Chapter 01: Security mindset

1. Classify each of the following as a violation of confidentiality, of integrity, of availability, or of some combination thereof.
   a. John copies Mary's homework.
   b. Paul crashes Linda's system.
   c. Carol changes the amount of Angelo's check from $100 to $1,000.
   d. Gina forges Roger's signature on a deed.
   e. Rhonda registers the domain name "AddisonWesley.com" and refuses to let the publishing house buy or use that domain name.
   f. Jonah obtains Peter's credit card number and has the credit card company cancel the card and replace it with another card bearing a different account number.
   g. Henry spoofs Julie's IP address to gain access to her computer.
2. Identify mechanisms for implementing the following. State what policy or policies they might be enforcing.
   a. A password changing program will reject passwords that are less than five characters long or that are found in the dictionary.
   b. Only students in a computer science class will be given accounts on the department's computer system.
   c. The login program will disallow logins of any students who enter their passwords incorrectly three times.
   d. The permissions of the file containing Carol's homework will prevent Robert from cheating and copying it.
   e. When World Wide Web traffic climbs to more than 80% of the network's capacity, systems will disallow any further communications to or from Web servers.
   f. Annie, a systems analyst, will be able to detect a student using a program to scan her system for vulnerabilities.
   g. A program used to submit homework will turn itself off just after the due date.
3. The aphorism "security through obscurity" suggests that hiding information provides some level of security. Give an example of a situation in which hiding information does not add appreciably to the security of a system. Then give an example of a situation in which it does.
4. Give an example of a situation in which a compromise of confidentiality leads to a compromise in integrity.
5. For each of the following statements, give an example of a situation in which the statement is true.
   a. Prevention is more important than detection and recovery.

b. Detection is more important than prevention and recovery.
c. Recovery is more important than prevention and detection.

Chapter 2: Software & OS Security

6. Give an example of a vulnerable program, identify Error, Fault, Flaw of that code.
7. Give an example of a vulnerable program, rewrite to make it safer/more defensive
8. Memory layout of a program
9. Memory layout of the stack memory
10. What is buffer overflow? Stack smashing
11. Describe countermeasures to protect program from buffer overflow attacks
12. What is a Trusted Computing Base (TCB)?
13. How to make OS a TCB?
14. List OS operations, HW design to contribute to making OS a TCB

Chapter 3: Authentication & Access Control

15. The Web site www.widget.com requires users to supply a user name and a password. This information is encoded into a cookie and sent back to the browser. Whenever the user connects to the Web server, the cookie is sent. This means that the user need only supply a password at the beginning of the session. Whenever the server requests re-authentication, the client simply sends the cookie. The name of the cookie is "identif"
    a. Assume that the password is kept in the clear in the cookie. What should the settings of the secure and expires fields be, and why?
    b. Assume that the name and password are hashed and that the hash is stored in the cookie. What information must the server store to determine the user name associated with the cookie?
    c. Is the cookie storing state or acting as an authentication token, or both? Justify your answer
16. Consider a computer system with three users: Alice, Bob, and Cyndy. Alice owns the file alice.rc, and Bob and Cyndy can read it. Cyndy can read and write Bob's file bob.rc, but Alice can only read it. Only Cyndy can read and write her file cyndy.rc. Assume that the owner of each of these files can execute it.
    a. Create the corresponding access control matrix.
    b. Cyndy gives Alice permission to read cyndy.rc, and Alice removes Bob's ability to read alice.rc. Show the new access control matrix.
17. Alice can read and write to the file x, can read the file y, and can execute the file z. Bob can read x, can read and write to y, and cannot access z.
    a. Write a set of access control lists for this situation. Which list is associated with

which file?

b. Write a set of capability lists for this situation. With what is each list associated?

18. Revoking an individual's access to a particular file is easy when an access control list is used. How hard is it to revoke a user's access to a particular set of files, but not to all files? Compare and contrast this with the problem of revocation using capabilities.

19. Given the security levels TOP SECRET, SECRET, CONFIDENTIAL, and UNCLASSIFIED (ordered from highest to lowest), and the categories A, B, and C, specify what type of access (read, write, or both) is allowed in each of the following situations. Assume that discretionary access controls allow anyone access unless otherwise specified.

    a. Paul, cleared for (TOP SECRET, {A, C}), wants to access a document classified (SECRET, { B, C }).

    b. Anna, cleared for (CONFIDENTIAL, {C}), wants to access a document classified (CONFIDENTIAL, {B}).

    c. Jesse, cleared for (SECRET, {C}), wants to access a document classified (CONFIDENTIAL, {C}).

    d. Sammi, cleared for (TOP SECRET, {A, C}), wants to access a document classified (CONFIDENTIAL, {A}).

    e. Robin, who has no clearances (and so works at the UNCLASSIFIED level), wants to access a document classified (CONFIDENTIAL, {B}).