Module 6 Assessment (Monitoring and Analysis & Countermeasures and Controls p3rd)

Due Oct 30 at 12:59am **Points** 20 **Questions** 20 **Available** Oct 16 at 12am - Oct 31 at 12:59am **Time Limit** 45 Minutes
Allowed Attempts 2

Take the Quiz Again

Attempt History

	Attempt	Time	Score
LATEST	Attempt 1	14 minutes	17 out of 20

ⓘ Answers will be shown after your last attempt

Score for this attempt: **17** out of 20
Submitted Oct 25 at 10:54am
This attempt took 14 minutes.

Question 1

1 / 1 pts

Which of the following best describes a nontechnical control?

- A control uses technical means within computer systems to reduce risk
- A control that uses training and written documents such as security policies to reduce risk
- A control that is highly complex and requires technical details to explain
- A control that is preventive in nature

B is correct. Nontechnical controls include user training and written documents such as security policies. A, C, and D are incorrect. A technical control is a control that uses technical means within computer systems to reduce risk. A nontechnical control is not necessarily highly complex. Nontechnical controls can be preventive, detective, corrective, or a combination of these, so singling out their preventive role is not the best description.

Question 2

1 / 1 pts

Which of the following is the best choice to identify a system that requires a database to detect attacks?

- Anomaly-based IDS
- Signature-based IDS
- HIPS
- NIPS

B is correct. A signature-based intrusion detection system (IDS) compares activity to a signature file to identify attacks. A, C, and D are incorrect. An anomaly-based IDS requires a baseline. Both a host-based IPS (HIPS) and a network-based IPS (NIPS) can use either anomaly-based or signature-based detection methods.

Question 3

1 / 1 pts

An organization wants to monitor a server for intrusions. What should be used?

- HIDS

NIDS

Antivirus software

Host-based firewall

A is correct. A host-based IDS (HIDS) is installed on a system such as a server or workstation. It monitors activity on the host but cannot monitor network activity. B, C, and D are incorrect. A network-based intrusion detection system (NIDS) monitors traffic going through a network It uses agents to monitor traffic on routers and switches, and the agents forward the traffic to a central management console. Antivirus software monitors for malware. A host-based firewall is installed on a single server and can filter traffic, but it does not monitor for intrusions.

Question 4

1 / 1 pts

A security professional is performing a penetration test on a system. When should the penetration test stop?

At the completion of the vulnerability assessment

When the tested system fails

Before causing damage to a live system or network

After fully exploiting the vulnerability

C is correct. A penetration test should stop before causing damage to a live system or network. The goal is not to affect the mission or the organization, but instead to prove that the mission can be affected. A, B, and D are incorrect. A penetration test starts with a vulnerability assessment, so it wouldn't be stopped at the completion of the vulnerability assessment. A penetration test should stop before a system fails or before it has fully exploited the vulnerability.

Question 5

1 / 1 pts

A network is using an anomaly-based IDS. The administrators have modified the network by upgrading and changing some components. What be done to ensure that the IDS can accurately detect events?

- Reinstall the IDS
- Upgrade the IDS
- Update the signature database
- Update the baseline

D is correct. An anomaly-based intrusion detection system (IDS) attempts to document normal behavior in the form of a baseline, so if the normal behavior is modified by changing the environment, the baseline must be updated. A, B, and C are incorrect. It is not necessary to reinstall or upgrade the IDS. A signature-based (not anomaly-based) detection method uses signatures.

Question 6

1 / 1 pts

Of the following choices, what is NOT an example of a preventive control?

- Written policies and procedures
- Employee background checks
- Intrusion detection system
- Encryption of data

C is correct. An intrusion detection system is a detective control, not a preventive control. A, B, and D are incorrect. All of these answers are example of preventive controls.

Question 7

1 / 1 pts

Security administrators from within the organization are asked to perform a vulnerability test. They have full knowledge of the internal network. What type of vulnerability assessment will they do?

