3.8.12 Practice Questions

Candidate: Seolito Rodríguez (rodriguez77)

Date: 1/23/2024, 10:02:49 PM • **Time Spent:** 00:14

Score: 0%

Passing Score: 80%

Question 1. × Incorrect

A user has called to complain that her computer won't boot. It stops on the system startup screen right after the memory has been tested and displays a 301 keyboard error.

Which of the following troubleshooting steps is the BEST to try first?

○ Download and install the latest keyboard driver from the manufacturer's website.

○ Install a new keyboard on the computer.

○ Verify that the latest UEFI firmware updates have been applied.

→ ○ Verify that no keys are being pressed down during POST.

Explanation

You should have the user verify that no keyboard keys are being pressed during POST. With any error, you should always check the obvious first. This error is almost always caused by a stuck key on the keyboard or something resting on a keyboard key.

Firmware updates rarely cause issues that would display a keyboard error during startup. The same is true of a keyboard driver. Updating the driver would rarely cause a keyboard error during startup.

On rare occasions, you may need to install a new keyboard. However, you should look for the obvious problems first.

References

3.8.3 BIOS/UEFI Facts
3.8.10 BIOS/UEFI Security Facts
q_bios_301_keyboard_error_pp7.question.fex

Question 2.

× Incorrect

An employee complains that every time they turn their computer off, the computer's time is set to 12:00 p.m., and the date is set back to January 1, 1990.

Which of the following is the MOST likely cause of this anomaly?

→ ○ The CMOS battery has failed.

○ The CMOS chip is failing.

○ The CMOS settings are not being saved before the computer powers off.

○ The CMOS chip on the motherboard is loose.

Explanation

The CMOS (a physical part of the motherboard) is a memory chip that houses setting configurations. The CMOS is able to maintain its setting when the computer is powered off by using a CMOS battery. If the CMOS battery is failing, you may see the effects (such as the time and day being slightly off). If the CMOS battery has failed, it will typically reset the date and time back to the date the CMOS was created.

The CMOS is reset and loses all custom settings if the CMOS battery fails. Additionally, the system clock resets when the CMOS loses power.

Unless the battery fails, CMOS settings are rarely lost (not saved) before the computer powers off.

The CMOS chip rarely fails or comes loose on the motherboard. These would rarely be the cause of the CMOS chip losing its settings.

References

3.8.3 BIOS/UEFI Facts
3.8.10 BIOS/UEFI Security Facts
q_bios_cmos_batt_fail_pp7.question.fex

Question 3.

× Incorrect

What is the role of the CMOS in a modern computer?

- ○ Coordinates the use of system hardware with the operating system.
- → ○ Saves information about system devices.
- ○ Tests hardware during system startup.
- ○ Loads the operating system into memory.

Explanation

The CMOS saves information about system devices.

The BIOS tests hardware during system startup, coordinates the use of system hardware with the operating system, and loads the operating system into memory.

References

3.8.3 BIOS/UEFI Facts
3.8.10 BIOS/UEFI Security Facts
q_bios_cmos_role_pp7.question.fex

Question 4.

× Incorrect

When you boot your computer, it hangs after asking you for the current time and date. What is the MOST likely problem?

- ○ The computer needs more RAM.
- ○ The BIOS is outdated.
- → ○ The CMOS battery has failed.
- ○ Daylight savings time has started or ended.

Explanation

The system time and date are managed by the BIOS's real-time clock (RTC). If the CMOS memory battery goes dead, the RTC reverts back to a default date and time.

The BIOS being outdated, daylight savings time beginning or ending, or a need for more RAM would not cause the computer to ask for the current date and time.

References

3.8.3 BIOS/UEFI Facts

3.8.10 BIOS/UEFI Security Facts

q_bios_date_time_request_pp7.question.fex

Question 5.

× Incorrect

When do you need to upgrade the system BIOS?

○ Whenever the BIOS settings need to be modified.

→ ○ Whenever a BIOS update provides functionality that is not currently supported, but is required by the operating system or hardware.

○ Whenever you add a new peripheral device, such as a keyboard, mouse, or printer.

○ Whenever you install a new hard disk drive.

Explanation

In general, you need to upgrade the system BIOS whenever the current BIOS does not support a function required by the operating system or by the hardware. Use the CMOS program to change system configuration settings used by the BIOS.

Installing a new hard drive, modifying the BIOS settings, or adding a new peripheral device do not normally require a BIOS update.

