Section Quiz

Candidate: Dunkan Gibson (dunkan.gibson)
Date: 3/8/2022 7:18:49 pm • Time spent: 03:01

Score: 90% Passing Score: 80%

Question 1: ✔ Correct

You create a new document and save it to a hard drive on a file server on your company's network. Then you employ an encryption tool to encrypt the file using AES. This activity is an example of accomplishing which security goal?

- Non-repudiation
- Availability
- Confidentiality
- Integrity

EXPLANATION

Encrypting a file while it is stored on a hard drive is usually done to provide protection for the object's confidentiality.

Hashing is used to provide integrity. Using mechanisms like backups and avoiding single points of failure provide availability protection. Non-repudiation is usually provided for during a secured communication, not while a file is stored on a hard drive.

REFERENCES

7.4.9 File Encryption Facts

q_file_encryption_confident_secp7.question.fex

Question 2: ✔ Correct

Which of the following should you set up to ensure encrypted files can still be decrypted if the original user account becomes corrupted?

- VPN
- GPG
- PGP
- DRA

EXPLANATION

If a user account becomes corrupted or the password is forgotten, any encrypted files are lost. To help remedy this, a data recovery agent (DRA) can be set up. The DRA is simply another account that can decrypt the encrypted files.

Pretty Good Privacy (PGP) is an older utility used to encrypt and decrypt data and messages.

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.

GNU Privacy Guard (GPG) is a command line utility that's used to encrypt and decrypt data and messages.

REFERENCES

7.4.9 File Encryption Facts

q_file_encryption_dra_secp7.question.fex

Question 3: ✔ Correct

You want a security solution that protects the entire hard drive and prevents access even if the drive is moved to another system. Which solution should you choose?

- VPN
- EFS
- BitLocker
- IPsec

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 that 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 it 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

7.4.9 File Encryption Facts

q_file_encryption_encrypt_01_secp7.question.fex

Question 4: ✔ Correct

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

- VPN
- BitLocker
- IPsec
- EFS

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 that encrypts the entire contents of a hard drive, protecting all files on the disk. BitLocker uses a special key that 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

7.4.9 File Encryption Facts

q_file_encryption_encrypt_02_secp7.question.fex

Question 5: ✔ Correct

You've used BitLocker to implement full volume encryption on a notebook system. The notebook motherboard does not have a TPM chip, so you've used an external USB flash drive to store the BitLocker startup key.

You use EFS to encrypt the C:\Secrets folder and its contents.

Which of the following is true in this scenario? (Select two.)

- [x] By default, only the user who encrypted the C:\Secrets\confidential.docx file will be able to open it.
- [x] If the C:\Secrets\confidential.docx file is copied to an external USB flash drive, the file will be saved in an unencrypted state.
- [ ] The EFS encryption process will fail.
- [ ] Only the user who encrypted the C:\Secrets\confidential.docx file is able to boot the computer from the encrypted hard disk.
- [ ] If the C:\Secrets\confidential.docx file is copied to an external USB flash drive, the file will remain in an encrypted state.
- [ ] Any user who is able to boot the computer from the encrypted hard disk will be able to open the C:\Secrets\confidential.docx file.

EXPLANATION

BitLocker uses full volume encryption, while EFS is used to encrypt individual files and folders. The following are true in this scenario:

- If the C:\Secrets\confidential.docx file is copied to an external USB flash drive, the file will be saved in an unencrypted state.
- Only the user who encrypted the C:\Secrets\confidential.docx file will be able to open it by default.

With BitLocker enabled, any user who has the appropriate startup key or PIN is able to boot the system from the encrypted drive. However, only the user who encrypted the C:\Secrets\ folder will be able to access files within it unless additional user accounts are explicitly added.

REFERENCES

7.4.9 File Encryption Facts

q_file_encryption_encrypt_03_secp7.question.fex

Question 6: ✔ Correct

Which utility would you MOST likely use on OS X to encrypt and decrypt data and messages?

- IPsec
- VPN
- GPG
- PGP

EXPLANATION

GNU Privacy Guard (GPG) is a command line utility that's used to encrypt and decrypt data and messages. GPG is a open source utility and can be used on many different systems, including Windows, Linux, Android, and Apple's OS X.

Pretty Good Privacy (PGP) is an older utility used to encrypt and decrypt data and messages. PGP was purchased a while ago and commercialized. It's owned by NortonLifeLock, formally known as Symantec, and provides products that can protect all sorts of devices, even smartphones. While PGP can be used on OS X, GPG is used by default.

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. A VPN is not used on OS X to encrypt and decrypt data and messages.

IPSec is a protocol used to encrypt VPN communication.