- White box
- Black box
- Gray box
- Zero knowledge

A is correct. In a white box test (also known as a full knowledge test), testers have full access to the internal network and know the network infrastructure, including what systems it hosts. B, C, and D are incorrect. In a black box test, testers don't ahve any knowledge of the internal network prior to starting the testing. External consultants hired to test an organization's security vulnerabilities often do black box testing. In a geray box test, testers have a least some level of knowledge about the network. Zero knowledge testing isn't an actual term, but it refers to black box testing where the testers have zero knowledge.

Incorrect

Question 8

0 / 1 pts

Attackers recently attacked a web server hosted within a demilitarized zone (DMZ). The network was protected with firewalls and intrusion detection systems, with each component logging events and forwarding some of the logs to a remote system. What logs are the most valuable to re-create the event during and prior to the attack?

- (●) Firewall logs on the web server
- ( ) System logs on the web server
- ( ) Logs on remotes systems
- ( ) Application logs on the web server

C is correct. After an attack, remote logs are the most valuable to re-create the events druing and prior to the attack. A, B, and D are incorrect. Any logs on a local sysem should be treated with suspicion because the attacker may have modified them.

Question 9

1 / 1 pts

Which of the following best describes a technical control?

- (●) A control that uses technical means within computer systems to reduce risk
- ( ) A control that uses training and written documents such as security policies to reduce risk
- ( ) A control that is highly complex and requires technical details to explain
- ( ) A control that is preventive in nature

A is correct. A technical control is a control that uses technical means within computer systems to reduce risk. B, C, and D are incorrect. Nontechnical controls include user training and written documents such as security policies. A technical control is not necessarily highly complex. Technical controls can be preventive, detective, corrective, or a combination of these.

Question 10

1 / 1 pts

Of the following choices, what is not a valid method of detection used by HIDSs?

- ( ) Anomaly-based
- ( ) Signature-based
- ( ) Knowledge-based
- (●) Reporting-based

D is correct. Reporting-based is not a valid method of detection used by any intrusion detection system IDS), including host-based intrusion detection system. A, B, and C are incorrect. A signature-based (sometimes called knowledge-based) detection method is similar in concept to antivirus signatures. Many attacks have unique characteristics documented in signature files. The IDS uses these signature files to identify and detect attacks. In an anomaly-based IDS, the IDS attempts to document normal behavior in the form of a baseline. It then monitors the activity and constantly compares it to the baseline, looking for anomalies.

Question 11

1 / 1 pts

An organization wants to monitor a critical server for intrusions. What should be used?

- (●) HIDS
- ( ) NIDS
- ( ) Signature-based IDS
- ( ) Network-based firewall

A is correct. A host-based intrusion detection system (HIDS) is installed on a system such as a server or workstation and monitors activity on the host. B, C, and D are incorrect. A network-based IDS (NIDS) monitors traffic going through a network. It uses agents monitoring traffic on routers and switches, and the agents forward the traffic to a Central management console. A signature-based IDS isn't required, but a host-based IDS is. A network-based firewall monitors network traffic.

Question 12

1 / 1 pts

You are designing a backup strategy for several key servers. You have time to do a full backup on Sunday, but you must minimize the amount of time needed to complete backups during other days of the week. What strategy should you use?

- Full backups daily
- Full/differential
- Full/incremental
- Daily copies

C is correct. A full/incremental backup strategy minimizes the time needed for backups during the week. However, the recovery can take longer because multiple backups may need to be restored to recover the data. A, B, and D are incorrect. Performing full backups daily would not reduce the amount of time needed to complete backups. A full/differential backup strategy takes longer to back up during the week than a full/incremental strategy. However, the recovery time is reduced because a maximum of two backups are needed to recover the data. Daily copies would not reduce the amount of time need to complete backups.

Incorrect

Question 13

0 / 1 pts

Of the following choices, what is NOT an example of a corrective control?

- A disaster recovery plan
- A backup and restore procedures
- An intrusion prevention system
- Forensic analysis

D is correct. Forensic analysis is a detective control, not a corrective control. A, B, and C are incorrect. All of the other answers are examples of corrective controls.

Question 14

1 / 1 pts

Your organization is considering restricting the software that can run on several isolated systems to specific applications. What is this called?

