CompTIA A+ Core 2 (220-1102) Practice Exam (Sample)

Study Guide

BY EXAMZIFY

Everything you need from our exam experts!

Notice: Examzify makes every reasonable effort to obtain from reliable sources accurate, complete, and timely information about this product.

Questions

1. **After identifying malware on a user's system, what is the next step according to malware removal best practices?**
   - **A. Enable System Restore and create a restore point**
   - **B. Educate the user on avoiding malware**
   - **C. Update antivirus software and perform a full system scan**
   - **D. Move the infected system to a lab with no network connectivity**

2. **What type of document would a network administrator likely provide to a technician for a network upgrade detailing switchports?**
   - **A. Process diagram**
   - **B. Physical network diagram**
   - **C. Fiber backbone diagram**
   - **D. Logical topology diagram**

3. **What does a Virtual Machine enable in an IT environment?**
   - **A. Hosting applications on a single server**
   - **B. Running multiple operating systems on one physical machine**
   - **C. Increasing physical server capacity**
   - **D. Managing cloud resources**

4. **What is the purpose of system updates?**
   - **A. To improve system performance, security, and functionality**
   - **B. To install new hardware components**
   - **C. To remove unnecessary software**
   - **D. To downgrade system settings**

5. **A SOHO technician wants to upgrade two computers quickly without retaining user settings. Which installation method would be MOST likely used?**
   - **A. Unattended installation**
   - **B. Remote network installation**
   - **C. In-place upgrade**
   - **D. Clean installation**

6. Which network topology is characterized by all devices connecting to a central hub or switch?

A. Mesh topology

B. Star topology

C. Bus topology

D. Ring topology

7. Which type of network attack involves modifying a user's DNS settings to redirect traffic?

A. DDoS

B. Man-in-the-middle

C. DNS Spoofing

D. Session Hijacking

8. For data removal from recycled PCs, which method is the most effective?

A. Standard formatting

B. HD drilling

C. Low-level formatting

D. HD partitioning

9. Which of the following best describes endpoint protection measures?

A. Only protecting hardware devices

B. Protecting end-user devices with security software

C. Restricting network access to authorized personnel

D. Monitoring internal server threats

10. What is the main function of the Central Processing Unit (CPU) in a computer?

A. To store and retrieve data

B. To execute instructions and process data

C. To manage user interfaces

D. To connect to external devices

Answers

1. D
2. B
3. B
4. A
5. A
6. B
7. C
8. C
9. B
10. B

Explanations

1. After identifying malware on a user's system, what is the next step according to malware removal best practices?

A. Enable System Restore and create a restore point

B. Educate the user on avoiding malware

C. Update antivirus software and perform a full system scan

D. Move the infected system to a lab with no network connectivity

After identifying malware on a user's system, the next step according to malware removal best practices is to move the infected system to a lab with no network connectivity. This is crucial because isolating the infected machine prevents the malware from spreading to other systems or networks. By disconnecting the system from the internet and other connected devices, you minimize the risk of data exfiltration, further infections, or disruptions to other systems. In this context, the other choices, while important steps in the overall malware removal process, would not be prioritized immediately after detection. Enabling System Restore and creating a restore point is useful for recovery, but it does not directly address the active threat. Educating the user on avoiding malware is a key preventative measure for the future but comes after containment of the current infection. Updating antivirus software and performing a full system scan is an essential action, but it should be done after isolating the system. This ensures that the antivirus can effectively address the malware without interference from network communications or additional spread.

2. What type of document would a network administrator likely provide to a technician for a network upgrade detailing switchports?

A. Process diagram

B. Physical network diagram

C. Fiber backbone diagram

D. Logical topology diagram

A physical network diagram is the appropriate document for a network administrator to provide for detailing switchports during a network upgrade. This type of diagram represents the actual hardware layout of the network, including all physical components such as switches, routers, and the connections between them. It shows where devices are located and how they are interconnected, which is crucial for technicians to understand physical switchport configurations and connections. This visual representation allows technicians to easily identify which ports on the switches are available for new connections, how they are interconnected with other devices, and any specific configurations that might be relevant to the upgrade process. This understanding is essential for effectively executing the network upgrade, ensuring that connectivity and throughput are maintained according to the network design. In contrast, while a process diagram outlines the steps involved in a particular procedure, a fiber backbone diagram focuses specifically on the layout of fiber-optic cables used to connect different parts of the network, and a logical topology diagram represents the conceptual layout and the paths data can take through the network rather than the physical connections. None of these options provide the detail on physical switch ports and their configurations essential for a technician during an upgrade.

