Correct Answer: A

QUESTION 112
What type of subsystem is an application program that operates outside the operating system and carries out functions for a group of users, maintains some common data for all users in the group, and protects the data from improper access by users in the group?

A. Prevented subsystem
B. Protected subsystem
C. File subsystem
D. Directory subsystem

Correct Answer: B

QUESTION 113
A 'Pseudo flaw' is which of the following?

A. An apparent loophole deliberately implanted in an operating system.
B. An omission when generating Pseudo-code.
C. Used for testing for bounds violations in application programming.
D. A Normally generated page fault causing the system halt.

Correct Answer: A

QUESTION 114
Which of the following yellow-book defined types of system recovery happens after a system fails in an uncontrolled manner in response to a TCB or media failure and the system cannot be brought to a consistent state?

A. Recovery restart
B. System reboot
C. Emergency system restart
D. System Cold start

Correct Answer: C

QUESTION 115
Which one of the following describes a reference monitor?

A. Access control concept that refers to an abstract machine that mediates all accesses to

objects by subjects.

B. Audit concept that refers to monitoring and recording of all accesses to objects by subjects.

C. Identification concept that refers to the comparison of material supplied by a user with its reference profile.

D. Network control concept that distributes the authorization of subject accesses to objects.

Correct Answer: A

QUESTION 116
What can best be described as an abstract machine which must mediate all access to subjects to objects?

A. A security domain
B. The reference monitor
C. The security kernel
D. The security perimeter

Correct Answer: B

QUESTION 117
What is the PRIMARY component of a Trusted Computer Base?

A. The computer hardware
B. The security subsystem
C. The operating system software
D. The reference monitor

Correct Answer: D

QUESTION 118
Which of the following is best defined as a mode of system termination that automatically leaves system processes and components in a secure state when a failure occurs or is detected in the system?

A. Fail proof
B. Fail soft
C. Fail safe
D. Fail resilient

Correct Answer: C

QUESTION 119

LOMAC uses what Access Control method to protect the integrity of processes and data?

A.   Linux based EFS.
B.   Low Water-Mark Mandatory Access Control.
C.   Linux based NFS.
D.   High Water-Mark Mandatory Access Control.

Correct Answer: B

QUESTION 120

On Linux, LOMAC is implemented as:

A.   Virtual addresses
B.   Registers
C.   Kernel built in functions
D.   Loadable kernel module

Correct Answer: D

QUESTION 121

LOMAC is a security enhancement for what operating system?

A.   Linux
B.   Netware
C.   Solaris
D.   None of the above

Correct Answer: A

QUESTION 122

What was introduced for circumventing difficulties in classic approaches to computer security by limiting damages produced by malicious programs?

A.   Integrity-preserving
B.   Reference Monitor
C.   Integrity-monitoring
D.   Non-Interference

Correct Answer: B

QUESTION 123

A feature deliberately implemented in an operating system as a trap for intruders is called a:

A. Trap door
B. Trojan horse
C. Pseudo flaw
D. Logic bomb

Correct Answer: C

QUESTION 124

Fault tolerance countermeasures are designed to combat threats to

A. an uninterruptible power supply
B. backup and retention capability
C. design reliability
D. data integrity

Correct Answer: C

QUESTION 125

A 'Psuedo flaw' is which of the following?

A. An apparent loophole deliberately implanted in an operating system program as a trap for intruders.
B. An omission when generating Psuedo-code.
C. Used for testing for bounds violations in application programming.
D. A normally generated page fault causing the system to halt.

Correct Answer: A

QUESTION 126

What Distributed Computing Environment (DCE) component provides a mechanism to ensure that services are made available only to properly designated parties?

A. Directory Service
B. Remote Procedure Call Service
C. Distributed File Service
D. Authentication and Control Service

Correct Answer: A

QUESTION 127

What can be accomplished by storing on each subject a list of rights the subject has for every object?

A.   Object
B.   Capabilities
C.   Key ring
D.   Rights

Correct Answer: B

QUESTION 128

In the Information Flow Model, what relates two versions of the same object?

A.   Flow
B.   State
C.   Transformation
D.   Successive points

Correct Answer: A

QUESTION 129

What is a security requirement that is unique to Compartmented Mode Workstations (CMW)?

A.   Sensitivity Labels
B.   Object Labels
C.   Information Labels
D.   Reference Monitors

Correct Answer: C

QUESTION 130

The Common Criteria (CC) represents requirements for IT security of a product or system under which distinct categories?

A.   Functional and assurance
B.   Protocol Profile (PP) and Security Target (ST)
C.   Targets of Evaluation (TOE) and Protection Profile (PP)
D.   Integrity and control

Correct Answer: A