

1. Which of the following are the primary components of a discretionary access control (DAC) model?
Each correct answer represents a complete solution. Choose two.

2.
A. User's group
B. File and data ownership
C. Smart card
D. Access rights and permissions

Answer: B,D

3. The network you administer allows owners of objects to manage the access to those objects via access control lists. This is an example of what type of access control?

4.
A. RBAC
B. MAC
C. CIA
D. DAC

Answer: D

- 3 Which of the following categories of implementation of the access control includes all these security services?

- A. Administrative access control
B. Logical access control
C. Physical access control
D. Preventive access control

Answer: B

5. Which of the following attacks allows the bypassing of access control lists on servers or routers, and helps an attacker to hide? Each correct answer represents a complete solution. Choose two.

6.
A. DNS cache poisoning
B. MAC spoofing
C. IP spoofing attack
D. DDoS attack

Answer: B,C

5. Which of the following are types of access control attacks? Each correct answer represents a complete solution. Choose all that apply.

- A. Dictionary attack
B. Mail bombing
C. Spoofing
D. Brute force attack

Answer: B,C,D

6. Kerberos is a computer network authentication protocol that allows individuals communicating over a non-secure network to prove their identity to one another in a secure manner.

Which of the following statements are true about the Kerberos authentication scheme? Each correct answer represents a complete solution. Choose all that apply.

- A. Kerberos requires continuous availability of a central server.
- B. Dictionary and brute force attacks on the initial TGS response to a client may reveal the subject's passwords.
- C. Kerberos builds on Asymmetric key cryptography and requires a trusted third party.
- D. Kerberos requires the clocks of the involved hosts to be synchronized.

Answer: A,B,D

7. In which of the following access control models, owner of an object decides who is allowed to access the object and what privileges they have?

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

Answer: D

8. An organization has implemented a hierarchical-based concept of privilege management in which administrators have full access, HR managers have less permission than the administrators, and data entry operators have no access to resources.

Which of the following access control models is implemented in the organization?

- A. Role-based access control (RBAC)
- B. Network-based access control (NBAC)
- C. Mandatory Access Control (MAC)
- D. Discretionary access control (DAC)

Answer: A

9. Which of the following is an entry in an object's discretionary access control list (DACL) that grants permissions to a user or group?

- A. Access control entry (ACE)
- B. Discretionary access control entry (DACE)
- C. Access control list (ACL)
- D. Security Identifier (SID)

Answer: A

10. Access control systems enable an authority to control access to areas and resources in a given physical facility or computer-based information system.

Which of the following services provided by access control systems is used to determine what a subject can do?

- A. Authentication
- B. Authorization
- C. Accountability
- D. Identification

Answer: B

11. Which of the following decides access control on an object in the mandatory access control (MAC) environment?

- A. Sensitivity label
- B. Event log
- C. System Access Control List (SACL)
- D. Security log

Answer: A