Module 7 Assessment (Auditing 3rd)

Due Nov 5 at 11:59pm **Points** 20 **Questions** 20
Available Oct 23 at 12am - Nov 6 at 11:59pm **Time Limit** 45 Minutes
Allowed Attempts 2

Instructions

You have two attempts to take this assessment with the highest score being retained. The assessment has a time limit of 45 minutes.

Suggestion: take the assessment in the beginning of the module and then after the reading and assignments are done. You can then use the results of both to gauge your learning and retention.

Take the Quiz Again

Attempt History

	Attempt	Time	Score
LATEST	Attempt 1	18 minutes	16 out of 20

(!) Answers will be shown after your last attempt

Score for this attempt: **16** out of 20
Submitted Oct 30 at 7:15pm
This attempt took 18 minutes.

Question 1

1 / 1 pts

An organization wants to determine whether users are following policies related to passwords. Of the following choices, what provides the most reliable method?

○ Ask the users

○ Require users to e-mail their correct passwords to a security administrator

○ Complete a penetration test

● Perform a password audit

D is correct. A password audit checks to see whether users are following the policies related to passwords. Many vulnerability assessment tools include this capability.

A, B, and C are incorrect. Asking users would not be reliable. Users should not be encouraged to give their password to anyone. A penetration test attempts to exploit vulnerabilities, so it is not relevant here.

Question 2

1 / 1 pts

Audit logs combined with strong authentication and authorization practices provide an important security element. What is this?

○ Confidentiality

○ Separation of duties

○ Availability

● Nonrepudiation

D is correct. Audit logs combined with strong authentication and authorization practices provide nonrepudiation. When actions by specific users are recorded, the users are unable to deny that they took an action.

A, B, and C are incorrect. Audit logs do not provide confidentiality, separation of duties, or availability.

Question 3

1 / 1 pts

An organization wants to determine whether there are any vulnerabilities in its processes and procedures. What can the organization use to identify vulnerabilities?

● A security audit

○ A password audit

○ A penetration test

○ A clipping level audit

A is correct. Security audits help an organization identify vulnerabilities in its processes and procedures.

B, C, and D are incorrect. A password audit checks to see whether users are following the policies related to passwords (but not other policies and procedures). A penetration test attempts to exploit vulnerabilities, not just discover them. A clipping level uses a predetermined level as a threshold and ignores events until the threshold is met, but there is no such thing as a clipping level audit.

Question 4

1 / 1 pts

An organization uses configuration management to ensure that servers are deployed with similar settings. What can be done to determine whether a server has been modified?

○ Reimage the server

● Compare it to the baseline

○ Check the change management logs

○ Ask the administrators

B is correct. You can check the system against a baseline to determine whether it has been modified. Part of configuration management is the establishment of a baseline configuration, and this is often done with imaging.

A, B, and D are incorrect. If the server is reimaged, it will be returned to the original configuration, but this does not indicate whether it has been modified. Change management logs will identify authorized changes, but not unauthorized changes, so this may not be accurate. Asking administrators isn’t as reliable as a comparison to the baseline.

Question 5

1 / 1 pts

Which of the following best identifies what you would find in an audit log entry?

● Who, what, when, where

○ Who, what, when, why

○ What, when, where, why

○ What, when, where, how

A is correct. An audit log records details such as who, what, when, and where for any events of interest.

B, C, and D are incorrect. Audit logs cannot determine why someone took an action. Although an audit log may indicate how an action occurred, the how isn't definitive.   Additionally, who performed the action is much more important than how.

Incorrect

Question 6

0 / 1 pts

A user has attempted to login twice with the wrong password, and on the third attempt, the user logs in successfully. However, these two failures were not logged in a security log. What is preventing the first two attempts from being logged?

● Account lockout

○ Audit trail exception

○ Password exception

○ The clipping level

D is correct. A clipping level uses a predetermined level as a threshold and ignores events until the threshold is met.

A, B, and C are incorrect. Account lockout causes a user account to be locked out after a specified number of incorrect login attempts. Audit trail exception and password exception are distracters and not valid terms in this context.

Question 7

1 / 1 pts

An accounting system ignores logon failures until an account has three logon failures within a 30-minute period. It then generates an alert. What is the accounting system using?

○ Account lockout

○ Password policy

○ Snipping level

● Clipping level

D is correct. A clipping level uses a predetermined level as a threshold. A classic example is three or five logon failures in a short period, such as within 30 minutes. Although many operating systems use account lockout policies to actually lock the account after a predetermined level, the question doesn’t ask what happens to the account, but instead asks what the accounting system is using to ignore the first two logon failures and only generate the alert after three logon failures. A password policy ensures that users have strong passwords and change them regularly. Snipping level isn’t a valid term associated with accounting systems.

Question 8

1 / 1 pts

A user entered an incorrect password three times. Now, the user is no longer able to log on. What caused this to occur?

○ Password policy

● Account lockout policy

○ Clipping level

○ Audit trail

B is correct. An account lockout policy locks out an account after a predetermined number of failed logins. The password policy ensures that users create strong passwords and change them often. The account lockout policy is using a clipping level by ignoring failed login attempts until it detects a preset threshold, but the clipping level doesn’t lock the account. An audit trail is one or more logs used to reconstruct events leading up to and occurring during an incident.

Question 9

1 / 1 pts

What type of control is an audit trail?

○ Preventive control

○ Corrective control

● Detective control

○ Physical access control

C is corret. An audit trail is a technical detective control, because it uses technology and can detect incidents after they occur. A preventive control attempts to prevent incidents. A corrective control attempts to reverse the impact of an incident after it has occurred. A physical access control is an item that you can physically touch.

Incorrect

Question 10

0 / 1 pts

Of the following choices, what is an example of an auditable event logged in an operating system's security log?

