D. Provide useful information to track down processing errors.

Correct Answer: C

QUESTION 572
Tracing violations, or attempted violations of system security to the user responsible is a function of?

A. authentication
B. access management
C. integrity checking
D. accountability

Correct Answer: D

QUESTION 573
According to the Minimum Security Requirements (MSR) for Multi-User Operating Systems (NISTIR 5153) document, which of the following statements pertaining to audit data recording is incorrect?

A. The system shall provide end-to-end user accountability for all security-relevant events.
B. The system shall protect the security audit trail from unauthorized access.
C. For maintenance purposes, it shall be possible to disable the recording of activities that require privileges.
D. The system should support an option to maintain the security audit trail data in encrypted format.

Correct Answer: C

QUESTION 574
Which of the following questions is less likely to help in assessing controls over audit trails?

A. Does the audit trail provide a trace of user actions?
B. Are incidents monitored and tracked until resolved?
C. Is access to online logs strictly controlled?
D. Is there separation of duties between security personnel who administer the access control function and those who administer the audit trail?

Correct Answer: B

QUESTION 575
You should keep audit trail on which of the following items?

A. Password usage.
B. All unsuccessful logon.
C. All of the choices.
D. All successful logon.

Correct Answer: C

QUESTION 576
In addition to providing an audit trail required by auditors, logging can be used to

A. provide back out and recovery information
B. prevent security violations
C. provide system performance statistics
D. identify fields changed on master files

Correct Answer: B

QUESTION 577
Which of the following should NOT be logged for performance problems?

A. CPU load.
B. Percentage of use.
C. Percentage of idle time.
D. None of the choices.

Correct Answer: D

QUESTION 578
Which of the following should be logged for security problems?

A. Use of mount command.
B. Percentage of idle time.
C. Percentage of use.
D. None of the choices.

Correct Answer: A

QUESTION 579
Which of the following services should be logged for security purpose?

A. bootp
B. All of the choices.
C. sunrpc
D. tftp

Correct Answer: B

QUESTION 580
The auditing method that assesses the extent of the system testing, and identifies specific program logic that has not been tested is called

A. Decision process analysis
B. Mapping
C. Parallel simulation
D. Test data method

Correct Answer: D

QUESTION 581
Who should NOT have access to the log files?

A. Security staff.
B. Internal audit staff.
C. System administration staff.
D. Manager's secretary.

Correct Answer: D

QUESTION 582
Which of the following correctly describe the use of the collected logs?

A. They are used in the passive monitoring process only.
B. They are used in the active monitoring process only.
C. They are used in the active and passive monitoring process.
D. They are used in the archiving process only.

Correct Answer: C

QUESTION 583
All logs are kept on archive for a period of time. What determines this period of time?

A. Administrator preferences.
B. MTTR
C. Retention polices
D. MTTF

Correct Answer: C

QUESTION 584
Logs must be secured to prevent:

A. Creation, modification, and destruction.
B. Modification, deletion, and initialization.
C. Modification, deletion, and destruction.
D. Modification, deletion, and inspection.

Correct Answer: C

QUESTION 585
To ensure dependable and secure logging, all computers must have their clock synchronized to:

A. A central timeserver.
B. The log time stamp.
C. The respective local times.
D. None of the choices.

Correct Answer: A

QUESTION 586
To ensure dependable and secure logging, logging information traveling on the network should be:

A. Stored
B. Encrypted
C. Isolated
D. Monitored

Correct Answer: B

QUESTION 587
The activity that consists of collecting information that will be used for monitoring is called:

A. Logging
B. Troubleshooting
C. Auditing
D. Inspecting

Correct Answer: A

QUESTION 588
How often should logging be run?

A. Once every week.
B. Always
C. Once a day.
D. During maintenance.

Correct Answer: B

QUESTION 589
Which of the following are security events on Unix that should be logged?

A. All of the choices.
B. Use of Setgid.
C. Change of permissions on system files.
D. Use of Setuid.

Correct Answer: A

QUESTION 590
Which of the following are potential firewall problems that should be logged?

A. Reboot
B. All of the choices.
C. Proxies restarted.
D. Changes to configuration file.

Correct Answer: B