CISSP Guide to Security Essentials, 2nd Edition

Chapter 2 Solutions

Review Questions

1. The process of obtaining a subject's proven identity is known as:

   a. Enrollment

   b. Identification

   c. Authentication

   d. Authorization

2. Which of the following is the best example of multi-factor authentication?

   a. Biometric

   b. None of these

   c. What the user knows

   d. Token

3. The only time that a user may share his or her password with another user is:

   a. When the other user requires higher access privileges

   b. During a disaster

   c. Only temporarily until the other user is issued a userid and password

   d. It is never appropriate for a user to share his or her password

4. The term *False Reject Rate* refers to:

   a. How often a biometric system will reject an invalid user

b. How often a biometric system will accept an invalid user

c. How often a biometric system will reject a valid user

d. How often a biometric system will accept a valid user

5. *Password quality* refers to:

a. Password encryption

b. Password expiration

c. Password complexity

d. All of the above

6. Every month, the human resources department issues a list of employees terminated in the previous month. The security manager should:

a. Use the list to conduct an audit of computer accounts to make sure the terminated employees' accounts have been terminated

b. Make sure that computer accounts are terminated as soon as possible after the issuance of the list of terminated employees

c. Request that the human resource department notify account managers of terminations daily instead of monthly

d. Request that the list of terminated employees be encrypted for security reasons

7. The principal security weakness with RADIUS is:

a. Traffic is not encrypted

b. Passwords do not expire

c. It uses the TCP protocol

d. RADIUS sessions are connectionless

8. The use of LDAP as a single source for authentication data helps an organization to achieve:

a. Fewer password resets

b. Effective password management

c. Single sign-on

d. Reduced sign-on

9. An auditor has produced a findings report that cites the lack of separation of duties as a significant problem. Management should consider:

a. Separating development and production environments

b. Outsourcing the indicated process

c. Stop outsourcing the indicated process

d. Examining the indicated process and reassigning duties among a greater number of individuals

10. All of the following controls are preventive controls EXCEPT:

a. Fencing

b. Surveillance cameras

c. Firewalls

d. Bollards

11. An attack on a server that originates from many sources is known as a:

a. DDoS

b. DoS

c. Botnet

d. Teardrop

12. The most effective way to protect audit log data is to:

a. Write audit log data to tape

b. Write-protect audit log data

c. Write audit log data to write-once media

d. Write audit log data to optical storage

13. The purpose of a defense in depth strategy is:

a. To make protected assets difficult to find

b. To ensure that protected assets are reachable

c. To protect assets from unauthorized access

d. To protect assets using a variety of controls

14. Anti-malware is a form of:

a. Preventive control

b. Detective control

c. Corrective control

d. Recovery control

15. The most effective way to prevent password cracking is:

a. Make the password hash files inaccessible

b. Remove password cracking tools from the target system

c. Protect passwords using strong encryption

d. Remove the target system from the network

Hands-On Projects

Project 2-1

Students are directed to observe the levels of authentication through experiencing the

online merchant Amazon.com. The levels that the student will observe are:

1. No identification. Here, the site knows nothing about the user's identity. This is seen in step 3.
2. Identification. Here, the site remembers the user's identity through a persistent cookie. This is seen in step 5.
3. Authentication. Here, the site recognizes the user's identity through a session cookie. This is the highest level of authentication, where the user is permitted to perform transactions.

Instructors may have students perform this exercise using a different web site. The web site behavior that is implemented by Amazon is commonly used.

Project 2-2

In this project, students set up and interact with firewall software. This helps students to better understand how firewalls work by performing tasks on their computer and observing (directly and through review of log entries) firewalls at work.

Project 2-3

Students have the opportunity to observe anti-virus software, without risking infection with real malware. After checking to see that their computer's anti-virus software is installed, running, and properly configured, students are directed to download the EICAR test file from eicar.org.

EICAR test files are simple text files containing a string of characters that virtually all

anti-virus programs recognize as malware. This capability was developed as a safe way to test whether anti-virus software is actually working properly. An EICAR test file does not contain code or anything harmful—just a string of characters that matches a signature in an anti-virus program's database.

Project 2-4

In this project, students are able to encrypt and decrypt text files and be able to observe plaintext and corresponding ciphertext. Students are directed to use WinZip, although 7Zip may also be used. Mac users can use the built-in *zip* command.

Instructors may direct students to experiment with encryption, to help students observe how ciphertext changes greatly even when the plaintext or the key is changed slightly. You may explain that this is a part of the value of modern cryptography, which makes it difficult for an attacker to break a cryptosystem.

Case Projects

Case Project 2-1

In this project, students are asked to develop a specification for initial registration and authentication into an investment management system. For each use case, students are directed to specify what users of the system are required to do to complete each function. Students may draw from their experience in dealing with online merchants and online banking to develop the plan. Features that students might use include:

- Various methods of confirmation for initial registration
- Reauthenticating when performing sensitive transactions
- Multi-factor authentication
- Various methods of confirming sensitive transactions to prevent cross-site request forgery and other attacks
- After-the-fact notification of sensitive transactions
- Various methods (such as CAPTCHA) to confirm that the subject performing a transaction is a human and not a machine

Case Project 2-2

Students are directed to observe a real-world set of defense in depth controls used to protect an IT system or a physical work facility.

Instructors need to be sure that students understand the difference between defense in depth and resilience. For example, two separate paths from the Internet to an application server, each with its own firewall, is not a defense in depth but the avoidance of a single point of failure.

As another example, a firewall and an anti-virus gateway could be considered a defense in depth—in general—against malware, although each protects in its own way. Similarly, while a moat and a drawbridge each protect a castle from intruders, they do so in different ways: a moat may block a good climber who cannot swim, whereas a drawbridge may block a good swimmer who cannot climb.

Case Project 2-3

Students are asked to learn about script injection vulnerabilities (including JavaScript injection and SQL injection), by finding one or more sites that visibly demonstrate a successful injection attack.

Students are then asked to describe potential safeguards that can be used to protect a system against injection attacks. In general, students should take one of these approaches:

- A system could carefully parse and sanitize input fields to remove any and all signs of code injection
- A system could provide a more intelligent list of choices instead of using a freeform text field. For example, a system that requests a date could use drop-down values that a user would select, as opposed to asking the user to input a date.

In a classroom setting, students could weigh the value in the two above approaches, as well as any others that are proposed.

Case Project 2-4

In this project, students are asked to develop a user access request process. Here, students will need to think beyond the use of technology and understand how technology can be effectively applied in a real organization.

The process that students need to develop will contain a request form, two procedures, and recordkeeping. Students with different thinking styles will develop different results; some may develop a flowchart while others will develop step-by-step instructions.

The final step of the case project asks students to discuss how auditors would audit a user

access request process. This helps students see their business process (and underlying technology) from the outside in.

In the classroom, an instructor could direct students to trade their process documents and ask students to comment on the ability to audit processes developed by other students. This would help students experience objectivity by viewing processes developed by others.