Exam Report: 13.8.8 Practice Questions

Date: 4/15/2020 5:09:15 pm
Time Spent: 1:39

Candidate: Garsteck, Matthew
Login: mGarsteck

Overall Performance

Your Score: 60%

Passing Score: 80%

View results by: Objective Analysis Individual Responses

Individual Responses

Question 1: Incorrect

Which of the following security solutions would prevent a user from reading a file which she did not create?

- ~~BitLocker~~
- VPN
- EFS
- IPSec

Explanation

EFS is a Windows file encryption option that encrypts individual files so that only the user who created the file can open it. Decryption is automatic when the file owner opens it. Other users cannot open the encrypted file unless specifically authorized. BitLocker is a Microsoft security solution which encrypts the entire contents of a hard drive, protecting all files on the disk. BitLocker uses a special key which is required to unlock the hard disk. You cannot unlock/decrypt a drive simply by moving it to another computer.

A virtual private network (VPN) uses an encryption protocol (such as IPSec, PPTP, or L2TP) to establish a secure communication channel between two hosts, or between one site and another site. Data that passes through the unsecured network is encrypted and protected.

References

TestOut PC Pro - 13.8 File Encryption
[e_encrypt_pp6.exam.xml Q_SEC_DATA_01]

Question 2: Incorrect

Which of the following protocols establish a secure connection and encrypt data for a VPN? (Select THREE).

- PPTP
- FTP

- [x] IPSec
- [x] L2TP

Explanation

A virtual private network (VPN) uses an encryption protocol (such as IPSec, PPTP, or L2TP) to establish a secure communication channel between two hosts, or between one site and another site. Data that passes through the unsecured network is encrypted and protected.

The Remote Desktop Protocol (RDP) is used by Windows Terminal Services based applications, including Remote Desktop. FTP is used for transferring files and will not establish a secure connection.

References

TestOut PC Pro - 13.8 File Encryption
[e_encrypt_pp6.exam.xml Q_SEC_DATA_02]

Question 3: Incorrect

Which of the following forms of networking is highly susceptible to eavesdropping (data interception) and must be secured accordingly?

- ISDN
- Satellite
- Wireless
- ~~Dial up~~
- DSL

Explanation

All forms of networking are potentially vulnerable to eavesdropping. Wireless networks by definition broadcast network transmissions openly and therefore can be detected by outsiders. Subsequently wireless networks should maintain data encryption to minimize the risk of transmitting information to unintended recipients.

References

TestOut PC Pro - 13.8 File Encryption
[e_encrypt_pp6.exam.xml Q_SEC_DATA_03]

Question 4: Correct

Which of the following provides the BEST security for wireless networks?

- WPA2
- WAP
- WEP
- 802.11a

Explanation

Wi-Fi Protected Access (WPA) provides encryption and user authentication for wireless networks.

Wired Equivalent Privacy (WEP) also provides security, but WPA is considered more secure than WEP. A wireless access point (WAP) is a hardware device, like a switch, that provides access to the wireless network. 802.11a is a wireless networking standard that defines the signal characteristics for communicating on the wireless network. CSMA/CD is a media access control method that controls when a device can communicate on the network.

References

TestOut PC Pro - 13.8 File Encryption
[e_encrypt_pp6.exam.xml Q_SEC_DATA_04]

Question 5: Correct

Which of the following wireless security methods uses a common shared key configured on the wireless access point and all wireless clients?

- WPA Personal and WPA2 Personal
- WEP, WPA Personal, and WPA2 Personal
- WPA Enterprise and WPA2 Enterprise
- WEP
- WEP, WPA Personal, WPA Enterprise, WPA2 Personal, and WPA2 Enterprise

Explanation

Shared key authentication can be used with WEP, WPA, and WPA2. Shared key authentication used with WPA and WPA2 is often called WPA Personal or WPA2 Personal.

WPA Enterprise and WPA2 Enterprise use 802.1x for authentication. 802.1x authentication uses usernames and passwords, certificates, or devices such as smart cards to authenticate wireless clients.

References

TestOut PC Pro - 13.8 File Encryption
[e_encrypt_pp6.exam.xml Q_SEC_DATA_05]

Question 6: Correct

A VPN is used primary for what purpose?

- Support the distribution of public Web documents
- Support secured communications over an untrusted network
- Allow the use of network-attached printers
- Allow remote systems to save on long distance charges

Explanation

All of the other items listed in this question are benefits or capabilities that are secondary to this primary purpose.

References

TestOut PC Pro - 13.8 File Encryption
[e_encrypt_pp6.exam.xml Q_SEC_DATA_06]

Question 7: Correct

A user stores sensitive data on a USB flash drive.

Which of the following can be used to encrypt the data on this drive?

- Bitlocker To Go
- Run as administrator
- Administrative share
- Single sign-on

Explanation

Bitlocker To Go can be used to encrypt a USB flash drive.

A single sign-on permits a user and their programs to use their credentials to automatically log in to other sites and services. It's not used for encryption. Run as administrator is used to run an application with elevated privileges, not to encrypt data. An administrative share is used by administrators to access system drives. It's not used for encryption.

References

TestOut PC Pro - 13.8 File Encryption
[e_encrypt_pp6.exam.xml Q_SEC_BITLOCKER_01]

Question 8: Incorrect

A user has a file that contains sensitive data.

Which of the following can be used to encrypt a single file?

- ~~BitLocker~~
- EFS
- Single sign-on
- Administrative share

Explanation

Encrypting File Server (EFS) is a Windows feature that can be used to encrypt a single file or multiple files and folders.

BitLocker is a Windows feature that encrypts an entire disk. A single sign-on permits a user and their programs to use their credentials to automatically log in to other sites and services; it's not used for encryption. An administrative share is used by administrators to access system drives; it's not used for encryption.

TestOut PC Pro - 13.8 File Encryption
[e_encrypt_pp6.exam.xml Q_SEC_BITLOCKER_02]

Question 9: Correct

You want a security solution that protects the entire hard drive, preventing access even when it is moved to another system.

Which of the following is the BEST method for achieving your goals?

- BitLocker
- IPsec
- EFS
- VPN

Explanation

BitLocker is a Microsoft security solution that encrypts the entire contents of a hard drive, protecting all files on the disk. BitLocker uses a special key, which is required to unlock the hard disk. You cannot unlock/decrypt a drive simply by moving it to another computer.

EFS is a Windows file encryption option, but only encrypts individual files. Encryption and decryption is automatic and dependent upon the file's creator and whether other uses have read permissions. A virtual private network (VPN) uses an encryption protocol (such as IPsec, PPTP, or L2TP) to establish a secure communication channel between two hosts or between one site and another site. Data that passes through the unsecured network is encrypted and protected.

References

TestOut PC Pro - 13.8 File Encryption
[e_encrypt_pp6.exam.xml Q_SEC_BITLOCKER_03]

Question 10: Correct

Which of the following components is a special hardware chip included on the computer motherboard that contains software in firmware that generates and stores cryptographic keys?

- USB device
- BitLocker partition
- Trusted Platform Module (TPM)
- BIOS/UEFI

Explanation

A Trusted Platform Module (TPM) is a special hardware chip included on the computer motherboard that contains software in firmware that generates and stores cryptographic keys.

The TPM chip must be enabled in the BIOS/UEFI. A USB device is used to save the BitLocker key on a system that does not have a TPM chip. Implementing BitLocker requires two NTFS partitions.

TestOut PC Pro - 13.8 File Encryption
[e_encrypt_pp6.exam.xml Q_SEC_BITLOCKER_04]