys. The attacker can then read any information the two people exchange.

8. Which of the following hash algorithms is the least secure: MD5, SHA1, or SHA2?

   MD5 is less secure than SHA1 and SHA2 and is not secure for most applications.

10. How would you allow a user to execute a specific, privileged command without giving the user the **root** password or permission to use sudo to run any command with **root** privileges?

    You can create a setuid program that belongs to a group that only the user who is to execute it belongs to and that has no permissions for other users. Alternately, you can edit the **sudoers** file to grant the user permission to use sudo to execute the command.