**Chapter 15 – Operating System Security**

**TRUE/FALSE QUESTIONS:**

T F 1) An OS associates a set of privileges with each process.

T F 2) The misfeasor is generally an outsider.

T F 3) The objective of the intruder is to gain access to a system or to increase

the range of privileges accessible on a system.

T F 4) Worms and bot programs are self-contained programs that can be

scheduled and run by the operating system.

T F 5) Intrusion detection systems are only designed to detect malicious

software behavior.

T F 6) The owner of the object can generally perform any action on the

security descriptor.

T F 7) The Security ID identifies a user uniquely across all of the machines

on the network.

T F 8) Manual analysis of logs is preferred, as it is more likely to identify

abnormal activity.

T F 9) The needs and policy relating to backup and archive should be determined

during the final stages of implementation.

T F 10) Firewalls are traditionally configured to limit access by port or protocol,

from some or all external systems.

T F 11) All users with access to a system will have the same access to all data

and resources on that system.

T F 12) Host-based firewalls, IDS, and IPS software also may improve security

by limiting remote network access to services on the system.

T F 13) You should stage and validate all patches on test systems before deploying

them in production.

T F 14) The superuser is exempt from the usual file access control constraints

and has systemwide access.

T F 15) DAC is based on the roles that users assume in a system rather than

the user’s identity.

**MULTIPLE CHOICE QUESTIONS:**

1. On a typical system the highest level or privilege is referred to as \_\_\_\_\_\_\_\_\_ .

A) administrator B) supervisor

C) root access D) all of the above

2) A \_\_\_\_\_\_\_\_\_ is an individual who is not authorized to use the computer and who

penetrates a system’s access controls to exploit a legitimate user’s account.

A) clandestine user B) superuser

C) masquerader D) misfeasor

3) A \_\_\_\_\_\_\_\_\_\_ is an individual who seizes supervisory control of the system and

uses this control to evade auditing and access controls or to suppress audit collection.

A) misfeasor B) clandestine user

C) superuser D) masquerader

4) A \_\_\_\_\_\_\_\_\_ is a legitimate user who accesses data, programs, or resources for which

such access is not authorized, or who is authorized for such access but misuses his or

her privileges.

A) superuser B) misfeasor

C) masquerader D) clandestine user

5) The \_\_\_\_\_\_\_\_ determines which users and groups can access this object for which operations.

A) DACL B) SACL

C) RPC D) ACE

6) \_\_\_\_\_\_\_\_ define the type and contents of a security descriptor.

A) SACLs B) Flags

C) Owners D) DACLs

7) \_\_\_\_\_\_\_\_ is the identifier by which this user is known to the system for purposes of security.

A) ACE B) Access token

C) SID D) Password scheme

8) Effective \_\_\_\_\_\_\_\_\_ helps ensure that in the event of a system breach or failure, system

administrators can more quickly and accurately identify what happened and thus most

effectively focus their remediation and recovery efforts.

A) logging B) archiving

C) security D) patching

9) \_\_\_\_\_\_\_\_ is the traditional method of implementing access control.

A) MAC B) RAC

C) DAC D) RBAC

10) \_\_\_\_\_\_\_\_ controls access based on comparing security labels with security clearances.

A) RBAC B) MAC

C) DAC D) RAC

11) \_\_\_\_\_\_\_\_\_ defenses aim to harden programs to resist attacks.

A) Coding B) Compile-time

C) Runtime D) Programming

12) A \_\_\_\_\_\_\_\_\_\_ is a dedicated computer that interfaces with computers outside a network

and has special security precautions built into it in order to protect sensitive files on

computers within the network.

A) firewall B) ACL

C) matrix D) guard

13) \_\_\_\_\_\_\_\_\_ implements a security policy that specifies who or what may have access

to each specific system resource and the type of access that is permitted in each instance.

A) Guard page B) Access control

C) Firewall D) All of the above

14) Recognition by voice pattern, handwriting characteristics, and typing rhythm

are examples of \_\_\_\_\_\_\_\_ .

A) cyclical biometrics B) recognition biometrics

C) dynamic biometrics D) static biometrics

15) Recognition by fingerprint, retina, and face are examples of \_\_\_\_\_\_\_\_\_\_\_ .

A) static biometrics B) dynamic biometrics

C) recognition biometrics D) cyclical biometrics

**SHORT ANSWER QUESTIONS:**

1. With \_\_\_\_\_\_\_\_ a process has complete control of the system and can add or change programs and files, monitor other processes, send and receive network traffic, and alter privileges.
2. A key security issue in the design of any \_\_\_\_\_\_\_\_\_ is to prevent, or at least detect, attempts by a user or a piece of malicious software from gaining unauthorized privileges on the system.
3. System access threats fall into two general categories: intruders and \_\_\_\_\_\_\_\_ .
4. The three classes of intruders are: clandestine user, misfeasor, and \_\_\_\_\_\_\_\_ .
5. Intrusion detection systems can be classified as host-based or \_\_\_\_\_\_\_\_\_\_\_ .
6. \_\_\_\_\_\_\_ is the process of retaining copies of data over extended periods of time in order to meet legal and operational requirements to access past data.
7. \_\_\_\_\_\_\_ is the process of making copies of data at regular intervals, allowing the recovery of lost or corrupted data over relatively short time periods.
8. System security begins with the installation of the \_\_\_\_\_\_\_\_\_ .
9. \_\_\_\_\_\_\_\_\_ controls access based on the roles that users have within the system and on rules stating what accesses are allowed to users in given roles.
10. \_\_\_\_\_\_\_\_\_ controls access based on the identity of the requestor and on access rules stating what requestors are or are not allowed to do.
11. \_\_\_\_\_\_\_\_ defenses aim to detect and abort attacks in executing programs.
12. \_\_\_\_\_\_\_\_\_\_ is a condition at an interface under which more input can be placed into a buffer or data-holding area than the capacity allocated, overwriting other information.
13. The design goals for a \_\_\_\_\_\_\_\_ are: acts as a choke point, enforces the local security policy, is secure against attacks.
14. Electronic keycards, smart cards, and physical keys are authenticators that are referred to as a \_\_\_\_\_\_\_\_\_\_ .
15. An IDS comprises three logical components: sensors, user interface, and \_\_\_\_\_\_\_\_ .