- Signature-based
- Anomaly-based
- Whitelisting
- MAC filtering

C is correct. Once type of whitelisting restricts the software that can run on a system to specific applications or services. A, B, and D are incorrect. Signature-based and anomaly-based are two types of detection methods for intrusion detection systems (IDS) and intrusion prevention systems (IPS), but they don't use whitelisting. Media access control (MAC) filtering is another type of whitelisting, but used MAC addresses to restrict traffic to specific systems.

Incorrect

Question 15

0 / 1 pts

You are designing a backup strategy for several key servers. You have time to do a full backup on Sunday, but not enough time to do full backups daily. Additionally, you must reduce the amount of time needed to complete a restore if needed.

What strategy should you use?

- Full backups daily
- Full/differential
- Full/incremental
- Daily copies

B is correct. A full/differential backup strategy takes longer to backup up during the week than a full/incremental strategy. However, the recovery time is reduced because a maximum of two backups is needed to recover the data. A, C, and D are incorrect. Performing full backups daily would not reduce the amount of time needed to complete backups. A full/incremental back strategy minimizes the time needed for backups during the week. However, the recovery can take longer because multiple backups may be needed to be restored to recover the data. Daily copies would not reduce the amount of time needed to complete backups.

Question 16

1 / 1 pts

A vulnerability assessment reported a vulnerability, but investigation shows that the vulnerability does not actually exist. What is this called?

- A false positive
- A false negative
- A penetration test failure
- A penetration test success

A is correct. A false positive occurs when a vulnerability assessment indicates that a vulnerability exists even though it doesn't. B, C, and D are incorrect. A false negative occurs when a vulnerability assessment indicates that a vulnerability doesn't exist even though it does. A vulnerability assessment result does not indicate success or failure of a penetration test.

Question 17

1 / 1 pts

An organization wants to ensure that users are aware of what they can and cannot do with IT systems owned and controlled by the organization. What should be used to document these guidelines?

- A security policy
- A configuration control policy
- An acceptable use policy
- A backup policy

C is correct. An acceptable use policy lets users know what they can and cannot do with IT systems owned and controlled by the organization. A, B, and D are incorrect. A security policy may include an acceptable use policy, but more often a separate use policy is implemented. A configuration control policy identifies procedures for configuration control, such as the use of images for baselines. A backup policy identifies what data should be backed up and how long data should be retained.

Question 18

1 / 1 pts

A critical database server is hosting data for a web farm. A recent outage on the database server resulted in substantial losses for the organization. You're asked what can be done to prevent a similar incident in the future. What do you suggest?

- Use a RAID implementation on the server
- Create a failover cluster
- Create redundant connections
- Identify an alternate location

B is correct. A failover cluster provides fault tolerance for one or more servers. A simple two-node failover cluster can ensure that if one server fails, the other server is available to take over without any loss of service. A, C, and D are incorrect. A Redundant Array of Independent/Inexpensive Disks (RAID) provides fault tolerance for disk subsystems. Redundant connections provide fault tolerance for network connections. An alternate location can be used if a disaster affects the entire site or location.

Question 19

1 / 1 pts

What type of controls is an Intrusion Detection System (IDS)?

- Administrative
- Corrective
- Detective
- Preventive

C is correct. An intrusion detection system (IDS) is detective in nature because it attempts to detect attacks that are in progress and provide notifications. A, B, and D are incorrect. Administrative controls focus on the management of risk and the management of IT security using managerial practices and written documents. A corrective control takes action to reverse the effects or impact of an event. A preventive control is focused on preventing losses due to risks. An intrusion prevention systems (IPS, not mentioned in this question) is both detective and corrective in nature because it can take actions to block detected attacks but it must detect the attack first.

Question 20

1 / 1 pts

Of the following choices, what is NOT an example of a detective control?

- Audit logs
- Employee background checks
- Intrusion detection systems
- Forensics analysis

B is correct. An employee background check is a preventive control, not a detective control. A, C, and D are incorrect. All are examples of detective controls.

Quiz Score: **17** out of 20