

## Exam Report: 9.7.10 Practice Questions

Date: 1/28/2020 6:40:34 pm

Candidate: Garsteck, Matthew

Time Spent: 1:35

Login: mGarsteck

## Overall Performance

Your Score: 38%

View results by: ☐ Objective Analysis ☒ Individual Responses

## Individual Responses

▼ Question 1: 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
- ☐ Use a PIN instead of a startup key
- ☐ Save the startup key to the boot partition
- ☐ Disable USB devices in the BIOS

## 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

LabSim for Security Pro, Section 9.7.

[All Questions SecPro2017\_v6.exm FILE\_ENCRYPT\_01]

▼ Question 2: 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 the entire volume with EFS.
- ☐ Implement BitLocker without a TPM.
- ➡ ☒ Implement BitLocker with a TPM.
- ☐ Have each user encrypt user files with EFS.

## Explanation

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 will boot.

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.

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

LabSim for Security Pro, Section 9.7.

[All Questions SecPro2017\_v6.exm FILE\_ENCRYPT\_02]

### ▼ Question 3: Incorrect

Which of the following security measures encrypts the entire contents of a hard drive?

- ☐ BIOS password
- ☐ Hard disk password
-  ☐ DriveLock
- ☐ Chassis intrusion detection
- ☒ ~~Trusted Platform Module (TPM)~~

## Explanation

DriveLock encrypts the entire contents of a hard drive, protecting all files on the disk.

When a password is set for the hard drive, you cannot move the drive to another system to access the disk without the password (the password moves with the disk). A Trusted Platform Module (TPM) is a special chip on the motherboard that generates and stores cryptographic keys to verify that the hardware has not changed. This value can be used to prevent the system from booting if the hardware has changed. Chassis intrusion detection helps you identify when a system case has been opened. When the case cover is removed, the switch sends a signal to the BIOS. A BIOS password controls access to the system. If set, the administrator (or supervisor or setup) password is required to enter the CMOS program to make changes to BIOS settings.


## References

LabSim for Security Pro, Section 9.7.

[All Questions SecPro2017\_v6.exm FILE\_ENCRYPT\_03]

### ▼ Question 4: 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?

-  ☒ BitLocker
- ☐ EFS
- ☐ VPN
- ☐ 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 only encrypts individual files. Encryption and decryption is

automatic and dependent upon the file's creator and whether other users 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

LabSim for Security Pro, Section 9.7.

[All Questions SecPro2017\_v6.exm FILE\_ENCRYPT\_04]

### ▼ Question 5: Incorrect

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.

Which system components are encrypted in this scenario? (Select two.)

- ☐ Optical media
- ☐ System partition
- ➔ ☒ Master boot record
- ➔ ☐ C:\ volume
- ☒ BIOS

## Explanation

BitLocker uses full volume encryption, so the disk partition containing the C:\ volume is encrypted along with the master boot record.

However, BitLocker does not encrypt the 100 MB system partition that contains the boot files, nor the system BIOS or RAM.

## References

LabSim for Security Pro, Section 9.7.

[All Questions SecPro2017\_v6.exm FILE\_ENCRYPT\_06]

### ▼ Question 6: Incorrect

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.)

- ➔ ☒ By default, only the user who encrypted the C:\Secrets\confidential.docx file will be able to open it.
- ☐ 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.
- ☒ Only the user who encrypted the C:\Secrets\confidential.docx file will be 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, it will be saved in an unencrypted state.
- ☐ The EFS encryption process will fail.
- ☐ If the C:\Secrets\confidential.docx file is copied to an external USB flash drive, it will remain in an encrypted state.

## 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, it 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

LabSim for Security Pro, Section 9.7.

[All Questions SecPro2017\_v6.exm FILE\_ENCRYPT\_07]

### ▼ Question 7: Incorrect

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

- ➡ ☐ EFS
- ☐ VPN
- ☐ IPsec
- ☒ BitLocker

## 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

LabSim for Security Pro, Section 9.7.

[All Questions SecPro2017\_v6.exm FILE\_ENCRYPT\_05]

### ▼ Question 8: Incorrect

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?

- ➡ ☐ Confidentiality
- ☒ Integrity
- ☐ Availability
- ☐ Non-repudiation

## 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 usually while a file is stored on a hard drive.

## References

LabSim for Security Pro, Section 9.7.

[All Questions SecPro2017\_v6.exm FILE\_ENCRYPT\_08]