QUESTION 93

In the context of computer security, "scavenging" refers to searching

A. A user list to find a name.
B. Through storage to acquire information.
C. Through data for information content.
D. Through log files for trusted path information.

Correct Answer: C

QUESTION 94

Which security program exists if a user accessing low-level data is able to draw conclusions about high-level information?

A. Interference
B. Inference
C. Polyinstantiation
D. Under-classification

Correct Answer: B

QUESTION 95

Which of the following is not a form of a passive attack?

A. Scavenging
B. Data diddling
C. Shoulder surfing
D. Sniffing

Correct Answer: B

QUESTION 96

An example of an individual point of verification in a computerized application is

A. An inference check.
B. A boundary protection.
C. A sensitive transaction.
D. A check digit.

Correct Answer: D

QUESTION 97

Data inference violations can be reduced using

A. Polyinstantiation technique.
B. Rules based meditation.
C. Multi-level data classification.
D. Correct-state transformation.

Correct Answer: A

QUESTION 98

What is it called when a computer uses more than one CPU in parallel to execute instructions?

A. Multiprocessing
B. Multitasking
C. Multithreading
D. Parallel running

Correct Answer: A

QUESTION 99

What is the main purpose of undertaking a parallel run of a new system?

A. Resolve any errors in the program and file interfaces.
B. Verify that the system provides required business functionality.
C. Validate the operation of the new system against its predecessor.
D. Provide a backup of the old system.

Correct Answer: B

QUESTION 100

Which of the following provide network redundancy in a local network environment?

A. Mirroring
B. Shadowing
C. Dual backbones
D. Duplexing

Correct Answer: C

QUESTION 101

A server farm is an example of:

A. Server clustering
B. Redundant servers
C. Multiple servers
D. Server fault tolerance

Correct Answer: A

QUESTION 102

In which state must a computer system operate to process input/output instructions?

A. User mode
B. Stateful inspection
C. Interprocess communication
D. Supervisor mode

Correct Answer: D

QUESTION 103

What should be the size of a Trusted Computer Base?

A. Small - in order to permit it to be implemented in all critical system components without using excessive resources.
B. Small - in order to facilitate the detailed analysis necessary to prove that it meets design requirements.
C. Large - in order to accommodate the implementation of future updates without incurring the time and expense of recertification.
D. Large - in order to enable it to protect the potentially large number of resources in a typical commercial system environment.

Correct Answer: B

QUESTION 104

Which one of the following are examples of security and controls that would be found in a "trusted" application system?

A. Data validation and reliability
B. Correction routines and reliability
C. File integrity routines and audit trail

D.   Reconciliation routines and data labels

Correct Answer: C

QUESTION 105
Which of the following is an operating system security architecture that provides flexible support for security policies?

A.   OSKit
B.   LOMAC
C.   SE Linux
D.   Flask

Correct Answer: D

QUESTION 106
Which of the following statements pertaining to the security kernel is incorrect?

A.   It is made up of mechanisms that fall under the TCB and implements and enforces the reference monitor concept.
B.   It must provide isolation for the processes carrying out the reference monitor concept and they must be tamperproof
C.   It must be small enough to be able to be tested and verified in a complete and comprehensive manner
D.   Is an access control concept, not an actual physical component?

Correct Answer: D

QUESTION 107
What is a PRIMARY reason for designing the security kernel to be as small as possible?

A.   The operating system cannot be easily penetrated by users.
B.   Changes to the kernel are not required as frequently.
C.   Due to its compactness, the kernel is easier to formally verify.
D.   System performance and execution are enhanced.

Correct Answer: C

QUESTION 108

Which of the following implements the authorized access relationship between subjects and objects of a system?

A. Security model
B. Reference kernel
C. Security kernel
D. Information flow model

Correct Answer: C

QUESTION 109

The concept that all accesses must be meditated, protected from modification, and verifiable as correct is the concept of

A. Secure model
B. Security locking
C. Security kernel
D. Secure state

Correct Answer: C

QUESTION 110

What is an error called that causes a system to be vulnerable because of the environment in which it is installed?

A. Configuration error
B. Environmental error
C. Access validation error
D. Exceptional condition handling error

Correct Answer: B

QUESTION 111

Which of the following ensures that security is not breached when a system crash or other system failure occurs?

A. trusted recovery
B. hot swappable
C. redundancy
D. secure boot