

Session 4: Learner activity 1

Access control methods and models
Tutor version

ETFOUNDATION.CO.UK

Tutor copy: access control methods and models

Question 1

Which of the following is the strongest password?

- A. |ocrian#
- B. Marqu1sD3S0d
- C. This1sV#ryS3cure
- D. Thisisverysecure

Answer Q1

C. Answer C incorporates case-sensitive letters, numbers and special characters and is 16 characters long. The other answers do not have the complexity of answer C.

Question 2

Which of these is a security component of Windows 7?

- A. UAC
- B. UPS
- C. Gadgets
- D. Control Panel

Answer Q2

A. User Account Control (UAC) adds a layer of security to Windows Server 2008, Windows 7 and Windows Vista to protect against malware and user error and conserve resources. It enforces a type of separation of duties.

Question 3

What key combination helps to secure the log-in process?

- A. Windows+R
- B. Ctrl+Shift+Esc
- C. Ctrl+Alt+Del
- D. Alt+F4

Answer Q3

C. Ctrl+Alt+Del is the key combination used to help secure the log-in process. It can be added by configuring the local security policy.

Question 4

Which of the following is the most common authentication model?

- A. Username and password
- B. Biometrics
- C. Key cards
- D. Tokens

Answer Q4

A. The username and password combination is by far the most common authentication model. Although biometrics, key cards and tokens are also used, the password is still the most common.

Question 5

Which of the following access control methods uses rules to govern whether object access will be allowed? (Select the best answer.)

- A. Rule-based access control
- B. Role-based access control
- C. Discretionary access control
- D. Mandatory access control

Answer Q5

A. Rule-based access control (RBAC) uses rules to govern whether an object can be accessed. It is a type of mandatory access control.

Question 6

When using the mandatory access control (MAC) model, what component is needed?

- A. Labels
- B. Certificates
- C. Tokens
- D. RBAC

Answer Q6

A. Labels are required in the MAC model.

Question 7

Which of the following statements regarding the MAC model is true?

- A. MAC is a dynamic model.
- B. MAC enables an owner to establish access privileges to a resource.
- C. MAC is not restrictive.
- D. MAC users cannot share resources dynamically.

Answer Q7

D. In MAC, users cannot share resources dynamically. In other words, MAC is not a dynamic model; it is a static model. Owners cannot establish access privileges to a resource; that would be done by the administrator. MAC is indeed very restrictive, or as restrictive as the administrator wants it to be.

Question 8

In the discretionary access control (DAC) model, how are permissions identified?

- A. Role membership
- B. Access control lists
- C. They are predefined
- D. It is automatic

Answer Q8

B. In the DAC model, permissions to files are identified by access control lists (ACLs). Role membership is used in RBAC. The MAC model predefines permissions. Either way, it is not identified automatically.

Question 9

Robert needs to access a resource. In the DAC model, what is used to identify him or other users?

- A. Roles
- B. ACLs
- C. MAC
- D. Rules

Answer Q9

B. ACLs are used in the DAC model. This is different from role-based, rule-based and MAC models.

Question 10

You learn that a company has a high attrition rate. What should you ask the network administrator to do first? (Select the best answer.)

- A. Review user permissions and access control lists
- B. Review group policies
- C. Review performance logs
- D. Review the application log

Answer Q10

A. The first thing administrators should do when they notice that the company has a high attrition rate (high turnover of employees) is conduct a thorough review of user permissions, rights and access control lists. A review of group policies might also be necessary but is not as imperative. Performance logs and the application log will probably not bear any relation to that company having high levels of employee turnover.

Question 11

Your company has 1,000 users. Which of the following password management systems will work best for your company?

- A. Multiple access methods
- B. Password synchronisation
- C. Historical passwords
- D. Self-service password resetting

Answer Q11

D. It would be difficult for administrators to deal with thousands of users' passwords; therefore, the best management system for a company with 1,000 users would be self-service password resetting.

Question 12

In a DAC model, who is in charge of setting permissions to a resource?

- A. The owner of the resource
- B. The administrator
- C. Any user of the computer
- D. The administrator and the owner

Answer Q12

A. In a DAC model, the owner of the resource is in charge of setting permissions. In a MAC model, the administrator is in charge.

Question 13

Jason needs to add several users to a group. Which of the following will help him get the job done faster?

- A. Propagation
- B. Inheritance
- C. Template
- D. Access control lists

Answer Q13

C. By using a template, you can add many users to a group at once simply by applying the template to the users. Propagation and inheritance deal with how permissions are exchanged between parent folders and subfolders. Access control lists show who was allowed access to a particular resource.

Question 14

How are permissions defined in the MAC model?

- A. Access control lists
- B. User roles
- C. Defined by the user
- D. Predefined access privileges

Answer Q14

D. The MAC model uses predefined access privileges to define which users have permission to use resources.

Question 15

Which of the following would lower the level of password security?

- A. After a set number of failed attempts, the server will lock the user out, forcing her to call the administrator to re-enable her account.
- B. Passwords must be longer than eight characters and contain at least one special character.
- C. All passwords are set to expire after 30 days.
- D. Complex passwords that users cannot change are randomly generated by the administrator.

Answer Q15

D. To have a secure password scheme, passwords should be changed by the user. They should not be generated by the administrator. If an administrator were to generate the password for the user, it would have to be submitted in some way to the user in written (and unencrypted) form. That creates a security issue, especially if the user does not memorise the password and leaves a written version of it lying around. All the other answers would increase the level of password security.

**PRODUCED
BY**



South Essex College has produced
this resource on behalf of the
Education and Training Foundation

**FUNDED
BY**



**Department
for Education**

This programme is funded by
the Department for Education