Exam Report: 3.3.4 Practice Questions

Date: 4/4/29 5:52:16 pm
Time Spent: 0:44

Candidate: Garsteck, Matthew
Login: mGarsteck

Overall Performance

Your Score: 0%

Passing Score: 80%

View results by: ○ Objective Analysis ● Individual Responses

Individual Responses

Question 1: Incorrect

You have implemented a regular backup schedule for a Windows system, backing up data files every night and creating a system image backup once per week. For security reasons, your company has decided not to store a redundant copy of the backup media at an off-site location. Which of the following would be the best backup and storage option?

● ~~Use differential backups and store them in a locked room.~~

➡ ○ Use incremental backups and store them in a locked fireproof safe.

○ Use differential backups and store them on a shelf next to the backup device.

○ Use incremental backups and store them in a drawer in your office.

Explanation

Incremental backups back up every file that's changed since the last full or incremental backup. If you can't store backups at an off-site location, you should make sure that the backups are locked up and that measures are taken to protect the backups from a disaster.

Differential backups back every file that's changed since the last full backup.

Strategies such as locking the backups in a different room, keeping them on a shelf, or storing them in a drawer would not protect the backup against natural disasters.

References

TestOut Ethical Hacker Pro - 3.3 Countermeasures and Prevention
[e_counter_prev_eh1.exam.xml Q_COUNTER_PREV_BACKUP_01_EH1]

Question 2: Incorrect

You are in the process of implementing policies and procedures that require employee identification. You observe employees holding a secure door for others to pass through. Which of the following training sessions should you implement to help prevent this in the future?

○ Why employees should wear their badge at all times.

○ Why employees should never share their ID badge with anyone.

● ~~What to do if you encounter a person without a badge.~~

➡ ○ How to prevent piggybacking and tailgating.

Explanation

Piggybacking implies that the person who has opened the door with their credentials knows that others are following them in through the secure door.

Tailgating means that others are following through the door without the knowledge of the person who has opened the door.

ID badges are a great and easy way to identify who is authorized to be in a given area. Employees should be trained to:

- Wear their badge at all times.
- Respond appropriately if they encounter a person without a badge.
- Prevent piggybacking and tailgating.
- Never share their ID badge with anyone.

References

TestOut Ethical Hacker Pro - 3.3 Countermeasures and Prevention
[e_counter_prev_eh1.exam.xml Q_COUNTER_PREV_EMPLOYEE_01_EH1]

▼ Question 3: Incorrect

You have a set of DVD-RW discs that were used to archive files from your latest project. You need to prevent the sensitive information on the discs from being compromised. Which of the following methods should you use to destroy the data?

○ Delete the data on the discs.

● ~~Degauss the discs.~~

➡ ○ Shred the discs.

○ Write junk data on the discs.

Explanation

To completely prevent reading data from discs, destroy them using a DVD shredder or crushing.

Degaussing only works for magnetic media such as floppy and hard disk drives.

Simply deleting data offers little protection.

Overwriting the data is not efficient in this scenario as the discs can simply be destroyed.

References

TestOut Ethical Hacker Pro - 3.3 Countermeasures and Prevention
[e_counter_prev_eh1.exam.xml Q_COUNTER_PREV_PAPER_SHRED_01_EH1]

▼ Question 4: Incorrect

Which of the following best describes a physical barrier used to deter an aggressive intruder?

○ Alarmed carrier PDS

● ~~Anti-passback system~~

○ Double-entry doors

➡ ○ Large flowerpots

Explanation

Just as ID badges are an easy way to identify people, bollards are an easy physical barrier to deter aggressive intruders. Bollards can be small straight concrete pillars, flat barricades, ball shaped pieces of concrete, large flowerpots, or even cement picnic tables. The idea is to prevent attackers from forcing themselves in by driving through an exterior wall or door.

A double-entry door has two doors that are locked from the outside but have crash bars on the inside that allow easy exit. Double-entry doors are typically used only for emergency exits, and alarms sound when the doors are opened.

An anti-passback system prevents a card holder from passing their card back to someone else.

In an alarmed carrier PDS , the welds and/or glue used to secure a hardened carrier are replaced with an electronic alarm system that can detect attempts to compromise the carrier and access the protected cable within it.

References

TestOut Ethical Hacker Pro - 3.3 Countermeasures and Prevention
[e_counter_prev_eh1.exam.xml Q_COUNTER_PREV_PHYS_PREVENT_01_EH1]

Question 5: Incorrect

Joe, a bookkeeper, works in a cubicle environment and is often called away from his desk. Joe doesn't want to sign out of his computer each time he leaves. Which of the following is the best solutions for securing Joe's workstation?

○ Apply multifactor authentication on his computer.

○ Change the default account names and passwords.

● ~~Set a strong password, that require special characters.~~

➡ ○ Configure the screen saver to require a password.

Explanation

The best solution is to configure the screen saver or screen lock to be applied after a short period of nonuse and to require a password to return to the desktop.

Setting a strong password will not secure his computer when he is called away. Setting a strong password is a best practice.

Applying multifactor authentication will make it harder to hack the workstation. However; this will not secure his computer when he is called away.

Changing the default account names and passwords will not make his workstation more secure when he is called away.

References

TestOut Ethical Hacker Pro - 3.3 Countermeasures and Prevention
[e_counter_prev_eh1.exam.xml Q_COUNTER_PREV_USER_AWARE_01_EH1]