Cisco IT Essentials Practice Test (Sample)

Study Guide

Everything you need from our exam experts!

Questions

1. **Which command line tool should be used to register a DLL file in Windows 10?**

   A. register.dll

   B. regsvr32

   C. cmdreg

   D. dllregister

2. **What is the correct compressed format of the IPv6 address 2001:0db8:eeff:000a:0000:0000:0000:0001?**

   A. 2001:0db8:eeff:a:0:0:0:1

   B. 2001:db8:eeff:a::1

   C. 2001:db8:eeff:0:a:0:0:1

   D. 2001:db8:eeff:0a::1

3. **What is the essential function of encryption in data security?**

   A. Enhancing data speed

   B. Transforming data into a secure format

   C. Backing up data securely

   D. Removing duplicate data

4. **How does a public IP address differ from a private IP address?**

   A. Public IP addresses are used internally

   B. Private IP addresses are routable on the internet

   C. Public IP addresses are accessible over the internet

   D. Private IP addresses are always static

5. **Which technology regulates voltage and current for a computer's power needs?**

   A. Power supply unit

   B. Voltage regulator

   C. Transformers

   D. Integrated circuits

6. Which two types of expansion slots are commonly used by a wireless NIC in a computer today?

A. ISA and PCI

B. PCI and PCIe

C. AGP and PCI

D. USB and PCIe

7. When hardware failure is detected by the BIOS, how is this failure commonly indicated?

A. Screen error message

B. Computer shuts down

C. Emitted beeping pattern

D. LED indicator lights

8. Which action should be avoided when working inside a computer case?

A. Using a grounding strap

B. Wearing loose clothing

C. Disconnecting power before servicing

D. Removing jewelry

9. What is essential to demonstrate a chain of custody in computer forensics?

A. Enlisting multiple technicians

B. Proper documentation procedures

C. Verbal agreements with clients

D. Independent verification by authorities

10. What port numbers would a technician be looking for in the captured packets for SNMP traffic?

A. 161 and 162

B. 8080 and 443

C. 25 and 110

D. 53 and 67

Answers

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

Explanations

1. Which command line tool should be used to register a DLL file in Windows 10?

A. register.dll

B. regsvr32

C. cmdreg

D. dllregister

The use of regsvr32 is the correct choice for registering a DLL (Dynamic Link Library) file in Windows 10. This command line tool is specifically designed for this task. When you execute regsvr32 followed by the path to the DLL file, it communicates with the operating system to register the DLL, which makes the functions within that library accessible to applications or processes that need to utilize them. Registering a DLL involves updating the Windows Registry so that the operating system can properly manage and access the library's functions. Regsvr32 handles this process efficiently and is a widely recognized and documented tool within the Windows environment. In contrast, the other options listed do not exist or are not appropriate for this specific task. For instance, register.dll and dllregister are not recognized commands within Windows, and cmdreg does not serve the purpose of registering DLL files. Therefore, regsvr32 stands out as the correct and appropriate tool for registering DLLs in the Windows operating system.

2. What is the correct compressed format of the IPv6 address 2001:0db8:eeff:000a:0000:0000:0000:0001?

A. 2001:0db8:eeff:a:0:0:0:1

B. 2001:db8:eeff:a::1

C. 2001:db8:eeff:0:a:0:0:1

D. 2001:db8:eeff:0a::1

The correct compressed format of the IPv6 address 2001:0db8:eeff:000a:0000:0000:0000:0001 is indeed 2001:db8:eeff:a::1. In IPv6, the compression rules allow for the removal of leading zeros from each segment, which is one way to simplify the address. In this case, '0db8' simplifies to 'db8' and '000a' simplifies to 'a'. The consecutive groups of zeros can be replaced with a double colon (::), but this can only be done once in an IPv6 address to avoid ambiguity. The segment '0000:0000:0000:0000' consists of four groups of zeros, which can be compressed as a single double colon. However, in this answer, it's applied to the last segment: the full address is reduced to '2001:db8:eeff:a::1', making it concise. This method reflects the efficiency of IPv6 addressing, designed to ensure easier readability and management of addresses.

3. What is the essential function of encryption in data security?

A. Enhancing data speed

B. Transforming data into a secure format

C. Backing up data securely

D. Removing duplicate data

Encryption plays a vital role in data security by transforming data into a secure format that is unreadable to unauthorized users. This process uses algorithms to encode the information, ensuring that even if data is intercepted or accessed without permission, it cannot be understood without the appropriate decryption key. The importance of encryption lies in its ability to protect sensitive information from breaches and unauthorized access, maintaining confidentiality and integrity throughout its transmission or storage. This is critical in various domains, including financial transactions, personal communications, and confidential business data. While enhancing data speed, securely backing up data, and removing duplicate data are valuable aspects of data management and system performance, they do not directly address the need for securing data from unauthorized access. Hence, the primary function of encryption is to create a secure representation of data, safeguarding it against potential threats.

