**Chapter 12 – Operating System Security**

**TRUE/FALSE QUESTIONS:**

T F 1. Most large software systems do not have security weaknesses.

T F 2. Each layer of code needs appropriate hardening measures in place to

provide appropriate security services.

T F 3. Lower layer security does not impact upper layers.

T F 4. It is possible for a system to be compromised during the installation

process.

T F 5. A plan needs to identify appropriate personnel to install and manage

the system, noting any training needed.

T F 6. The purpose of the system does not need to be taken into consideration

during the system security planning process.

T F 7. The default configuration for many operating systems usually

maximizes security.

T F 8. Ideally new systems should be constructed on an unprotected network

in order to prevent installation restrictions.

T F 9. A malicious driver can potentially bypass many security controls to

install malware.

T F 10. You should run automatic updates on change-controlled systems.

T F 11. Passwords installed by default are secure and do not need to be

changed.

T F 12. A very common configuration fault seen with Web and file transfer

servers is for all the files supplied by the service to be owned by the

same “user” account that the server executes as.

T F 13. Manual analysis of logs is a reliable means of detecting adverse

events.

T F 14. Performing regular backups of data on a system is a critical control

that assists with maintaining the integrity of the system and user data.

T F 15. Backup and archive processes are often linked and managed together.

**MULTIPLE CHOICE QUESTIONS:**

1. The first step in deploying new systems is \_\_\_\_\_\_\_\_\_.

A. security testing B. installing patches

C. planning D. secure critical content

2. Which of the following need to be taken into consideration during the system

security planning process?

A. how users are authenticated

B. the categories of users of the system

C. what access the system has to information stored on other hosts

D. all of the above

1. The first critical step in securing a system is to secure the \_\_\_\_\_\_\_\_\_\_.
2. base operating system
3. system administrator
4. malware protection mechanisms
5. remote access privileges
6. The following steps should be used to secure an operating system:
7. test the security of the basic operating system
8. remove unnecessary services
9. install and patch the operating system
10. all of the above
11. \_\_\_\_\_\_\_\_\_\_ applications is a control that limits the programs that can execute on the system to just those in an explicit list.

A. Virtualizing B. White listing

C. Logging D. Patching

1. Cryptographic file systems are another use of \_\_\_\_\_\_\_.

A. encryption B. testing

C. virtualizing D. acceleration

7. Once the system is appropriately built, secured, and deployed, the process of maintaining security is \_\_\_\_\_\_\_\_.

A. complete B. no longer a concern

C. continuous D. sporadic

8. The range of logging data acquired should be determined \_\_\_\_\_\_\_.

1. during security testing
2. as a final step
3. after monitoring average data flow volume
4. during the system planning stage

9. The \_\_\_\_\_\_ process makes copies of data at regular intervals for recovery of lost or corrupted data over short time periods.

A. logging B. backup

C. hardening D. archive

10. The \_\_\_\_\_\_ process retains copies of data over extended periods of time in order to meet legal and operational requirements.

A. archive B. virtualization

C. patching D. backup

11. The needs and policy relating to backup and archive should be determined \_\_\_\_\_\_.

1. as a final step
2. during the system planning stage
3. during security testing
4. after recording average data flow volume

12. \_\_\_\_\_\_ are resources that should be used as part of the system security planning process.

A. Texts

B. Online resources

C. Specific system hardening guides

D. All of the above

13. \_\_\_\_\_\_ systems should not run automatic updates because they may possibly introduce instability.

A. Configuration controlled B. Policy controlled

C. Change controlled D. Process controlled

14. The most important changes needed to improve system security are to \_\_\_\_\_\_.

A. disable remotely accessible services that are not required

B. ensure that applications and services that are needed are appropriately configured

C. disable services and applications that are not required

D. all of the above

15. Security concerns that result from the use of virtualized systems include \_\_\_\_\_\_.

A. guest OS isolation

B. guest OS monitoring by the hypervisor

C. virtualized environment security

D. all of the above

**SHORT ANSWER QUESTIONS:**

1. The three operating system security layers are: physical hardware, operating system kernel, and \_\_\_\_\_\_\_\_\_.
2. The aim of the specific system installation planning process is to maximize \_\_\_\_\_\_\_ while minimizing costs.
3. System security begins with the installation of the \_\_\_\_\_\_\_\_.
4. The final step in the process of initially securing the base operating system is \_\_\_\_\_\_\_\_.
5. \_\_\_\_\_\_ is a reactive control that can only inform you about bad things that have already happened.
6. \_\_\_\_\_\_\_ is the process of making copies of data at regular intervals allowing the recovery of lost or corrupted data over relatively short time periods of a few hours to some weeks.
7. \_\_\_\_\_\_ is the process of retaining copies of data over extended periods of time, being months or years, in order to meet legal and operational requirements to access past data.
8. \_\_\_\_\_\_\_ systems should validate all patches on test systems before deploying them to production systems.
9. Unix and Linux systems grant access permissions for each resource using the \_\_\_\_\_\_ command.
10. Unix and Linux systems use a \_\_\_\_\_\_\_\_ which restricts the server’s view of the file system to just a specified portion.
11. Configuration information in Windows systems is centralized in the \_\_\_\_\_\_\_, which forms a database of keys and values.
12. \_\_\_\_\_\_\_\_ refers to a technology that provides an abstraction of the computing resources that run in a simulated environment.
13. Guest OSs are managed by a \_\_\_\_\_\_, or VMM, that coordinates access between each of the guests and the actual physical hardware resources.
14. \_\_\_\_\_\_ virtualization systems are more common in clients, where they run along side other applications on the host OS, and are used to support applications for alternate operating system versions or types.
15. \_\_\_\_\_\_ virtualization systems are typically seen in servers, with the goal of improving the execution efficiency of the hardware.