Module_1_Assessment (Access Controls 3rd)

Due Sep 24 at 11:59pm **Points** 20 **Questions** 20
Available Sep 18 at 12am - Sep 25 at 11:59pm **Time Limit** 45 Minutes
Allowed Attempts 2

Instructions

You have two attempts to take this assessment with the highest score being retained. The assessment has a time limit of 45 minutes.

Suggestion: take the assessment in the beginning of the module and then after the reading and assignments are done. You can then use the results of both to gauge your learning and retention.

Take the Quiz Again

Attempt History

	Attempt	Time	Score
LATEST	Attempt 1	23 minutes	19 out of 20

ⓘ Answers will be shown after your last attempt

Score for this attempt: **19** out of 20
Submitted Sep 22 at 3:57pm
This attempt took 23 minutes.

Question 1 — 1 / 1 pts

Of the following choices, what represents a single-factor authentication technique?

- Requiring a user to use a smart card and a PIN
- Requiring a user to use a smart card and a fingerprint

- (selected) Requiring a user to use a password and a PIN
- Requiring a user to enter a password and use a fingerprint

PTS: 1
RATIONALE: C is correct. A password and a personal identification number (PIN) are both in the “something you know” factor. A, B, and D are incorrect. All of these are multifactor examples since they combine requirements from different factors. A smart card is in the “something you have” factor, a PIN (and a password) is in the “something you know” factor, and a fingerprint is in the “something you are” factor.

Question 2

1 / 1 pts

Of the following choices, what is NOT considered a subject in access control?

- Users
- Computers
- Applications
- (selected) Data

PTS: 1
RATIONALE: D is correct. Data is an object, not a subject. A, B, C are incorrect. Users, computers, and applications are all subjects. They can be granted to objects.

Question 3

1 / 1 pts

What is the primary goal of the Chines Wall model?

- Integrity
- Confidentiality
- Prevention of conflict of interest
- Enforcement of separation of duties

PTS: 1
RATIONALE: C is correct. The Chinese Wall is primarily used in financial services organizations and helps prevent a conflict of interest. A, B, and D are incorrect. The Chinese Wall model doesn't address integrity (Biba does), it doesn't address confidentiality (Bell-LaPadula does), and it doesn't address separation of duties (Clark-Wilson does).

Question 4

1 / 1 pts

A user has entered a username to begin a logon process. What has the user completed?

- Authentication
- Authorization
- Identification
- Access

PTS: 1
RATIONALE: C is correct. Identification occurs when a user professes an identity, and a username is an identity. A, B, and D are incorrect. Authentication occurs when a user proves the claimed identity (as with a password). Authorization provides a user access to a resource but only after authentication.

Question 5

1 / 1 pts

You are evaluating the performance of a biometric system for authentication. What provides the best measure of the overall performance of the system?

- FRR
- FAR
- CER
- DAC

PTS: 1
RATIONALE: C is the correct. The Crossover Error Rate (CER) identifies the point where the FAR and FRR of a biometric system are equal to each other, or when charted, where the two cross over. A lower CER indicates a better performing biometric system. A, B, and D are incorrect. The False Acceptance Rate (FAR – type 2 error) refers to the percentage of times a biometric system falsely identifies an unknown user as a known user. A lower CER indicates a better performing biometric system. Discretionary Access Control (DAC) is an access control model.

Question 6

1 / 1 pts

Which of the following is the strongest password?

- 123456
- IW1llP@SSSSCP
- TouZjeoZhwepiD
- P@ssword

PTS: 1
RATIONALE: B is correct. This example is the only one that combines uppercase and lowercase letters, numbers, and special characters and is of sufficient length. A, C, and D are incorrect. Passwords that don't use all character types are not as strong as those that do. 123456 uses only numbers. TouZjeoZhwepiD uses only uppercase and lowercase letters. P@ssword uses three character types and is shorter than IW1llP@SSSSCP.