○ Access through a firewall

○ Accessing a website through a proxy server

○ Reading a file

● The date and time when a service starts

C is correct. A security log records auditable events related to resources, such as when a user reads, modifies, or deletes a file. Firewall and proxy server logs are not operating system logs. A system log would record events such as when a service stops or starts, but not security events.

Question 11

1 / 1 pts

You suspect that many internal systems may be part of a botnet. What log would you review to verify your suspicions?

● Network-based firewall logs

○ Host-based firewall logs

○ Operating system logs

○ System security logs

A is correct. Network-based firewall logs record traffic on the network, and because many systems are involved, network-based firewalls is the best choice. Each of the other logs are local logs on individual systems. This would require checking logs on multiple systems, rather than checking logs on a single network-based firewall.

Question 12

1 / 1 pts

What is the purpose of reviewing logs?

● Detecting potential security events

○ Preventing potential security events

○ Correcting potential security events

○ Deterring potential security events

A is correct. Security professionals and auditors can detect potential security events by reviewing logs after the event has occurred. Reviewing the logs doesn't prevent an incident that has already occurred, and reviewing the logs does not enable security professionals and auditors to correct the effects of an incident. While logging some activity, such as proxy servers, can deter events, reviewing the logs doesn't deter the activity.

Question 13

1 / 1 pts

An organization handles credit card data from customers on a regular basis. What provides the security objectives and requirements that the organization must follow?

● PCI DSS

○ HIPAA

○ FIPS Pub 200

○ NITS SP 800-53

A is correct. The Payment Card Industry Data Security Standard (PCI DSS) provides 6 control objectives and 12 supporting requirements that organizations must follow if they process credit card payments from customers. The Health Insurance Portability and Accountability Act (HIPAA) covers organizations handling health- and medical-related data. Federal Information Processing Standard Publication 200 (FIPS Pub 200) identifies standards required by federal agencies. NIST SP 800-53 provides information on recommended security controls.

Question 14

1 / 1 pts

A badge reader records employee names, dates, and times when employees enter and exit a secure server room. An auditor reviewed the logs and noticed that they showed that many employees entered the room, but the logs do not show when all of the employees exited the room. What does this indicate?

○ The badge reader is operational

● Tailgating

○ The mantrap is not being used

○ Unauthorized entry

B is correct. Logs that include entries showing employees entered a secure area but do not include entries showing they exited indicate tailgating is occurring. Some employees are using their credentials to exit (and the logs show them exiting), but other employees are following closely behind these employees without showing their credentials (and the log doesn’t include entries for these employees). While it is possible the badge reader has a problem, it is recording some employees exiting, so this isn’t the most likely cause. Mantraps prevent tailgating, and if a mantrap is in use, employees would be forced to use it. There isn’t any indication of unauthorized entry.

Question 15

1 / 1 pts

Who would measure the effectiveness of an organization’s security controls?

○ A manager

● An Auditor

○ A data owner

○ An administrator

B is correct. An auditor would measure the effectiveness of a security control. An internal auditor might have other roles, such as an administrator, a manager, or a data owner. However, when measuring the effectiveness of security controls, they are acting as an auditor.

Question 16

1 / 1 pts

Of the following choices, what is a primary method used for configuration control?

● Baseline

○ Change management requests

○ Security logs

○ Password audits

A is correct. A baseline is a primary method used for configuration control and it ensures that systems start in a known state. Automated or manual processes periodically examine the systems to verify the system still has the same configuration settings from the baseline. An organization doesn't approve and implement all change management requests, so examining the requests does not give an accurate representation of the server configuration. Security logs and password audits aren't typically used for configuration control.

Incorrect

Question 17

0 / 1 pts

Which of the following is NOT a valid method used for configuration control?

● Imaging

○ Microsoft’s Group Policy

○ Change management

○ Proxy server logs

D is correct. Proxy server logs record what websites users visit and are not used for configuration control. Each of the other choices can be used for configuration control.

Question 18

1 / 1 pts

Of the following choices, what can help ensure that system modifications do NOT cause unintended outages?

○ Security audit

● Change management

○ Configuration control

○ Audt trail

B is correct. A change management program allows stakeholders to request changes and helps reduce unintended outages from unauthorized changes. A security audit examines an organization's policies and procedures to determine whether those who work in the organization follow these policies and procedures. Configuration control helps ensure that systems are configured in a secure manner and similarly to each other. An audit trail is one or more logs that can re-create events leading up to and occurring during an incident.

Question 19

1 / 1 pts

Managemetn within an organization wants t deterine whether there are any vulnerabilities in the organization's processes and procedures. Of the follwoing choices, what can the organization use to identify vulnerabilities?

● A security audit

○ A password audit

○ A penetraton test

○ A clipping level audit

A is correct. Security audits help an organization identify vulnerabilities in its processes and procedures.

B, C, and D are incorrect. A password audit checks to see whether users are following the policies related to passwords (but not other policies and procedures). A penetration test attempts to exploit vulnerabilities, not just discover them. A clipping level uses a predetermined level as a threshold and ignores events until the threshold is met, but there is no such theng as a clipping level audit.

Incorrect

Question 20

0 / 1 pts

Which of the following methods could you use to segment networks within your organization? (Select Two)

☐ Implement a VPN.

☑ Create a quarantine network.

☑ Implement a VLAN.

☐ Separate the data and control planes.

C and D are correct. A virtual local area network (VLAN) segments traffic with a switch. Software-defined networking (SDN) also provides logical segmentatoin by separating the data and control planes.

A and B are incorrect. A virtual private network (VPN) provides access to a private network via a public network, such as the Internet. A quarantine network is used by network access control solutions to redirect unhealthy clients.

Quiz Score: **16** out of 20