References

3.8.3 BIOS/UEFI Facts
3.8.10 BIOS/UEFI Security Facts

q_bios_system_bios_upgrd_pp7.question.fex

Question 6. × **Incorrect**

To fix a problem you are having with your PC, you have determined that you must flash the computer's BIOS.

Which of the following would MOST likely need to be completed prior to flashing the BIOS? (Select two.)

→ □ Download the flash utility or tool from the manufacturer's website.

□ Test the memory to ensure that it is functioning properly.

□ Locate the flash utility or tool that was shipped with your computer.

→ □ Properly identify the motherboard.

□ Create a backup of the hard disk in the event of a failure.

Explanation

To successfully flash your BIOS, it is critical that you research and know the exact make, model, and revision of your motherboard to ensure that the correct flash file is used. Using the wrong flash file will probably cause errors.

Although your computer may have shipped with a tool to perform a BIOS flash, it is best to download the latest tool to ensure that the flash is performed correctly.

Testing the memory and creating a hard backup will not aid you while flashing a PC's BIOS.

References

3.8.3 BIOS/UEFI Facts
3.8.10 BIOS/UEFI Security Facts
q_bios_tasks_before_mem_flash_pp7.question.fex

Question 7.

× Incorrect

You have purchased a new notebook. This notebook system uses UEFI firmware and comes with Windows 11 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?

○ Set the boot order to boot from the hard disk first in the UEFI configuration.

→ ○ Disable SecureBoot in the UEFI configuration.

○ Enable SecureBoot in the UEFI configuration.

○ Reinstall Windows 11 on the system.

○ Enable the TPM chip on the motherboard.

Explanation

In this scenario, 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, the UEFI firmware will not boot it by default.

Reinstalling Windows 11 does not meet the requirements of this scenario.

If SecureBoot is already enabled, the TPM chip on the motherboard must already be enabled as well.

The boot order configuration is not preventing the system from booting in this scenario.

References

3.8.3 BIOS/UEFI Facts
3.8.4 Edit BIOS/UEFI Settings
3.8.8 BIOS/UEFI Security
3.8.10 BIOS/UEFI Security Facts

q_sec_biosf_disable_secureboot_pp7.question.fex

Question 8. × Incorrect

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

What should you do?

○ Require complex passwords in the Local Security Policy.

→ ○ Configure a user password in the BIOS/UEFI.

○ Configure chassis instruction detection.

○ Configure an administrator 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

3.8.3 BIOS/UEFI Facts
3.8.8 BIOS/UEFI Security
3.8.9 Configure BIOS/UEFI Security Settings
3.8.10 BIOS/UEFI Security Facts

q_sec_biosf_os_boot_password_pp7.question.fex

Question 9.

× **Incorrect**

Which of the following functions are performed by the Trusted Platform Module (TPM)?

○ Generates authentication credentials.

○ Encrypts data on the hard disk drive.

○ Performs bulk encryption.

→ ○ Creates a hash based on installed system components.

Explanation

A Trusted Platform Module (TPM) is a hardware cryptoprocessor that resides on the motherboard that stores and generates cryptographic keys. Using these keys, the TPM can generate a hash value based on the components installed in the system. The hash value can be used to verify that system components have not been modified when the system boots. Because each system will have a unique hash value, the hash can also be used as a form of system identification. Keys generated by the TPM can be used for encryption and authentication, but the TPM does not perform the actual encryption.

The TPM is not designed to perform bulk encryption, directly encrypt data on the hard disk drive, or generate authentication credentials.

References

3.8.8 BIOS/UEFI Security
3.8.9 Configure BIOS/UEFI Security Settings
3.8.10 BIOS/UEFI Security Facts

q_sec_biosf_tpm_function_pp7.question.fex

Question 10. × Incorrect

You have just purchased a new computer. This system uses UEFI firmware and comes with Windows 11 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 it, an error message is displayed that indicates the digital signature on the update file is invalid.

Which of the following MOST likely caused this to happen?

→ ○ The update file has been tampered with.

○ SecureBoot has been enabled in the UEFI firmware configuration.

○ Interim UEFI updates that have been released since the system was manufactured need to be installed before you can install the latest update.

○ The system has a rootkit malware infection.

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.

The latest UEFI update most likely includes all of the changes that were implemented in earlier updates.

There is no indication that the system has been infected with rootkit malware in this scenario.

References

3.8.3 BIOS/UEFI Facts
3.8.10 BIOS/UEFI Security Facts

q_sec_biosf_update_file_tampered_pp7.question.fex