Exam Report: 13.1.5 Practice Questions

Date: 4/15/2020 3:55:55 pm Candidate: Garsteck, Matthew
Time Spent: 7:20 Login: mGarsteck

Overall Performance

Your Score: 64%

Passing Score: 80%

View results by: Objective Analysis Individual Responses

Individual Responses

Question 1: Correct

During an airline flight, a laptop user makes last-minute changes to a presentation that contains sensitive company information.

Which of the following would make it difficult for other passengers to view this information on the laptop display?

- Privacy filter
- Mantrap
- Smart card
- Cable lock

Explanation

A privacy filter narrows the viewing angle of the laptop display so that only the person directly in front can see the display.

A cable lock can be used to secure valuable items that can be easily removed from the workplace, like laptops. It would do nothing to prevent others from viewing the laptop display. Smart cards can provide authentication, but do nothing to prevent others from viewing the laptop display. A mantrap is used to control access between two areas that have different security levels. It helps prevent tailgating by requiring that the entry into the mantrap from one area close before entry to the second area is possible.

References

TestOut PC Pro - 13.1 Security Best Practices
[e_best_pp6.exam.xml Q_WS_SEC_01]

Question 2: Correct

A technician assists Joe, an employee in the sales department who needs access to the client database, by granting him administrator privileges. Later, Joe discovers he has access to the salaries in the payroll database.

Which of the following security practices was violated?

- Principle of least privilege
- Entry control roster

- ◯ Multifactor authentication
- ◯ Strong password policy

Explanation

The technician violated the principle of least privilege, the practice of limiting access rights for users to the bare minimum permissions they need to perform their work.

Strong passwords are recommended to prevent unauthorized access, but in this scenario, the database is not password-protected. Multifactor authentication is the process of authenticating a user by validating two or more claims presented by the user, each from a different category, such as a password and the possession of a mobile phone, or a password and a fingerprint. Security personnel can grant access to a physical area using the entry control roster. A database is not normally protected by physical security.

References

TestOut PC Pro - 13.1 Security Best Practices
[e_best_pp6.exam.xml Q_WS_SEC_02]

Question 3: Incorrect

Employees in a small business have a habit of transferring files between computers using a USB flash drive and often bring in files from outside the company. Recently, a computer was infected with malware from a USB flash drive even though the employee did not access any files.

Which of the following options would prevent this issue in the future?

- ◯ Set strong passwords.
- ➡ ◯ Disable autorun.
- ◉ ~~Configure screen savers to require a password.~~
- ◯ Enable BitLocker.

Explanation

Disabling autorun would prevent the malware from installing when the flash drive was attached.

Setting strong passwords is a best practice, but would not prevent the malware on a flash drive from installing. BitLocker is used to encrypt drives and will not prevent malware on a flash drive from installing. Configure screen savers to require a password is a best practice, but would not prevent the malware on a flash drive from installing.

References

TestOut PC Pro - 13.1 Security Best Practices
[e_best_pp6.exam.xml Q_WS_SEC_03]

Question 4: Correct

Bob calls and complains that he has suddenly started getting a lot of unwanted email.

Which of the following is the BEST type of software to install to help solve Bob's problem?

- ○ Anti-malware
- ○ Anti-plagiarism
- ○ Anti-virus
- ➡ ◉ Anti-spam

Explanation

In computer terms, SPAM email (or junk email) is the unsolicited email users receive. One of the best ways to prevent receiving this type of email is to use anti-spam software.

Anti-malware software helps protects a computer from software that is intentionally designed to cause harm or damage to your computer. Anti-virus software helps protect the infiltration and spread of malicious code that is designed to alter the way a computer operates. Anti-plagiarism software helps detect when someone has plagiarized someone else's material.

References

TestOut PC Pro - 13.1 Security Best Practices
[e_best_pp6.exam.xml Q_WS_SEC_04]

Question 5: Incorrect

Which of the following security practices are the BEST example of the principle of least privilege?

- ➡ ○ All users on a Windows workstation are limited users except for one user, who is responsible for maintaining the system.
- ○ All users on a Windows workstation have been assigned strong passwords.
- ○ The Guest user account on a Windows workstation has been disabled.
- ◉ ~~Autorun has been disabled on a Windows workstation.~~

Explanation

The principle of least privilege specifies that users should have only the degree of access to the workstation necessary for them to complete their work and no more. Making all users limited users except for those who need administrative access is an example of the principle of least privilege.

The other practices listed are workstation security best practices, but are not necessarily examples of the principle of least privilege.

References

TestOut PC Pro - 13.1 Security Best Practices
[e_best_pp6.exam.xml Q_WS_SEC_05]

Question 6: Correct

Which are examples of a strong password? (Select TWO).

- ☐ Morganstern
- ➡ ☑ TuxP3nguinsRn0v3l

- [ ] skippy
- [x] il0ve2EatIceCr3am
- [ ] NewYork

Explanation

A strong password is one that:

- Is at least 6 characters long (longer is better)
- Is not based on a word found in a dictionary
- Contains both upper-case and lower-case characters
- Contains numbers
- Does not contain words that can be associated with you personally
- Is changed frequently

The passwords *il0ve2EatIceCr3am* and *TuxP3nguinsRn0v3l* both meet the above criteria.