3. What does a Virtual Machine enable in an IT environment?

A. Hosting applications on a single server

B. Running multiple operating systems on one physical machine

C. Increasing physical server capacity

D. Managing cloud resources

A Virtual Machine (VM) enables running multiple operating systems on one physical machine, allowing for efficient utilization of hardware resources. This capability is crucial in virtualized environments because it allows an organization to isolate different workloads, test new operating systems or applications, and run applications that may be dependent on specific environments without the need for separate physical hardware. Each virtual machine operates as an independent computer, complete with its own virtual CPU, memory, storage, and network interfaces. This virtualization technology is particularly valuable for maximizing physical server capacity, as it allows multiple VMs to share the underlying physical server's resources, leading to better investment in hardware and energy usage efficiency. Additionally, the flexibility provided by VMs supports various use cases, including development, testing, and production environments simultaneously running different systems on the same physical machine. While hosting applications on a single server, increasing physical server capacity, and managing cloud resources are important aspects of IT environments, the core function of a virtual machine is primarily centered around enabling multiple operating systems to coexist and operate effectively on a single piece of hardware.

4. What is the purpose of system updates?

A. To improve system performance, security, and functionality

B. To install new hardware components

C. To remove unnecessary software

D. To downgrade system settings

The purpose of system updates is to improve system performance, security, and functionality. This is essential because updates often include patches that address vulnerabilities in the operating system, thereby enhancing security measures against potential attacks or malware. Additionally, performance enhancements may optimize how the system runs by fixing bugs, improving resource management, or adding new features that can make the user experience more efficient and smooth. Updates may also provide compatibility improvements, ensuring that the system can work effectively with new applications or hardware that may be released after the original version. Overall, keeping a system updated is a crucial best practice for maintaining the health and reliability of both personal and organizational computing environments.

5. A SOHO technician wants to upgrade two computers quickly without retaining user settings. Which installation method would be MOST likely used?

A. Unattended installation

B. Remote network installation

C. In-place upgrade

D. Clean installation

The most appropriate method for upgrading the two computers quickly without retaining user settings is a clean installation. This method involves completely wiping the existing operating system and user data, then installing a fresh version of the operating system. Since the requirement is not to preserve user settings, a clean installation ensures that the new operating system is installed on a blank slate, eliminating any previous configuration or data. This approach is particularly useful in scenarios where a technician wants to ensure that the systems are running optimally with the latest software and configurations. While unattended installation allows for a quick and automated setup process, it typically retains existing settings or personal files unless specifically configured otherwise. In-place upgrades, on the other hand, generally preserve user settings and data as they upgrade the existing operating system to a newer version. Therefore, for a rapid, no-retention upgrade, the clean installation method fits the requirements perfectly.

6. Which network topology is characterized by all devices connecting to a central hub or switch?

A. Mesh topology

B. Star topology

C. Bus topology

D. Ring topology

The star topology is characterized by all devices connecting to a central hub or switch. In this configuration, each device on the network has its own individual cable connecting it directly to the hub or switch, which serves as a central point of communication. This structure allows for easy addition and removal of devices without disrupting the network, as each device operates independently and communicates through the central point. In star topology, if one cable or device fails, it does not affect the others on the network, which enhances reliability and simplifies troubleshooting. Additionally, the central hub or switch can manage traffic and has the capability to create a more efficient network by intelligently directing data packets to the appropriate devices. Other topologies, such as mesh, bus, and ring, have different configurations that do not involve all devices being connected to a single central point. For example, in a mesh topology, each device can connect to multiple other devices, creating multiple pathways for data, while in a bus topology, all devices share a single communication line. In ring topology, devices are connected in a circular arrangement, where each device is connected to two others, forming a closed loop.

