We offer free update service for one year!
https://www.certqueen.com

Exam : **220-1202**

Title : CompTIA A+ Certification Exam: Core 2

Version : DEMO

1. Topic 1, Multiple Choice Questions

Which of the following best describes a security consequence of using software that is EOL?
A. The software will stop working.
B. The vendor will not support future features.
C. New vulnerabilities will not be patched.
D. Users will incur increased licensing costs.
Answer: C
Explanation:
The correct answer is C. New vulnerabilities will not be patched. EOL means end of life. When software or an operating system reaches EOL, the vendor typically stops providing security patches and official support. Quentin Docter's Complete Study Guide explains that when most operating systems reach EOL, the vendor stops supplying security patches, creating a major vulnerability because the system is no longer protected from the latest vulnerabilities. The Sybex practice-test material also states that end of extended support means no support, including security updates and patches, and that if a vulnerability is discovered, the user of an EOL operating system is at risk of attack. EOL software does not necessarily stop working immediately. Future features and licensing costs may be affected, but the most important security consequence is that newly discovered vulnerabilities may remain unpatched.

2.A user cannot upload files to corporate servers from their mobile device when outside the office, but uploads work fine in-office.
What should a technician do to determine the root cause?
A. Check the data usage limit
B. Enable airplane mode
C. Verify the last device reboot
D. Enable Bluetooth connectivity
Answer: A
Explanation:
If uploading fails only offsite, mobile data limits or restrictions are the likely cause. Data caps or network management can interfere with uploads.
From Travis Everett – All-in-One Exam Guide:
"When mobile users experience network issues, always check if the device has reached a data cap or roaming restriction."

3.A user frequently misplaces their Windows laptop and is concerned about it being stolen. The user would like additional security controls on their laptop.
Which of the following is a built-in technology that a technician can use to enable full drive encryption?
A. Active Directory
B. New Technology File System
C. Encrypting File System
D. BitLocker
Answer: D
Explanation:
BitLocker is Microsoft's full disk encryption technology built into Windows Pro and Enterprise editions. It

encrypts the entire drive, protecting data if the device is lost or stolen. BitLocker can use TPM (Trusted Platform Module) and can be configured with PINs or USB keys for added security.
A. Active Directory is for centralized user and policy management in domains.
B. NTFS is the file system format and doesn't provide encryption by itself.
C. EFS (Encrypting File System) encrypts individual files or folders, not the entire drive.
Reference: CompTIA A+ 220-1102 Objective 2.2: Compare and contrast security measures and encryption tools.
Study Guide Section: Encryption options — BitLocker vs. EFS

4.Which of the following is the quickest way to move from Windows 10 to Windows 11 without losing data?
A. Using gpupdate
B. Image deployment
C. Clean install
D. In-place upgrade
Answer: D
Explanation:
An in-place upgrade is the fastest and most efficient way to upgrade from Windows 10 to Windows 11 while keeping all user data, applications, and settings intact. This method is often used when the hardware meets Windows 11 requirements and no system reconfiguration is necessary.
A. gpupdate is used to refresh Group Policy settings — unrelated to OS upgrades.
B. Image deployment typically replaces the current OS and may not retain user data unless specifically customized.
C. A clean install requires formatting the drive and starting fresh, which removes all data.
Reference: CompTIA A+ 220-1102 Objective 1.4: Given a scenario, use appropriate Microsoft operating system installation methods.
Study Guide Section: In-place upgrade vs. clean install methods

5.An end user's computer is unable to start. A technician examines the machine and does not hear any unusual noises but determines that no OS is found.
Which of the following is most likely corrupt?
A. Basic input/output system
B. New Technology File System
C. Trusted Platform Module
D. Master boot record
Answer: D
Explanation:
“No OS found” commonly indicates the firmware can’t locate boot instructions for the installed OS. If the drive isn’t obviously failing (no unusual noises) and BIOS/UEFI settings are reasonable, a classic cause is a corrupt Master Boot Record (MBR) (on MBR-partitioned disks). Mike Meyers’ Lab Manual explains that when BIOS can’t find an OS, causes may include configuration issues or drive problems, but also states: “If the correct drive is already first in the boot sequence, the master boot record… may be corrupt and need to be rebuilt.”
The Lab Manual also explains what the MBR does: the first sector contains boot code that informs the

system about installed operating systems, and “without this bit of code, your OS will never load.” The All-in-One guide describes the same: BIOS looks at the first sector for instructions, and without the MBR code, the OS won’t load.
NTFS corruption wouldn’t typically present as “no OS found” at the firmware stage, and TPM issues usually create different security/boot errors. Therefore, MBR (D) is most likely.