Examcollection

SY0-101

CompTIA

Security+

Question: 1
Which of the following is NOT a valid access control mechanism?

A. DAC (Discretionary Access Control) list.
B. SAC (Subjective Access Control) list.
C. MAC (Mandatory Access Control) list.
D. RBAC (Role Based Access Control) list.

Answer: B

Explanation:
The three basic access control mechanisms are: MAC (Mandatory Access Control), DAC (Discretionary Access Control) and RBAC (Role Based Access Control). There is no SAC (Subjective Access Control) list.

Incorrect Answers:
C: The three basic access control mechanisms are: MAC (Mandatory Access Control), DAC (Discretionary Access Control) and RBAC (Role Based Access Control). MAC is based on predefined access privileges to a resource.
A: The three basic access control mechanisms are: MAC (Mandatory Access Control), DAC (Discretionary Access Control) and RBAC (Role Based Access Control). DAC is based on the owner of the resource allowing other users access to that resource.
D: The three basic access control mechanisms are: MAC (Mandatory Access Control), DAC (Discretionary Access Control) and RBAC (Role Based Access Control). RBAC is based on the role or responsibilities users have in the organization.

References:
Michael Cross, Norris L. Johnson, Jr. and Tony Piltzecker, Security+ Study Guide and DVD Training System, Rockland, MA, Syngress, 2002, pp. 8-10.
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p. 13.

Question: 2
Which of the following best describes an access control mechanism in which access control decisions are based on the responsibilities that an individual user or process has in an organization?

A. MAC (Mandatory Access Control)
B. RBAC (Role Based Access Control)
C. DAC (Discretionary Access Control)
D. None of the above.

Answer: B

Explanation:
Access control using the RBAC model is based on the role or responsibilities users have in the organization.
These usually reflect the organization's structure and can be implemented system wide.

Incorrect Answers:
A: Access control using the MAC model is based on predefined access privileges to a resource.
C: Access control using the DAC model is based on the owner of the resource allowing other users access to that resource.
D: Access control using the RBAC model is based on the role or responsibilities users have in the organization.

References:
Michael Cross, Norris L. Johnson, Jr. and Tony Piltzecker, Security+ Study Guide and DVD Training System, Rockland, MA, Syngress, 2002, pp. 8-10.
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p. 13.

Question: 3
Which of the following best describes an access control mechanism that allows the data owner to create and administer access control?

A. MACs (Mandatory Access Control)
B. RBACs (Role Based Access Control)
C. LBACs (List Based Access Control)
D. DACs (Discretionary Access Control)

Answer: D

Explanation:
The DAC model allows the owner of a resource to control access privileges to that resource. This model is dynamic in nature and allows the owner of the resource to grant or revoke access to individuals or groups of individuals.

Incorrect Answers:
A: Access control using the MAC model is based on predefined access privileges to a resource.
B: Access control using the RBAC model is based on the role or responsibilities users have in the organization.
C: Access control using the LBAC model is based on a list of users and the privileges they have been granted to an object. This list is usually created by the administrator.

References:
Michael Cross, Norris L. Johnson, Jr. and Tony Piltzecker, Security+ Study Guide and DVD Training System, Rockland, MA, Syngress, 2002, pp. 8-10, 668.
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p. 13.

Question: 4
Which of the following is an inherent flaw in the DAC (Discretionary Access Control) model?

A. DAC (Discretionary Access Control) relies only on the identity of the user or process, leaving room for a Trojan horse.
B. DAC (Discretionary Access Control) relies on certificates, allowing attackers to use those certificates.
C. DAC (Discretionary Access Control) does not rely on the identity of a user, allowing anyone to use an account.
D. DAC (Discretionary Access Control) has no known security flaws.

Answer: A

Explanation:
The DAC model is more flexible than the MAC model. It allows the owner of a resource to control access privileges to that resource. Thus, access control is entirely at the digression of the owner, as is the resource that is shared. In other words, there are no security checks to ensure that malicious code is not made available for sharing.

References:
Michael Cross, Norris L. Johnson, Jr. and Tony Piltzecker, Security+ Study Guide and DVD Training System, Rockland, MA, Syngress, 2002, p. 720.
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p. 393.

Question: 5
Which of the following access control methods provides the most granular access to protected objects?

A. Capabilities
B. Access control lists
C. Permission bits
D. Profiles

Answer: B

Explanation:
Access control lists enable devices in your network to ignore requests from specified users or systems, or grant certain network capabilities to them. ACLs allow a stronger set of access controls to be established in your network. The basic process of ACL control allows the administrator to design and adapt the network to deal with specific security threats.

