Exam Report: 13.3.8 Practice Questions

Date: 4/15/2020 4:21:56 pm
Time Spent: 1:56

Candidate: Garsteck, Matthew
Login: mGarsteck

Overall Performance

Your Score: 13%

Passing Score: 80%

View results by: Objective Analysis Individual Responses

Individual Responses

Question 1: Correct

A public library has purchased a new laptop computer to replace their older desktop computers and is concerned that they are vulnerable to theft.

Which of the following laptop features should be used to physically secure the laptop?

- A multi-factor password policy
- Biometric authentication
- A cable lock
- An external encryption device

Explanation

A cable lock can be used to physically secure a laptop to deter theft.

Biometric authentication does not physically secure a laptop. A multi-factor password policy does not physically secure a laptop. An external encryption device does not physically secure a laptop.

References

TestOut PC Pro - 13.3 Physical Security
[e_phys_pp6.exam.xml Q_SEC_PHY_01]

Question 2: 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 are the BEST solutions for securing Joe's workstation? (Select TWO).

- [ ] Configure the screen lock to be applied after short period of nonuse.
- [x] ~~Set a strong password.~~
- [ ] Configure the screen saver to require a password.

☐ Change the default account names and passwords.

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 is a best practice, but is not the best solution in this scenario. Applying multifactor authentication will make it harder to hack the workstation, but is not the best solution in this scenario. Change the default account names and passwords will make the workstation more secure, but is not the best solution in this scenario.

References

TestOut PC Pro - 13.3 Physical Security
[e_phys_pp6.exam.xml Q_SEC_PHY_02]

Question 3: Incorrect

You are a security consultant and have been hired to evaluate an organization's physical security practices. All employees must pass through a locked door to enter the main work area. Access is restricted using a biometric fingerprint lock.

A receptionist is located next to the locked door in the reception area. She uses an iPad application to log any security events that may occur. She also uses her iPad to complete work tasks as assigned by the organization's CEO.

Network jacks are provided in the reception area such that employees and vendors can access the company network for work-related purposes. Users within the secured work area have been trained to lock their workstations if they will be leaving them for any period of time.

Which of the following recommendations are you MOST likely to make to this organization to increase their security? (Select TWO).

➡ ☐ Train the receptionist to keep her iPad in a locked drawer when not in use.

➡ ☑ Disable the network jacks in the reception area.

☐ Replace the biometric locks with smart cards.

☐ Require users to use screensaver passwords

☑ ~~Move the receptionist's desk into the secured area.~~

Explanation

You should recommend the following:

- Disable the network jacks in the reception area. Having these jacks in an unsecured area allows anyone who comes into the building to connect to the company's network.
- Train the receptionist to keep her iPad in a locked drawer when not in use. Tablet devices are small and easily stolen if left unattended.

The receptionist's desk should remain where it is currently located because it allows her to visually verify each employee as they access the secured area. Biometric locks are generally considered more secure than smart cards because cards can be easily stolen. Training users to lock their workstations is more secure

References

TestOut PC Pro - 13.3 Physical Security
[e_phys_pp6.exam.xml Q_SEC_PHY_03]

Question 4: Incorrect

You have 5 salespersons who work out of your office and who frequently leave their laptops laying on their desk in their cubicles. You are concerned that someone might walk by and take one of these laptops.

Which of the following is the BEST protection to implement to address your concerns?

- Implement screen saver passwords.
- Encrypt all company data on the hard drives.
- Use cable locks to chain the laptops to the desks.
- ~~Require strong passwords in the local security policy.~~

Explanation

The main concern in this case is with laptops being stolen. The best protection against physical theft is to secure the laptops in place using a cable lock. Requiring strong passwords or using encryption might prevent unauthorized users from accessing data on the laptops, but does not prevent physical theft.

References

TestOut PC Pro - 13.3 Physical Security
[e_phys_pp6.exam.xml Q_SEC_PHY_04]

Question 5: 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 a week. For security reasons, your company has decided to not store a redundant copy of the backup media at an offsite location.

Where would be the next best place to keep your backup media?

- On a shelf next to the backup device.
- In a locked fireproof safe.
- In a drawer in your office.
- ~~In a locked room.~~

Explanation

If you can't store backup tapes at an offsite location, you should make sure that the backup tapes are locked up (for security), and that measures are taken to protect the tapes from a disaster (such as a fire).

Strategies such as locking the tapes in a different room, keeping them on a shelf, or storing them in a drawer do not address both concerns.

[e_phys_pp6.exam.xml Q_SEC_PHY_05]

Question 6: Incorrect

You are responsible for disposing of several old workstations formerly used by accountants in your organization's Finance department. Before being shipped to a computer recycler, you decide to make sure any old data on the hard drives is erased. To do this, you use the Windows XP Installation CDs that came with these systems to delete all partitions from the hard drives.

