Exam Report: 13.5.5 Practice Questions

Date: 4/15/2020 4:33:02 pm
Time Spent: 1:00

Candidate: Garsteck, Matthew
Login: mGarsteck

Overall Performance

Your Score: 29%

Passing Score: 80%

View results by: Objective Analysis Individual Responses

Individual Responses

Question 1: Incorrect

Which security measure can be used to generate and store cryptographic keys?

- DriveLock
- ~~BIOS/UEFI password~~
- Chassis intrusion detection
- Trusted Platform Module (TPM)

Explanation

A Trusted Platform Module (TPM) is a special chip on the motherboard that generates and stores cryptographic keys. The TPM can be used by applications (such as Bitlocker on Windows systems) to generate and save keys that are used for encryption.

DriveLock is a disk encryption solution. Chassis intrusion detection helps you identify when a system case has been opened. A BIOS/UEFI password controls access to the BIOS/UEFI setup program.

References

TestOut PC Pro - 13.5 BIOS/UEFI Security
[e_biossec_pp6.exam.xml Q_SEC_BIOSF_01]

Question 2: Incorrect

Which of the following functions are performed by the TPM?

- Perform bulk encryption.
- Create a hash based on installed system components.
- Encrypt data on the hard disk drive.
- ~~Generate authentication credentials.~~

Explanation

A Trusted Platform Module (TPM) is a hardware cryptoprocessor that resides on

References

TestOut PC Pro - 13.5 BIOS/UEFI Security
[e_biossec_pp6.exam.xml Q_SEC_BIOSF_02]

Question 3: Incorrect

You want to configure your computer so that a password is required before the operating system will load.

What should you do?

- ○ Configure an administrator password in the BIOS/UEFI.
- ◉ ~~Require complex passwords in the local security policy.~~
- ○ Configure chassis instruction detection.
- ➡ ○ Configure a user password in the BIOS/UEFI.

Explanation

Configuring a user password in the BIOS/UEFI requires that a valid password is entered before the operating system will load.

When an administrative password is set, it must be entered in order to access the firmware setup program. Chassis intrusion detection helps you identify when a system case has been opened. Password settings in the local security policy control passwords associated with user accounts that are configured within the operating system. These passwords are used after the system loads the operating system, not before.

References

TestOut PC Pro - 13.5 BIOS/UEFI Security
[e_biossec_pp6.exam.xml Q_SEC_BIOSF_03]

Question 4: Incorrect

You have purchased a used computer from a computer liquidator. When you boot the computer, you find that there has been a password set on the BIOS. You need to clear the password so that you can edit the CMOS settings.

What should you do?

- ➡ ○ Remove the motherboard battery for a few seconds.
- ◉ ~~Press Ctrl + Alt + Del while booting the computer.~~
- ○ Flash the BIOS.
- ○ Press F2 while booting the computer.

Explanation

You can clear the BIOS password by removing the motherboard battery for few seconds or, on older systems, by setting a motherboard jumper.

Flashing the BIOS probably will not remove the password.

References

[e_biossec_pp6.exam.xml Q_SEC_BIOSF_04]

Question 5: Correct

Which of the following indicates that a system case cover has been removed?

- Chassis intrusion detection
- Trusted Platform Module (TPM)
- DriveLock
- BIOS password

Explanation

Chassis intrusion detection helps you identify when a system case has been opened. When the case cover is removed, an alert is recorded in 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. 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. DriveLock is a disk encryption solution.

References

TestOut PC Pro - 13.5 BIOS/UEFI Security
[e_biossec_pp6.exam.xml Q_SEC_BIOSF_05]

Question 6: Incorrect

You just bought a new notebook. This system uses UEFI firmware and came with Windows 10 preinstalled. However, you want to use Linux on this system. You download your favorite distribution and install it on the system, removing all Windows partitions on the hard disk in the process. When the installation is complete, you find that the operating system won't load when the system is rebooted.

Which of the following would allow your computer to boot to Linux?

- Disable SecureBoot in the UEFI configuration.
- Reinstall Windows 10 on the system.
- Enable the TPM chip on the motherboard.
- ~~Enable SecureBoot in the UEFI configuration.~~
- Set the boot order to boot from the hard disk first in the UEFI configuration.

Explanation

You should disable the SecureBoot option in the UEFI configuration. SecureBoot requires the operating system installed on the hard drive to be digitally signed. If it isn't digitally signed, then the UEFI firmware will not boot it by default.

Reinstalling Windows 10 doesn't meet the requirements of the scenario. If

References

TestOut PC Pro - 13.5 BIOS/UEFI Security
[e_biossec_pp6.exam.xml Q_SEC_BIOSF_06]

Question 7: Correct

You just bought a new computer. This system uses UEFI firmware and comes with Windows 10 preinstalled. You recently accessed the manufacturer's support website and saw that a UEFI firmware update has been released. You download the update. However, when you try to install the update, an error message is displayed that indicates the digital signature on the update file is invalid.

Which of the following is MOST likely caused this to happen?

- ○ The system has a rootkit malware infection.
- ◉ The update file has been tampered with.
- ○ SecureBoot has been enabled in the UEFI firmware configuration.
- ○ Interim UEFI updates released since the system was manufactured need to be installed before you can install the latest update.

Explanation

UEFI requires firmware updates to be digitally signed by the hardware vendor. Using digital signatures, unauthorized changes to firmware updates (such as the insertion of malware) can be detected.

The SecureBoot feature requires that operating systems be digitally signed before they can be booted on the system. The latest UEFI update most likely includes all of the changes implemented in early updates. There is no indication that the system has been infected with rootkit malware in this scenario.

References

TestOut PC Pro - 13.5 BIOS/UEFI Security
[e_biossec_pp6.exam.xml Q_SEC_BIOSF_07]