Question 7

1 / 1 pts

What access control model provides users with ownership of data and gives them full control over the data?

- DAC
- MAC
- Role-BAC
- SSO

PTS: 1
RATIONALE: A is correct. The Discretionary Access Control (DAC) model gives users ownership of data and enables them to exercise full control over the data, including assigning permissions to others. B, C, and D are incorrect. The Mandatory Access Control (MAC) model uses labels and the Role-base Access Control (Role-BAC model uses groups, but neither supports ownership of the data by users. Single Sign-on (SSO) is related to authentication, not access control.

Question 8

1 / 1 pts

Which of the following is NOT an example of a physical access control?

- A locked door
- An alarm system
- A guard
- An account lockout

PTS: 1
RATIONALE: D is correct. Account lockout is a logical control that can be used to lock out an account after too many incorrect password attempts. A, B, and C are incorrect. Examples of physical access controls include locked doors, alarm systems, guards, cipher locks, and cameras.

Question 9

1 / 1 pts

What is the primary goal of the Biba model?

- (•) Integrity
- ( ) Confidentiality
- ( ) Availability
- ( ) Authentication

PTS: 1
RATIONALE: A is correct. The Biba model is a Mandatory Access Control (MAC) model, and it enforces integrity. B, C, and D are incorrect. The Bell-LaPadula model enforces confidentiality. Access control models don't provide availability or authentication.

Question 10

1 / 1 pts

What is the difference between identification and authentication?

- ( ) Identification occurs when the user provides a password and authentication occurs when the password is verified.
- (•) Identification occurs when a user claims an identity and the authentication occurs when the user proves the identity.
- ( ) Authentication occurs when a user professes an identity and identification occurs when the user is granted access to resources.
- ( ) Identification and authentication are the same thing.

PTS: 1
RATIONAL: B is correct. A user claims (or professes) an identity and then proves the identity with authentication such as with a password. A, C, and D are incorrect. The password does not provide the identity. Authorization (not identification) occurs when the user is granted access to resources. Identification and authentication are not the same.

Incorrect

Question 11

0 / 1 pts

An organization is designing a technical password policy. Which one of the following choices would NOT be included to ensure the creation and maintenance of strong passwords?

- A minimum length
- A maximum age
- A password audit
- A mix of characters

PTS: 1
RATIONALE: C is correct. A password audit verifies that passwords are strong, but it doesn't ensure the creation of strong passwords. A, B, and D are incorrect. A password policy requires the creation of strong passwords. Strong passwords have a minimum number of characters (minimum length), are changed regularly (maximum age), and are created with a mixture of characters (such as uppercase and lowercase letters, numbers, and symbols).

Question 12

1 / 1 pts

Which one of the following is a one-time password?

- (selected) A synchronous token
- An asynchronous token
- A Kerberos ticket-granting ticket
- A Chinese wall

PTS: 1
RATIONALE: A is correct. Token-based authentication uses a synchronous token as a one-time password. The user is able to enter a personal identification number (PIN) or password, displayed in a physical token that is also synchronized with a server. B, C, and D are incorrect. An asynchronous token would not be in sync, so it could not be used as a one-time password. Kerberos ticket-granting tickets are reused, so they are not one-time passwords. A Chinese wall is an access control model used to prevent a conflict of interest.

Question 13

1 / 1 pts

Of the following choices, which represents a multifactor authentication technique?

- (selected) Requiring a user to use a smart card and a PIN
- Requiring a user to use a smart card and a token
- Requiring a user to enter a password and a PIN

Requiring a retina scan and a fingerprint of the user

PTS: 1
RATIONALE: A is correct. A smart card is in the “something you have” factor and a PIN is in the “something you know” factor. B, C, and D are incorrect. All the other answers are single-factor examples because they combine requirements from a single factor. A smart card and a token are both in the “something you have” factor. A password and a personal identification number (PIN) are both in the “something you know” factor. A retina scan and fingerprint are both in the “something you are” factor.