Which of the following BEST describes what needs to be done before the systems are ready to be recycled?

- ~~Nothing, the systems are ready to be recycled.~~
- Use a Linux fdisk utility to completely remove the partitions on the systems.
- Use disk wiping software to fully erase the drives on the systems.
- Repartition and reformat the drives on the systems before disposal.

Explanation

You should use disk wiping software to fully erase the drives. The problem here is that partitioning and even reformatting doesn't completely remove old data from the drive. Data could potentially be recovered from the drive. To keep this from happening, you should use disk wiping software to erase the drive and write random characters multiple times to the drive to completely destroy any old data.

References

TestOut PC Pro - 13.3 Physical Security
[e_phys_pp6.exam.xml Q_SEC_PHY_06]

Question 7: Incorrect

You have purchased new computers and will be disposing of your old computers. Instead of recycling the computers, you decide to resell them by placing an ad on the Internet. These computers were previously used for storing sensitive information.

To properly protect the accidental discovery of the company's sensitive information, which of the following steps MUST be completed prior to getting rid of the computers?

- Delete user data and applications from the hard drives
- ~~Reformat the hard drives~~
- Include the original operating system discs and product keys with the computers
- Use data wiping software to clear the hard drives

Explanation

Data wiping software will sanitize or clean a device by removing all data remnants. Sanitization is necessary because deleting, overwriting, and reformatting (even multiple times) does not remove all data remnants. Sanitization securely removes sensitive data from storage media and is designed to solve the data remanence

Deleting data and applications from the hard drives or reformatting the drive will not permanently remove data from the system. Many tools can recover deleted files.

References

TestOut PC Pro - 13.3 Physical Security
[e_phys_pp6.exam.xml Q_SEC_PHY_07]

Question 8: Incorrect

You have a set of DVD-RW discs that have been used to archive files for your latest development project. You need to dispose of the discs.

Which of the following methods should you use to BEST prevent extracting data from the discs?

- Degaussing
- Write junk data over the discs 7 times
- Shredding
- ~~Delete the 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 multiple times is not efficient in this scenario as the discs can simply be destroyed.

References

TestOut PC Pro - 13.3 Physical Security
[e_phys_pp6.exam.xml Q_SEC_PHY_08]

Question 9: Incorrect

You have purchased new computers and will be disposing of your old computers. These computers were previously used for storing highly-sensitive customer order information, including credit card numbers.

To properly protect the accidental discovery of the company's sensitive information, which of the following steps MUST be completed prior to getting rid of the computers?

- Repartition the hard drives.
- Reinstall a fresh copy of Windows on the drives.
- Physically destroy the hard drives with a hammer.
- ~~Delete user data and applications from the hard drives.~~
- Reformat the hard drives.

Explanation

Reinstalling Windows, repartitioning the drives, or even reformatting them will not remove all data remnants. Deleting data and applications from the hard drives also will not permanently remove data from the system.

References

TestOut PC Pro - 13.3 Physical Security
[e_phys_pp6.exam.xml Q_SEC_PHY_09]

Question 10: Incorrect

While reviewing video files from your organization's security cameras, you notice a suspicious person using piggy-backing to gain access to your building. The individual in question did not have a security badge.

Which of the following would you MOST likely implement to keep this from happening in the future?

- Door locks with card readers
- Mantraps
- ~~Cable locks~~
- Lo-jack recovery service

Explanation

You could implement mantraps at each entrance to the facility. A mantrap is a specialized entrance with two doors that creates a security buffer zone between two areas. Once a person enters into the space between the doors, both doors are locked. To enter the facility, authentication must be provided. If authentication is not provided, the intruder is kept in the mantrap until authorities arrive.

Cable locks are used to secure computer hardware. Lo-jack recovery services are used to locate stolen or misplaced computer hardware. Door locks with card readers were already circumvented in this scenario using the piggy-backing technique.

References

TestOut PC Pro - 13.3 Physical Security
[e_phys_pp6.exam.xml Q_SEC_PHY_10]

Question 11: Incorrect

You provide desktop support at the branch office of a bank. One of the Windows workstations you manage is used by a bank employee to set up new customer accounts and fill out customer loan applications. Each user account on the system has been assigned a strong password. A cable lock has been installed to prevent it from being stolen.

Which of the following steps could be completed to BEST increase the security of this system? (Select TWO).

