Principles of Computer Security CompTIA Security+ and Beyond 3rd Edition Conklin Solutions Manual
Full Download: http://alibabadownload.com/product/principles-of-computer-security-comptia-security-and-beyond-3rd-edition-co

Principles of Computer Security:

CompTIA Security+™ and Beyond, Third Edition

Chapter 2 Solutions

Key Terms Quiz

1. Nonrepudiation
2. Clark-Wilson security model
3. Simple Security Rule
4. least privilege
5. Integrity
6. Phreaking, hacking
7. Authentication
8. layered security
9. Data aggregation
10. certificates

Multiple-Choice Quiz

1. **C.** The username/password combination is the single most common authentication mechanism in use today.
2. **B.** Don't forget, even though authentication was described at great length in this chapter, the *A* in the CIA of security represents availability, which refers to both the hardware and data being accessible when the user wants it.
3. **A.** This is the definition of the Simple Security Rule.
4. **D.** This is the definition for least privilege.
5. **B.** Job rotation can occur as specific intervals in time.
6. **C.** Bell-LaPadula is based on data confidentiality.

Copyright © 2012 by The McGraw-Hill Companies.

This sample only, Download all chapters at: alibabadownload.com

7. **C.** Separation of duties is the division of labor to prevent a single person from controlling too much of a process.
8. **A**. This is an example of security by obscurity, which seldom if ever works.
9. **B.** The problem with the Low-Water-Mark policy is that it lowers the integrity level of subjects to the level of the object, which will ultimately (potentially) result in subjects all having the level of trust of the lowest object on the system.
10. **A.** This is the definition of implicit deny.

Essay Quiz

1. You should have immediately noticed that all of the activities your boss is describing are indicative of social engineering attacks. Although you can't tell if these are disparate events or a single entity attempting to gain enough information about your company to launch a more serious attack, you should recommend that all employees be immediately reminded (or trained) on social engineering attacks and the many forms that they can take. You should also discuss what the employees should do if they are the target of a social engineering attempt. You may also want to recommend that your security personnel contact your attorneys (who might want to contact local law enforcement personnel) or your legal office to determine what could be done from a legal standpoint.
2. Passwords are the most common form of authentication but are also very easily compromised, for a variety of reasons. As a result of this, many organizations have turned to what is known as multifactor authentication, which means they will employ more than one technique to conduct authentication. Authentication is the process of using some mechanism to prove that you are who you claim to be. There are three general methods used in authentication. To verify your identity, you can provide something you know (such as the password), something you have (such as the security token mentioned), or something about you (something that you are—a biometric). By supplying a security token, the company makes it harder for an attacker to penetrate its security since he will now need not only a user's user ID/password but also a security token.
3. Not all environments are more concerned with confidentiality than integrity. In a financial institution, for example, viewing somebody's bank balance is an issue, but a greater issue

Copyright © 2012 by The McGraw-Hill Companies.

would be the ability to actually modify that balance. In environments where integrity is more important, a different model than the Bell-LaPadula security model is needed. Another example would be a newspaper, which might be more concerned about its stories being modified than about them being viewed, or a college, which might be more concerned about somebody's grades being modified than about somebody's grades being viewed (this is not to say privacy is not important, but it is generally of secondary importance to integrity).

4. Security through obscurity uses the approach of protecting something by hiding it. Noncomputer examples of this concept discussed earlier in the chapter include hiding your briefcase or purse if you leave it in the car so that it is not in plain view, hiding a house key under a doormat or in a planter, or pushing your favorite ice cream to the back of the freezer so that everyone else thinks it is gone. Other examples might include hiding money in a coffee can and burying it, hiding money in a mattress, or hiding valuables in a hollowed out book and placing it on a bookshelf. In most security circles, security through obscurity is considered a poor approach, especially if it is the only approach to security. An organization can use security through obscurity measures to try to hide critical assets, but other security measures should also be employed to provide a higher level of protection. For example, if an administrator moves a service from its default port to a more obscure port, an attacker can still actually find this service; thus, a firewall should be used to restrict access to the service. Plus, most people know that even if you do shove your favorite ice cream to the back of the freezer, someone may eventually find it.

5. Least privilege means that a subject (which may be a user, application, or process) should have only the rights and privileges necessary to perform its task, with no additional permissions. Limiting an object's privileges limits the amount of harm that can be caused, thus reducing an organization's exposure to damage. Users may have access to the files on their workstations and a select set of files on a file server, but no access to critical data that is held within the database. This rule lets an organization protect its most sensitive resources and helps ensure that whoever is interacting with these resources has a valid reason to do so. Banking and accounting are two environments where this might be employed.

Copyright © 2012 by The McGraw-Hill Companies.

Principles of Computer Security CompTIA Security+ and Beyond 3rd Edition Conklin Solutions Manual
Full Download: http://alibabadownload.com/product/principles-of-computer-security-comptia-security-and-beyond-3rd-edition-co

Lab Projects

Lab Project 2.1

Layered security examples are fairly common. Web sites generally have external firewalls to keep a certain amount of traffic off their network, but then also employ access controls on the individual systems to limit what individuals can do. Diversity of defense is not as common because this generally entails using different versions or types of the same defense to make it harder for intruders to access the entire network. A reason this is not often employed is that it requires additional overhead for administrators, who have to worry about multiple types of systems. One example that is fairly common, even though it's not often seen as a conscious security decision, is the use of different operating systems for different computers.

Lab Project 2.2

Microsoft Windows operating systems employ discretionary access control through the use of a discretionary access control list (DACL). The ACL is made up of an ACL header and zero or more access control entry (ACE) structures. An ACL with zero ACEs is called a null ACL and indicates that no user has access to the object. There are three rules for assigning ACLs: 1) If a user explicitly provides a security descriptor when creating the object, the security system applies it to the object. 2) If a user doesn't provide a security descriptor at creation, the system looks at the security descriptor in the directory where the new object is stored. Some of the object directory's ACE structure might be marked inheritable. 3) If neither is the case, the system retrieves the default ACL from the user's access token and applies it to the new object.

In UNIX-based systems, the well-known permission bits method is used to identify what type of access a user has for a given object. These bits determine access based on the individual user, a group that the user may be in, or all users considered as a whole. The specific permissions are set by the user, though a default is automatically assigned.

Copyright © 2012 by The McGraw-Hill Companies.

This sample only, Download all chapters at: alibabadownload.com