Question 14

1 / 1 pts

Of the following choices, what is NOT considered an object in access control?

Data

Hardware

Applications

Users

PTS: 1
RATIONALE: D is correct. A user is a subject (not an object) that can be granted access to an object, such as data, hardware, or an application. A, B, and C are incorrect. Data, hardware, and applications are all objects. Subjects are granted access to objects (resources).

Question 15

1 / 1 pts

Which of the following provides the strongest authentication?

- One-factor authentication
- Two-factor authentication
- Three-factor authentication
- Single Sign-on

PTS: 1
RATIONALE: C is correct. Three-factor authentication is stronger than one-factor authentication. If combines authentication mechanisms from each of the factors: something you know, something you have, and something you are. A, B, and D are incorrect. One-factor authentication uses only one of the factors and two-factor authentication uses only two factors. Single Sign-on (SSO) allows a user to authenticate once and then use the same credentials when accessing resources in the organization.

Question 16

1 / 1 pts

What enforces access controls for an operating system?

- The administrator
- The security kernel
- Physical security
- The processor

PTS: 1
RATIONALE: B is correct. The security kernel is the central part of the operating system that controls access to the system's resources. A, C, and D are incorrect. The administrator can configure security on a computer, physical security can enhance the computer's security, and the processor runs the operating system on the computer. However, the operating system's security kernel is what enforces he access controls.

Question 17

1 / 1 pts

What is the primary goal of the Bell-LaPadula model?

- Integrity
- Confidentiality
- Availability
- Authentication

PTS: 1
RATIONALE: B is correct. The Bell-LaPadula model enforces confidentiality. A, C, and D are incorrect. The Biba model is a Mandatory Access Control (MAC) model and enforces integrity. Access control models don't provide availability or authentication.

Question 18

1 / 1 pts

Of the following choices, what provides single sign-on capabilities?

- (●) Kerberos
- ( ) MAC
- ( ) DAC
- ( ) Role-BAC

PTS: 1
RATIONALE: A is correct. Kerberos provides single sign-on (SSO) capabilities. With SSO, users only have to log on once and they will use the same credentials to access multiple resources. B, C, and D are incorrect. Mandatory Access Control (MAC), Discretionary Access Control (DAC), and Role-based Access Control (Role-BAC) are access control models.

Question 19

1 / 1 pts

A user name Sally logs on with her username of Sally and a password of P@ssw0rd. What provides the identification and what provides the authentication?

- ( ) It's not possible to tell from the information given.
- (●) Sally is the identification and P@ssw0rd is the authentication.
- ( ) P@ssw0rd is the identification and Sally is the authentication.
- ( ) Both Sally and P@ssw0rd provide the authentication, and identification occurs when Sally is granted access to resources.

PTS: 1
RATIONALE: B is correct. Sally is the identification (the identity professed by the user) and P@ssw0rd is the authentication (what proves her identity). A, C, and D are incorrect. Because the identity is the username and the P@ssw0rd is the password that proves identity, it is possible to identify these in the scenario. Passwords do not provide identification. Identification occurs when a user professes an identity, not when a user is granted access to resources.

Question 20

1 / 1 pts

Which of the following access control models provides the highest level of security?

- Multifactor authentication
- DAC
- MAC
- Role-BAC

PTS: 1

RATIONALE: C is correct. The Mandatory Access Control (MAC) models uses labels to identify both subjects and objects. It provides the highest level of security between MAC, Discretionary Access Control (DAC), and Role-based Access Control (Role-BAC), and is commonly used by the military to ensure that data is protected in mission-critical systems. A, B, and D are incorrect. Multifactor Authentication provides strong authentication, but it is not an access control model. The DAC model offers the most granular level of access control. The Role-BAC uses roles to determine access.

Quiz Score: **19** out of 20