- [ ] Move the system to a locked room
- [x] ~~Disconnect the system from the network~~
- [ ] Disable the network jack to which the system is connected

- [x] Disable all USB ports in the BIOS/UEFI firmware configuration
- [ ] Remove the optical drive

Explanation

Because this system is used in a public are in close proximity to customers, you should disable all USB ports in the BIOS/UEFI firmware configuration and also remove the optical drive if it is capable of burning optical discs. This will help prevent data from being stolen from the system if it is left unattended.

Because this system is used by bank personnel to service customers, it really can't be locked in a separate room. Likewise, disconnecting from the network or disabling its network jack would also make it unable to perform its required function.

References

TestOut PC Pro - 13.3 Physical Security
[e_phys_pp6.exam.xml Q_SEC_PHY_11]

Question 12: Incorrect

Your client has hired you to evaluate their wired network security posture. As you tour their facility, you note the following:

- Server systems are kept in a locked server room.
- User accounts on desktop systems have strong passwords assigned.
- A locked door is used to control access to the work area. Users must use ID badges to enter the area.
- Users connect their personal mobile devices to their computers using USB cables.
- Users work in three 8-hour shifts per day. Each computer is shared by three users. Each user has a limited account on the computer they use.

Based on this information, which of the following would you MOST likely recommend your client do to increase security?

- ( ) Move the server systems to an empty cubicle in the work area.
- (•) ~~Assign users easy-to-remember simple passwords so they won't be tempted to write them down.~~
- ( ) Provision each employee with their own computer system.
- ( ) Disable the USB ports on user's workstations.

Explanation

Users connecting their personal mobile devices to their computers using USB cables represents a significant security risk. Malware could be spread throughout the network. They could also copy sensitive information from the network to the device. Disabling all USB ports on all workstations will prevent this from happening. You should configure the BIOS/UEFI firmware with a password to prevent users from re-enabling the ports.

Moving the server to an empty cubicle and assigning simple passwords will decrease the overall security of the network. It isn't necessary for each employee to have their own dedicated computer system.

TestOut PC Pro - 13.3 Physical Security
[e_phys_pp6.exam.xml Q_SEC_PHY_12]

Question 13: Correct

A technician upgrades the hard drive on a computer in the accounting department and decides to donate the old drive to a local trade school.

Which of the following is the BEST method to ensure that the accounting data can't be recovered?

- Standard format
- Degauss
- diskpart format
- Drive wipe

Explanation

Drive wipe is a software-based method of overwriting the actual data that makes up files on the hard drive. The overwriting process is performed multiple times to remove the magnetic traces of previous data. The drive remains usable after a disk wipe.

A standard format removes only the reference to files and does not remove the actual data that made up the files. Software tools can easily recover this data.

Degaussing a disk removes the data, but also removes lower-level formatting making the disk unusable for the local trade school.

Like a standard format, data from a disk that is repartitioned using diskpart can be recovered.

References

TestOut PC Pro - 13.3 Physical Security
[e_phys_pp6.exam.xml Q_SEC_PHY_DATA_DESTRUCTION_01]

Question 14: Incorrect

A technician wants to destroy the data on a hard drive and repurpose it as a spare drive.

Which of the following data destruction methods allow the reuse of the hard drive?

- Degaussing
- ~~Shredding~~
- Incineration
- Drive wipe

Explanation

Drive wipe is a software-based method of overwriting the actual data that makes up files on the hard drive. The overwriting process is performed multiple times to remove the magnetic traces of previous data. The drive remains usable after a disk

Incineration completely destroys both the data and the physical hard drive.

Degaussing destroys the data on a hard drive, but also removes the low-level formatting. Degaussing can also destroy the electronic hardware in the drive. In either case, the drive will be unusable.

Shredding completely destroys both the data and the physical hard drive.

References

TestOut PC Pro - 13.3 Physical Security
[e_phys_pp6.exam.xml Q_SEC_PHY_DATA_DESTRUCTION_03]

Question 15: Incorrect

Jose, a medical doctor, has a mobile device that contains sensitive patient information. He is concerned about unauthorized access to the data if the device is lost or stolen.

Which of the following is the BEST option to prevent this from happening?

- Configure the device to wipe after a number of failed login attempts.
- ~~Install a locator application on the device so that it can be traced.~~
- Configure the device for multifactor authentication.
- Configure the device to remote wipe as soon as it reported lost.

Explanation

Mobile devices can be configured to be perform a factory reset or wipe when the device is reported lost or stolen. This is the BEST of the presented options.

Configuring the device for multifactor authentication will make it harder to hack, but is not the best solution presented.

Installing a locator application on the device makes it possible to trace, but is not the best solution presented.

Configuring the device to wipe after a number of failed login attempts is a good solution, but not the best solution presented.

References

TestOut PC Pro - 13.3 Physical Security
[e_phys_pp6.exam.xml Q_SEC_PHY_SECURE_MOBILE_DEVICES_02]