7. Which type of network attack involves modifying a user's DNS settings to redirect traffic?

A. DDoS

B. Man-in-the-middle

C. DNS Spoofing

D. Session Hijacking

DNS Spoofing is accurately identified as the type of network attack that involves modifying a user's DNS settings to redirect traffic. This type of attack works by providing false DNS responses, which leads a user to an incorrect IP address instead of the intended server. For example, if an attacker can alter the DNS settings on a user's device or exploit vulnerabilities in a DNS server, they can direct that user to a malicious website instead of a legitimate one. This manipulation can be particularly dangerous as it can result in phishing, data theft, or the distribution of malware. The core of the attack revolves around deceiving the DNS system, which is responsible for translating user-friendly domain names into IP addresses that computers use to communicate. Other network attack types mentioned, such as DDoS (which disrupts services by overwhelming them with traffic), Man-in-the-middle (which intercepts communications between two parties without their knowledge), and Session Hijacking (which takes control of an active session after the user has logged in) do not specifically involve modifying DNS settings to redirect traffic. They utilize different methods and targets, making DNS Spoofing the correct choice in this context.

8. For data removal from recycled PCs, which method is the most effective?

A. Standard formatting

B. HD drilling

C. Low-level formatting

D. HD partitioning

Low-level formatting is considered one of the most effective methods for data removal from recycled PCs. This process involves initializing a hard drive to its most basic state, which can include rewriting the data on the disk. Although traditional low-level formatting is somewhat outdated due to modern hard drive designs, the principle remains relevant; it can render the data unrecoverable by merely altering the disk's structure and removing file system data. This method goes beyond standard formatting, which simply removes the pointers to data but keeps the data itself intact, making it still potentially recoverable with the right tools. Similarly, HD partitioning is primarily used to create separate sections on a drive, which again does not remove the data. HD drilling, while it does physically damage the drive and guarantees the impossibility of data recovery, is not a standard or efficient method for most situations where data needs to be sanitized, especially for less critical data removal scenarios. While low-level formatting, in a broader sense of erasing data through overwriting, can vary in effectiveness based on the technology used (like SSDs versus HDDs), it fundamentally aims at permanently eliminating access to previously stored information, which aligns with the requirement for effective data removal in recycled PCs.

9. Which of the following best describes endpoint protection measures?

A. Only protecting hardware devices

B. Protecting end-user devices with security software

C. Restricting network access to authorized personnel

D. Monitoring internal server threats

Endpoint protection measures primarily focus on securing end-user devices, such as computers, laptops, tablets, and smartphones, from various threats. This involves deploying security software that can offer features such as antivirus protection, antispyware, firewalls, intrusion detection, and prevention. The goal is to safeguard these endpoints from malware, ransomware, unauthorized access, and data breaches, effectively creating a vital layer in an organization's overall cybersecurity strategy. By focusing on protecting end-user devices with security software, organizations ensure that the devices used by employees are fortified against threats that can penetrate the network through less secure endpoints. This is particularly important as endpoints often serve as entry points for cyberattacks, making their protection critical to maintaining overall security. Other choices mention aspects that are important in cybersecurity but do not encapsulate the essence of endpoint protection. For instance, protecting only hardware devices overlooks the essential role of software and fails to address the broader context of endpoint management. Similarly, restricting network access pertains to network security practices rather than specifically to endpoint security. Monitoring internal server threats, while crucial for overall security, is more relevant to server management and does not focus on protecting end-user devices directly.

10. What is the main function of the Central Processing Unit (CPU) in a computer?

A. To store and retrieve data

B. To execute instructions and process data

C. To manage user interfaces

D. To connect to external devices

The main function of the Central Processing Unit (CPU) in a computer is to execute instructions and process data. The CPU is often referred to as the brain of the computer because it performs the fundamental operations of the system, which includes fetching instructions from memory, decoding them to determine the action to be taken, and executing those instructions to perform calculations or manipulate data as required by software applications. This execution cycle is crucial for running programs and performing tasks, making the CPU integral to overall system performance. Without the CPU effectively processing instructions and managing data operations, a computer would be unable to function as intended, leading to a lack of responsiveness to user inputs or failure to carry out applications. Options that focus on storing and retrieving data, managing user interfaces, or connecting to external devices describe functions that are performed by other components of the computer, such as storage devices, user interface hardware, and peripheral controllers. These actions support the CPU but do not represent its primary role. Hence, the focus on executing instructions and processing data highlights the CPU's essential purpose in a computer system.