Exam Report: 7.9.7 Practice Questions

Date: 1/22/2020 9:06:54 pm
Time Spent: 12:36

Candidate: Garsteck, Matthew
Login: mGarsteck

Overall Performance

Your Score: 60%

Passing Score: 80%

View results by: Objective Analysis Individual Responses

Individual Responses

Question 1: Incorrect

Which of the following is **not** an advantage when using an internal auditor to examine security systems and relevant documentation?

- An internal auditor is familiar with organizational goals.
- Orientation time is minimized.
- ~~An internal auditor has knowledge of the inner workings of the organization.~~
- Findings in the audit and subsequent summations are viewed objectively.

Explanation

An internal auditor's findings might not be viewed as objectively as those produced by an external auditor. The internal auditor's knowledge of the inner workings and goals of the organization can decrease the ability to produce an objective summary of the audit.

References

LabSim for Security Pro, Section 7.9.
[All Questions SecPro2017_v6.exm AUDITS_01]

Question 2: Correct

Properly configured passive IDS and system audit logs are an integral part of a comprehensive security plan. Which step must be taken to ensure that the information is useful in maintaining a secure environment?

- The accounting department must compress the logs on a quarterly basis.
- All logs should be deleted and refreshed monthly.
- Periodic reviews must be conducted to detect malicious activity or policy violations.
- All files must be verified with the IDS checksum.

Explanation

Audit logs are useless unless they are periodically reviewed. The frequency will vary based on the criticality of the system being monitored, but the logs must be reviewed by a knowledgeable member of the IT/Infosec team on a regular basis.

References

LabSim for Security Pro, Section 7.9.
[All Questions SecPro2017_v6.exm AUDITS_02]

Question 3: Correct

Which of the following describes *Privilege* auditing?

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

Explanation

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

The *principle of least privilege* specifies that an employee is granted the minimum privileges required to perform duties of 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

LabSim for Security Pro, Section 7.9.
[All Questions SecPro2017_v6.exm AUDITS_03]

Question 4: Correct

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

- Scanning
- ➡ Auditing
- CompSec
- Phishing

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/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

LabSim for Security Pro, Section 7.9.
[All Questions SecPro2017_v6.exm AUDITS_04]

Question 5: Incorrect

Match the IT audit activity on the left with the appropriate description on the right.

Documents incidents for security violations and incident response.

~~User access and rights review~~ Usage auditing

Identifies inefficient IT strategies, such as weak policies and procedures.

✓ Risk evaluation

Verifies the appropriate use of accounts and privileges.

~~Usage auditing~~ Escalation auditing

Checks user/group rights and privileges to identify cases of creeping privileges.

~~Escalation auditing~~ Privilege auditing

Determines whether privilege-granting processes are appropriate and whether computer use and escalation processes are in place and working.

~~Privilege auditing~~	User access and rights review

Explanation

An IT audit typically focuses on the computer systems and networks of an organization. An IT audit includes:

- An assessment of computer systems and networks to determine the effectiveness of the technical and procedural controls.
- A risk evaluation that identifies inefficient use of corporate resources and inefficient IT strategies, such as weak policies and procedures.
- A user access and rights review to determine whether privilege-granting processes are appropriate and whether computer use and escalation processes are in place and working.
- Privilege auditing, which checks user/group rights and privileges to identify cases of creeping privileges. Privilege auditing also aids in user/group administration.
- Usage auditing, which documents incidents for security violations and incident response. After a review of user activity logs, compromised accounts can be identified, actions can be evaluated, and incidents can be replicated.
- Escalation auditing, which verifies the appropriate use of accounts and privileges. For example, administrators should be required to use normal user accounts for most activities. Administrators might circumvent these protections by granting additional privileges to their normal user accounts.

References

LabSim for Security Pro, Section 7.9.
[All Questions SecPro2017_v6.exm AUDITS_05]