Unit OS7: Security

7.4. Quiz

Windows Operating System Internals - by David A. Solomon and Mark E. Russinovich with Andreas Polze

Copyright Notice

- These materials are part of the *Windows Operating System Internals Curriculum Development Kit,* developed by David A. Solomon and Mark E. Russinovich with Andreas Polze
- Microsoft has licensed these materials from David Solomon Expert Seminars, Inc. for distribution to academic organizations solely for use in academic environments (and not for commercial use)

Security Ratings

Which of the following is not required for a C2 rating?

a) Encrypted passwords
b) Object reuse protection
c) Secure logon
d) Auditing

C2 Security

C2 trusted path is provided by:

a) Secure logon
b) Directory-level discretionary access control
c) Secure attention sequence
d) Administrator protection of audit logs

Security System Components

What is the heart of the object access protection in Windows?

a) Local Security Authority
b) Security Reference Monitor
c) Active Directory
d) Security Accounts Database

Security System Components

The Windows security system consists of a number of kernel- and user-mode components. Which one is not among them?

a) Transactional Object Monitor (TOM)
b) Security Accounts Manager (SAM)
c) Graphical Identification and Authentification (GINA)

Security Settings

Changing the security settings for a file in Windows affects:

a) The next open-operation on the file (CreateFile)

b) The next write-operation on the file (WriteFile)

c) The next read-operation on the file (ReadFile)

Active Directory

The distributed authentication and authorization mechanism in Windows active directory relies on the following security protocol:

a) Odin

b) Zeus

c) Kerberos

Kerberos

Kerberos relies on:

a) Symmetric encryption

b) Asymmetric (public/private key) encryption

c) Secret one way functions

Access Check

Which of the following are not referred to for a security access check?

a) Token

b) Discretionary Access Control List (DACL)

c) System Access Control List (SACL)

d) Desired Access

Security Token

Which of the following is not part of the Windows Security Token?

a) Account SID
b) Assigned Privileges
c) Handle to Security Reference Monitor
d) List of groups a user belongs to

Access Control Entries

Which of the following is a valid access control entry (ACE) type?

a) Allow and Deny
b) Deny all
c) Deny
d) DACL

Auditing

Auditing ACE's are stored in an object's:

a) SACL
b) DACL
c) Token
d) SID

Impersonation

In client/server applications, impersonation is used to let a:

a) Client take on a security identity of a server
b) Client access same objects as the server
c) Server take on a security identity of a client
d) Server access objects on the client system

Privileges

When a privilege is needed, the Security Reference Monitor checks this by:

a) Querying the Local Security Authority process
b) Checking privilege in the access token
c) Checking privilege DACL for user access
d) Writing auditing event to the Security event log

Access Control Lists

If Alice is a member of the Manager's group and a file she wants to access has a DACL with three ACEs composed as follows, will Alice be able to read from the file?

1st ACE: Bob can't read from the file

2nd ACE: Manager's can't write the file

3rd ACE: Alice can write and delete the file

a) yes
b) no