The password *NewYork* is long enough and includes upper- and lower-case letters, but it doesn't contain numbers and could be easily dissected into a dictionary word. The password *skippy* is probably a pet name. The password *Morganstern* is probably someone's last name (perhaps a spouse's name or a maiden name).

References

TestOut PC Pro - 13.1 Security Best Practices
[e_best_pp6.exam.xml Q_WS_SEC_06]

Question 7: Correct

One of the Windows workstations you manage has four user accounts defined on it. Two of the users are limited users while the third (your account) is an administrative user. The fourth account is the Guest user account, which has been enabled to allow management employees convenient workstation access.

Each limited and administrative user has been assigned a strong password. File and folder permissions have been assigned to prevent users from accessing each other's files. Autorun has been disabled on the system.

Which of the following actions is MOST likely to increase the security of this system?

- ( ) Enable autorun on the system.
- (•) Disable the Guest account.
- ( ) Change the two limited user accounts to administrative users.
- ( ) Change your user account to a limited user.

Explanation

The Guest user account has no password and provides too much access to the system. Unless you have an overriding reason to do so, the Guest user account should remain disabled.

Changing your administrative user account to a limited user would prevent you from completing management tasks on the workstation. Changing the two limited user accounts to administrative users would decrease the security of the system as would enabling autorun functionality.

References

TestOut PC Pro - 13.1 Security Best Practices
[e_best_pp6.exam.xml Q_WS_SEC_07]

Question 8: Incorrect

One of the Windows workstations you manage has three user accounts defined on it. Two of the users are limited users while the third (your account) is an administrative user.

Each limited and administrative user has been assigned a strong password. File and folder permissions have been assigned to prevent users from accessing each other's files.

Which of the following would MOST likely increase the security of this system? (Select TWO).

- ~~Change the two limited user accounts to restricted users.~~
- Disable autorun on the system.
- Set a screensaver password.
- Enable the Guest account.
- Assign each user a simple password so they won't be tempted to write it down.

Explanation

You could increase the overall security of this system by disabling autorun on the system and setting a screensaver password.

Enabling the Guest user account would decrease the security of the system, as would assigning simple passwords to user accounts. There's no such thing as a restricted user on Windows operating systems.

References

TestOut PC Pro - 13.1 Security Best Practices
[e_best_pp6.exam.xml Q_WS_SEC_08]

Question 9: Correct

You provide desktop support at the branch office of a bank. One of the Windows workstations you manage is used to set up new customer accounts and fill out customer loan applications. Each user account on the system has been assigned a strong password. File and folder permissions have been assigned to prevent users from accessing each other's files.

Which of the following would MOST likely increase the security of this system? (Select TWO. Each option is a complete solution.)

- Enable the Guest account.
- Secure the computer system to the desk with a cable lock.
- Install a privacy filter on the monitor.
- Assign each user a simple password so they won't be tempted to write it down.

- [ ] Make user accounts members of the Administrators group.

Explanation

Because this system is used in close proximity to customers, you should install a privacy filter on the monitor. The privacy filter prevents customers from viewing sensitive information displayed on the monitor (such as usernames, passwords, and account numbers).

You should also secure this system to the desk with a cable lock. Securing the computer to the desk prevents a malicious person from stealing the computer and all of the sensitive information it contains. Enabling the Guest user account would decrease the security of the system as would assigning simple passwords to user accounts and making all users members of the Administrators group.

References

TestOut PC Pro - 13.1 Security Best Practices
[e_best_pp6.exam.xml Q_WS_SEC_09]

Question 10: Correct

Anna, a home office user, employs a technician to check the security on a computer that was hacked. The technician discovers that the user's password is the name of Anna's dog and hasn't been changed in over a year.

Which of the following security best practices should the technician recommend? (Select TWO).

- [x] Require a strong password.
- [ ] Restrict user permissions.
- [ ] Set the number of failed password attempts to two.
- [x] Set a password expiration period.
- [ ] Configure the screen saver to require a password.

Explanation

Strong passwords are harder to hack, and they should be changed frequently.

Screen saver passwords may not be needed in a home office environment. Restricting user permissions for Ann will not increase security. Setting a lower number of password attempts may not be warranted in a home office environment.

References

TestOut PC Pro - 13.1 Security Best Practices
[e_best_pp6.exam.xml Q_WS_SEC_POL_01]

Question 11: Incorrect

Match each security policy on the left with the appropriate description on the right. Each security policy may be used once, more than once, or not at all.

Provides a high-level overview of the organization's security program.

Organizational Security Policy

Defines an employee's rights to use company property.

Acceptable Use Policy

Identifies the requirements for credentials used to authenticate to company-owned systems.

✓ Password Policy

Identifies a set of rules or standards that define personal behaviors.

✓ Code of Ethics

Sets expectations for user privacy when using company resources.

~~Organizational Security Policy~~ Acceptable Use Policy

Specifies that user accounts should be locked after a certain number of failed login attempts.

✓ Password Policy

Explanation

An Organizational Security Policy is a high-level overview of the organization's security program. An Acceptable use Policy (AUP) defines an employee's rights to use company property. The AUP should also set expectations for user privacy when using company resources. Password Policy identifies the requirements for passwords used to authenticate to company-owned systems. For example, this policy may specify that user accounts should be disabled or locked out after a certain number of failed login attempts.

References

TestOut PC Pro - 13.1 Security Best Practices
[e_best_pp6.exam.xml Q_WS_SEC_POL_02]