REFERENCES

7.4.9 File Encryption Facts

q_file_encryption_ipsec_secp7.question.fex

Question 7: ✔ Correct

You would like to implement BitLocker to encrypt data on a hard disk, even if it is moved to another system. You want the system to boot automatically without providing a startup key on an external USB device.

What should you do?

- ➡ Enable the TPM in the BIOS.
- Save the startup key to the boot partition.
- Disable USB devices in the BIOS.
- Use a PIN instead of a startup key.

EXPLANATION

When a system boots, the startup key is required to unlock the encrypted volume. The system startup key can be saved in the Trusted Platform Module (TPM). With the startup key saved in the TPM, the system can start without additional intervention.

The system will not start without the startup key. Without a TPM, the startup key must be stored on a USB drive. You can require a PIN in addition to a startup key, but the PIN cannot replace the startup key. Storing the startup key on the boot drive would expose it to compromise.

REFERENCES

- 4.2.1 Operating System Hardening
- 4.2.2 Hardening Facts
- 4.2.3 Hardening an Operating System
- 4.2.4 Managing Automatic Updates
- 4.2.6 Configuring Microsoft Defender Firewall
- 4.2.8 Configuring Windows Defender with Firewall Advanced Security
- 7.2.4 Hardware-Based Encryption Devices
- 7.2.5 Cryptographic Implementation Facts
- 7.4.9 File Encryption Facts

q_file_encryption_tpm_01_secp7.question.fex

Question 8: ✔ Correct

You want to protect data on hard drives for users with laptops. You want the drive to be encrypted, and you want to prevent the laptops from booting unless a special USB drive is inserted. In addition, the system should not boot if a change is detected in any of the boot files.

What should you do?

- Have each user encrypt user files with EFS.
- ➡ Implement BitLocker without a TPM.
- Implement BitLocker with a TPM.
- Have each user encrypt the entire volume with EFS.

EXPLANATION

If you use BitLocker without a TPM, system integrity checks are not performed. The TPM is required for saving the startup file information that is used to verify system integrity. When using BitLocker without a TPM, you must use a startup key on a USB device. When using a TPM, this is an optional configuration.

Use BitLocker to encrypt the entire system volume and protect both operating system and user data. Use BitLocker with a Trusted Platform Module (TPM) to protect the boot environment components such as the BIOS, Master Boot Record, Boot Sector, Boot Manager, and Windows Loader. The system is shut down if a boot environment change is detected. Using BitLocker, drives are locked if they are moved to another computer, and you can require a startup key on a USB drive or a PIN before the system boots.

EFS encrypts individual files. With EFS, only the user who encrypted the file and any additionally designated users can access the file. EFS does not provide integrity checks for boot files.

REFERENCES

- 4.2.1 Operating System Hardening
- 4.2.2 Hardening Facts
- 4.2.3 Hardening an Operating System
- 4.2.4 Managing Automatic Updates
- 4.2.6 Configuring Microsoft Defender Firewall
- 4.2.8 Configuring Windows Defender with Firewall Advanced Security
- 7.2.4 Hardware-Based Encryption Devices
- 7.2.5 Cryptographic Implementation Facts
- 7.4.9 File Encryption Facts

q_file_encryption_tpm_02_ccsp7_question_fex

q_file_encryption_tpm_02_secp7.question.fex

Question 9: ✔ Correct

Which of the following database encryption methods encrypts the entire database and all backups?

- ➡ Transparent Data Encryption (TDE)
- Application-level
- Bitlocker
- Column-level

EXPLANATION

Transparent Data Encryption (TDE) encrypts the entire database and all backups. TDE:

- encrypts data at rest, which is data not being currently used.
- is called transparent because when an authorized user needs to access the data, it is automatically decrypted so the user does not see the process or need to do anything extra.

Column-level encryption allows the administrator to encrypt each column separately.

In application-level encryption, the program that is used to create or modify the data is responsible for encrypting the data.

BitLocker is a Microsoft security solution that encrypts the entire contents of a hard drive, protecting all files on the disk.

REFERENCES

7.4.9 File Encryption Facts

q_file_encryption_trans_data_secp7.question.fex

Question 10: ✕ Incorrect

You have transferred an encrypted file across a network using the Server Message Block (SMB) Protocol. What happens to the file's encryption?

- The encryption inherits from the new location.
- The file is unencrypted when moved.
- The encryption carries over to the new location.
- ~~An encrypted file cannot be moved using SMB.~~

EXPLANATION

A file is automatically unencrypted when you copy it over a network using the SMB Protocol.

The encryption does not carry over to the new location, nor does the file inherit from the new location.

A file can be moved using the SMB Protocol.

REFERENCES

7.4.9 File Encryption Facts

q_file_encryption_unencrypt_secp7.question.fex