Section Quiz

Candidate: Dunkan Gibson (dunkan.gibson)
Date: 4/27/2022 8:22:46 pm • Time spent: 05:30

Score: 100% Passing Score: 80%

Question 1: ✔ Correct

Which of the following terms identifies the process of reviewing log files for suspicious activity and threshold compliance?

- Phishing
- Scanning
- Auditing
- CompSec

EXPLANATION

Auditing is a complement to penetration testing and serves as documentation of attempted attacks that exceed preconfigured thresholds. Most operating systems, network devices, and security packages support the logging of usage data. Examples include the success or failure of login attempts, file access, and administrative tasks. The detailed configuration of audit logs is necessary to ensure that all pertinent data is captured and available for review. Audit logs are sometimes used as evidence in court proceedings.

REFERENCES

14.1.2 Audit Facts

q_audit_audit_01_secp7.question.fex

Question 2: ✔ Correct

Which of the following is a collection of recorded data that may include details about logons, object access, and other activities deemed important by your security policy and is often used to detect unwanted and unauthorized user activity?

- CPS (Certificate Practice Statement)
- Audit trail
- Syslog
- Chain of custody

EXPLANATION

An audit trail is a collection of recorded data that may include details about logons, object access, and other activities deemed important by your security policy that is often used to detect unwanted and unauthorized user activity.

Syslog is a standard protocol for recording system events, not user events. A chain of custody is a document related to evidence-gathering that contains details about personnel in possession and control of evidence from the time of discovery up through the time of presentation in court. A CPS (Certificate Practice Statement) is a document written by a certificate authority that outlines their certificate handling, management, and administration procedures.

REFERENCES

14.1.2 Audit Facts

q_audit_audit_02_secp7.question.fex

Question 3: ✔ Correct

A recreation of historical events is made possible through which of the following?

- Incident reports
- Audit trails
- Penetration testing
- Audits

EXPLANATION

The ability to recreate historical events is made possible through audit trails. Without the evidence in an audit trail, knowledge of activities that occurred in the past (minutes or longer) is fairly non-existent.

Audits are the security assessments performed by external auditors to check compliance with security policy and best business practices. Penetration testing is the use of hacker techniques and tools to assess security. An incident report is often produced from audit trails and is an example of the recreation of historical events rather than being the source that makes such reconstruction possible.

REFERENCES

14.1.2 Audit Facts

q_audit_audit_03_secp7.question.fex

Question 4: ✔ Correct

Which type of audit is performed by either a consultant or an auditing firm employee?

- Usage audit
- ➡ External audit
- Financial audit
- Internal audit

EXPLANATION

An external audit is performed by either a consultant or an auditing firm employee.

Internal audits are performed by an employee within an organization. He or she examines existing internal controls and maps the security structure for compliance with statutes and management goals.

Usage and financial audits can be performed by either internal or external auditors depending on the reason for the audit.

REFERENCES

14.1.2 Audit Facts

q_audit_external_secp7.question.fex

Question 5: ✔ Correct

Which of the following is true concerning internal audits?

- The auditor works independently.
- The process is very formal.
- They are generally nonobjective.
- They are always highly rigorous.

EXPLANATION

Internal audits tend to be nonobjective and, consequently, may not be as rigorous.

None of the other answers best describe internal audits.

REFERENCES

14.1.2 Audit Facts

q_audit_internal_secp7.question.fex

Question 6: ✔ Correct

Which of the following standards relates to the use of credit cards?

- PoLP
- PCI DSS
- SOX
- Financial audit

EXPLANATION

Personal Card Industry Data Security Standard (PCI DSS) compliance audits relate to the use of credit cards. These audits are regulated and enforced by major credit card companies.

A Sarbanes-Oxley (SOX) audit is a government audit by the SEC that relates to internal controls and focuses on IT security, access controls, data backup, change management, and physical security.

PoLP is the principle of least privilege. It does not apply in this scenario.

Financial audits are performed to ensure compliance with SOX or PCI DSS requirements.

REFERENCES

14.1.2 Audit Facts

q_audit_pci_secp7.question.fex

Question 7: ✔ Correct

Which of the following describes privilege auditing?

- An employee is granted the minimum privileges required to perform the duties of his or her position.
- ➡ Users' and groups' rights and privileges are checked to guard against creeping privileges.
- Users' activities are logged to document incidents for security investigations and incident response.
- No single user is granted sufficient privileges to compromise the security of an entire environment.

EXPLANATION

Privilege auditing checks users' and groups' rights and privileges to guard against creeping privileges. Privilege auditing also aids in user and group administration.

The principle of least privilege specifies that an employee is granted the minimum privileges required to perform the duties of his or her position. Separation of duties is the security principle that states that no single user is granted sufficient privileges to compromise the security of an entire environment. Usage auditing logs users' activities to document incidents for security investigations and incident response.

REFERENCES

14.1.2 Audit Facts

q_audit_privilege_secp7.question.fex

Question 8: ✔ Correct

Which component of an IT security audit evaluates defense in depth and IT-related fraud?

- User access and rights review
- Risk evaluation
- Financial audit
- External audit

EXPLANATION

A risk assessment includes an evaluation of:

- Defense in depth.
- Proper governance policies.
- Current redundancy plans.
- Proper use of corporate technology resources.
- Company and IT security strategies, policies, and procedures.
- IT-related fraud.

A user access and rights review, also known as privilege auditing, checks users' and groups' rights and privileges to guard against creeping privileges. Privilege auditing also aids in user and group administration.

An external audit is one performed by an outside auditor that is often done for compliance obligations.

A financial audit is performed to verify compliance with applicable requirements.

REFERENCES

14.1.2 Audit Facts

q_audit_risk_secp7.question.fex

Question 9: ✔ Correct

Which of the following is a government audit by the SEC that relates to internal controls and focuses on IT security, access controls, data backup, change management, and physical security?

- SOX
- PoLP
- Financial audit
- PCI DSS

EXPLANATION

A Sarbanes-Oxley (SOX) audit is a government audit by the SEC that relates to internal controls and focuses on IT security, access controls, data backup, change management, and physical security.

PoLP is the principle of least privilege. It does not apply to this scenario.

Personal Card Industry Data Security Standard (PCI DSS) compliance audits relate to the use of credit cards.

Financial audits are performed to ensure compliance with SOX or PCI DSS requirements.

REFERENCES

14.1.2 Audit Facts

q_audit_sox_secp7.question.fex

Question 10: ✔ Correct

Which of the following types of auditing verifies that systems are utilized appropriately and in accordance with written organizational policies?

- Financial audit
- Internal audit
- PoLP
- Usage audit

EXPLANATION

Usage auditing verifies that systems are utilized appropriately and in accordance with written organizational policies. These audits also ensure that rights are necessary for specific groups. If a granted right isn't used by a group, they may not need access to it.

Internal audits focus on improvement and don't negatively affect customer contracts.

PoLP is the principle of least privilege. It does not apply in this scenario.

Financial audits are performed to ensure compliance with SOX or PCI DSS requirements.

REFERENCES

14.1.2 Audit Facts

q_audit_usage_secp7.question.fex

Copyright © 2022 TestOut Corporation All rights reserved.