References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, pp. 13, 216, 219

Question: 6
You work as the security administrator at Company.com. You set permissions on a file object in a network operating system which uses DAC (Discretionary Access Control). The ACL (Access Control List) of the file is as follows:
Owner: Read, Write, Execute User A: Read, Write, - User B: -, -, - (None) Sales: Read,-, - Marketing: -, Write, - Other Read, Write, -
User "A" is the owner of the file. User "B" is a member of the Sales group. What effective permissions does User "B" have on the file?

A. User B has no permissions on the file.
B. User B has read permissions on the file.
C. User B has read- and write permissions on the file.
D. User B has read, write and execute permissions on the file.

Answer: A

Explanation:
ACLs have a list of users and their associated access that they have been granted to a resource such as a file.
When a user attempts to access a resource the ACL is checked to see if the user has the required privileges, if the required privileges are not found, access is denied. In this ACL, User B does not have an associated access privilege to the resource. Therefore User B has no permissions on the resource and will not be able to access it.

Incorrect Answers:
B, C, D: In this ACL, User B does not have an associated access privilege to the resource. Therefore User B has absolutely no permissions on the resource.

References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, pp. 13, 211
Michael Cross, Norris L. Johnson, Jr. and Tony Piltzecker, Security+ Study Guide and DVD Training System, Rockland, MA, Syngress, 2002, pp. 9-10.

Question: 7
You work as the security administrator at Company.com. Company has a RBAC (Role Based Access Control) compliant system for which you are planning the security implementation. There are three types of resources including files, printers, and mailboxes and four distinct departments with distinct functions including Sales, Marketing, Management, and Production in the system. Each department needs access to different resources. Each user has a workstation. Which roles should you create to support the RBAC (Role Based Access Control) model?

A. File, printer, and mailbox roles.
B. Sales, marketing, management, and production roles.
C. User and workstation roles.
D. Allow access and deny access roles.

Answer: B

Explanation:
Access control using the RBAC model is based on the role or responsibilities users have in the organization.
These roles usually reflect the organization's structure, such as its division into different departments, each with its distinct role in the organization. Thus the RBAC model could be based on the different departments.

Incorrect Answers:
A: The RBAC model is based on user roles, not on resource roles such as file, printer, and mailbox roles. These resource roles might not reflect the different departments' access requirements to them.
C: The RBAC model is based on user roles, not on a division between users and machines. Grouping all users together does not differentiate between the different access requirements of different users based on the role that those users fulfill in the organization.
D: By implementing allow access and deny access roles, we would create only two options: access to all resources or no access. This does not differentiate between the different access requirements of different users based on the role that those users fulfill in the organization.

References:
Michael Cross, Norris L. Johnson, Jr. and Tony Piltzecker, Security+ Study Guide and DVD Training System, Rockland, MA, Syngress, 2002, pp. 8-10.
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p. 13.

Question: 8
With regard to DAC (Discretionary Access Control), which of the following statements are true?

A. Files that don't have an owner CANNOT be modified.
B. The administrator of the system is an owner of each object.
C. The operating system is an owner of each object.
D. Each object has an owner, which has full control over the object.

Answer: D

Explanation:
The DAC model allows the owner of a resource to control access privileges to that resource. Thus, access control is entirely at the digression of the owner who has full control over the resource.

Incorrect Answers:
A: Each file does have an owner, which is the user that created the file, or the user to whom the creator of the file has transferred ownership.
B: The creator of the resource is the owner of that resource, not the administrator.
C: The creator of the resource is the owner of that resource, not the operating system.

References:
Michael Cross, Norris L. Johnson, Jr. and Tony Piltzecker, Security+ Study Guide and DVD Training System, Rockland, MA, Syngress, 2002, pp. 9-10.
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p. 13.

Question: 9
Which of the following are used to make access decisions in a MAC (Mandatory Access Control) environment?

A. Access control lists
B. Ownership
C. Group membership
D. Sensitivity labels

Answer: D

Explanation:
Mandatory Access Control is a strict hierarchical model usually associated with governments. All objects are given security labels known as sensitivity labels and are classified accordingly. Then all users are given specific security clearances as to what they are allowed to access.

Incorrect Answers:
A: DAC uses an Access Control List (ACL) that identifies the users who have been granted access to a resource.
B: DAC is based on the ownership of a resource. The owner of the resource controls access to that resource.
C: RBAC is based on group membership, which would reflect both the role users fulfill in the organization and the structure of the organization.

References:
Michael Cross, Norris L. Johnson, Jr. and Tony Piltzecker, Security+ Study Guide and DVD Training System, Rockland, MA, Syngress, 2002, pp. 8-9.
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p. 13.

Question: 10
Which of the following access control methods allows access control decisions to be based on security labels associated with each data item and each user?

A. MAC (Mandatory Access Control)
B. RBAC (Role Based Access Control)
C. LBAC (List Based Access Control)
D. DAC (Discretionary Access Control)