**Chapter 18 – Security Auditing**

**TRUE/FALSE QUESTIONS:**

T F 1. Although important, security auditing is not a key element in computer

security.

T F 2. The basic audit objective is to establish accountability for system

entities that initiate or participate in security-relevant events and actions.

T F 3. Means are needed to generate and record a security audit trail and to

review and analyze the audit trail to discover and investigate attacks and security compromises.

T F 4. Audit trails are different from audit logs.

T F 5. The audit analyzer prepares human-readable security reports.

T F 6. The security administrator must define the set of events that are

subject to audit.

T F 7. Event and audit trail analysis software, tools, and interfaces may be

used to analyze collected data as well as for investigating data trends and anomalies.

T F 8. According to ISO 27002, the person(s) carrying out the audit should be

independent of the activities audited.

T F 9. Data representing behavior that does not trigger an alarm cannot serve

as input to intrusion detection analysis.

T F 10. The first order of business in security audit trail design is the selection

of data items to capture.

T F 11. Protection of the audit trail involves both integrity and confidentiality.

T F 12. The foundation of a security auditing facility is the initial capture of

the audit data.

T F 13. All UNIX implementations will have the same variants of the syslog

facility.

T F 14. Thresholding is a form of baseline analysis.

T F 15. Applications, especially applications with a certain level of privilege,

present security problems that may not be captured by system-level or user-level auditing data.

**MULTIPLE CHOICE QUESTIONS:**

1. Security auditing can:
2. provide data that can be used to define anomalous behavior
3. maintain a record useful in computer forensics
4. generate data that can be used in after-the-fact analysis of an attack
5. all of the above
6. A \_\_\_\_\_\_\_ is conducted to determine the adequacy of system controls, ensure compliance with established security policy and procedures, detect breaches in security services, and recommend any changes that are indicated for countermeasures.

A. security audit trail B. security audit

C. user-level audit D. system-level audit trail

1. The \_\_\_\_\_\_\_\_\_ is logic embedded into the software of the system that monitors system activity and detects security-related events that it has been configured to detect.

A. event discriminator B. audit analyzer

C. archive D. alarm processor

1. The \_\_\_\_\_\_\_\_ is a module on a centralized system that collects audit trail records from other systems and creates a combined audit trail.

A. audit dispatcher B. audit analyzer

C. audit trail collector D. audit provider

1. The \_\_\_\_\_\_\_\_ is a module that transmits the audit trail records from its local system to the centralized audit trail collector.

A. audit dispatcher B. audit analyzer

C. audit trail collector D. none of the above

1. \_\_\_\_\_\_\_\_\_ identifies the level of auditing, enumerates the types of auditable events, and identifies the minimum set of audit-related information provided.

A. Event selection B. Data generation

C. Automatic response D. Audit analysis

1. Data items to capture for a security audit trail include:
2. events related to the security mechanisms on the system
3. operating system access
4. remote access
5. all of the above
6. \_\_\_\_\_\_\_\_\_ audit trails are generally used to monitor and optimize system performance.

A. User-level B. Physical-level

C. System-level D. All of the above

1. \_\_\_\_\_\_\_\_\_ audit trails may be used to detect security violations within an application or to detect flaws in the application’s interaction with the system.

A. Application-level B. System-level

C. User-level D. None of the above

1. Windows allows the system user to enable auditing in \_\_\_\_\_\_\_ different categories.

A. five B. seven

C. nine D. eleven

1. Severe messages, such as immediate system shutdown, is a(n) \_\_\_\_\_ severity.

A. alert B. emerg

C. crit D. warning

1. System conditions requiring immediate attention is a(n) \_\_\_\_\_\_\_ severity.

A. alert B. err

C. notice D. emert

1. With \_\_\_\_\_\_\_\_\_ the linking to shared library routines is deferred until load time so that if changes are made any program that references the library is unaffected.
2. statically linked shared libraries
3. dynamically linked shared libraries
4. system linked shared libraries
5. all of the above
6. \_\_\_\_\_\_ is the identification of data that exceed a particular baseline value.

A. Anomaly detection B. Real-time analysis

C. Thresholding D. All of the above

1. \_\_\_\_\_\_ software is a centralized logging software package similar to, but much more complex than, syslog.

A. NetScan B. McAfee

C. IPConfig D. SIEM

**SHORT ANSWER QUESTIONS:**

1. \_\_\_\_\_\_\_\_\_ is a form of auditing that focuses on the security of an organization’s IT assets.
2. A \_\_\_\_\_\_\_\_\_is a chronological record of system activities that is sufficient to enable the reconstruction and examination of the sequence of environments and activities surrounding or leading to an operation, procedure, or event in a security-relevant transaction from inception to final results.
3. A \_\_\_\_\_\_\_ is an independent review and examination of a system’s records and activities.
4. The \_\_\_\_\_\_\_\_ is an application or user who examines the audit trail and the audit archives for historical trends, for computer forensic purposes, and for other analysis.
5. The audit \_\_\_\_\_\_\_ are a permanent store of security-related events on a system.
6. Monitoring areas suggested in ISO 27002 include: authorized access, all privileged operations, unauthorized access attempts, changes to (or attempts to change) system security settings and controls, and \_\_\_\_\_\_\_\_\_\_.
7. \_\_\_\_\_\_\_\_ audit trail traces the activity of individual users over time and can be used to hold a user accountable for his or her actions.
8. RFC 2196 (*Site Security Handbook*) lists three alternatives for storing audit records: read/write file on a host, write-once/read-many device, and \_\_\_\_\_\_.
9. Windows is equipped with three types of event logs: system event log, security event log, and \_\_\_\_\_\_\_\_ event log.
10. \_\_\_\_\_\_ is UNIX’s general-purpose logging mechanism found on all UNIX variants and Linux.
11. Messages in the BSD syslog format consist of three parts: PRI, Header, and \_\_\_.
12. The \_\_\_\_\_\_ repository contains the auditing code to be inserted into an application.
13. \_\_\_\_\_\_ is the process of defining normal versus unusual events and patterns.
14. \_\_\_\_\_\_ is detection of events within a given set of parameters, such as within a given time period or outside a given time period.
15. SIEM software has two general configuration approaches: agentless and \_\_\_\_\_\_.