4. How does a public IP address differ from a private IP address?

A. Public IP addresses are used internally

B. Private IP addresses are routable on the internet

C. Public IP addresses are accessible over the internet

D. Private IP addresses are always static

Public IP addresses are assigned to devices that need to be accessed over the internet. They are unique across the entire internet and are used to identify a device so that it can send and receive data. This means that any device with a public IP address can communicate directly with other devices on the internet without any additional routing or translation. Private IP addresses, on the other hand, are used within local networks and are not routable on the internet. They allow devices on the same local network to communicate with one another, but they cannot be accessed directly from outside that network. This distinction is crucial for maintaining security and efficient use of IP addresses, as private addresses can be reused across different networks without conflict. The option indicating that private IP addresses are always static does not hold true, as private IP addresses can be dynamic, depending on the network configuration. Similarly, the assertion that public IP addresses are used internally is misleading since they are primarily for external communication. Thus, the correct answer highlights the accessibility of public IP addresses over the internet, serving as a fundamental aspect of how internet communication is structured.

5. Which technology regulates voltage and current for a computer's power needs?

A. Power supply unit

B. Voltage regulator

C. Transformers

D. Integrated circuits

The power supply unit (PSU) is crucial for regulating voltage and current to meet a computer's power needs. It takes the alternating current (AC) from the wall outlet and converts it into direct current (DC), which is used by the computer's components. The PSU also ensures that the output voltage levels align with the specific requirements of various parts, such as the motherboard, graphics card, and storage devices. Furthermore, a power supply unit typically includes voltage regulation circuitry to maintain stable voltage levels and prevent damage to sensitive electronic components. This makes it a central component in a computer system, as it not only provides power but also protects the system by adjusting voltage and current supplies according to the demands of the hardware. While other options such as voltage regulators, transformers, and integrated circuits play roles in managing or altering electrical signals, they do not encompass the overall power supply function that the PSU performs in a computer system.

6. Which two types of expansion slots are commonly used by a wireless NIC in a computer today?

A. ISA and PCI

B. PCI and PCIe

C. AGP and PCI

D. USB and PCIe

The use of PCI and PCIe expansion slots for wireless Network Interface Cards (NICs) is based on their ability to provide sufficient bandwidth and compatibility with modern computing systems. PCI (Peripheral Component Interconnect) has historically been a standard for connecting peripheral devices to the motherboard. However, it has largely been replaced by PCIe (Peripheral Component Interconnect Express), which offers faster data transfer rates and improved performance. As wireless technology has advanced, the need for high-speed connections has increased, making PCIe the preferred choice for wireless NICs in contemporary computers. PCIe provides multiple lanes for data transfer, which helps in handling the high data throughput required for modern wireless standards. In contrast, ISA (Industry Standard Architecture) is an older technology that is rarely used today due to its limitations in speed and efficiency. AGP (Accelerated Graphics Port) was specifically designed for graphics cards and is not suitable for wireless NICs. While USB (Universal Serial Bus) is commonly used for external wireless adapters, it is not an expansion slot in the same context as PCI and PCIe, which are integrated into the motherboard for internal components. Thus, the correct identification of PCI and PCIe as the two types of expansion slots commonly used by wireless NICs aligns

7. When hardware failure is detected by the BIOS, how is this failure commonly indicated?

A. Screen error message

B. Computer shuts down

C. Emitted beeping pattern

D. LED indicator lights

When hardware failure is detected by the BIOS, one of the most common methods of indication is through an emitted beeping pattern. This form of alert is known as a "POST beep code." During the Power-On Self-Test (POST), the BIOS performs a series of checks to ensure that the hardware components are functioning properly before the operating system is loaded. If it encounters a problem, it will often produce a series of beeps that correspond to specific error codes. These beep codes are standardized to some extent but can vary between motherboard manufacturers, so referring to the motherboard's documentation is essential for interpretation. This auditory feedback allows the user or technician to diagnose hardware issues without needing to rely solely on a visual display, which may not display any error messages if the failure is significant enough to prevent the system from booting normally. In contrast, while message displays, system shutdowns, or LED indicators may also signal issues, the use of beep codes stands out as a direct and immediate method employed during the initial boot process to alert users about hardware malfunctions.

8. Which action should be avoided when working inside a computer case?

A. Using a grounding strap

B. Wearing loose clothing

C. Disconnecting power before servicing

D. Removing jewelry

Wearing loose clothing should be avoided when working inside a computer case because such attire can inadvertently catch on components or tools, posing a risk of damage to the hardware or injury to the technician. Tight-fitting clothing is preferable as it minimizes the chance of snagging on any sensitive parts and enhances overall safety while performing any repairs or modifications. Using a grounding strap, disconnecting power before servicing, and removing jewelry are all best practices that help protect both the technician and the equipment. Grounding straps prevent static electricity from damaging components, disconnecting power ensures that there's no live electricity when working on internal parts, and removing jewelry helps avoid potential short circuits or physical injury from rings and watches getting caught in moving parts.

9. What is essential to demonstrate a chain of custody in computer forensics?

A. Enlisting multiple technicians

B. Proper documentation procedures

C. Verbal agreements with clients

D. Independent verification by authorities

Proper documentation procedures are critical for establishing a chain of custody in computer forensics. This concept refers to the process of maintaining and documenting evidence to ensure that it is preserved in its original condition and that its integrity remains intact from the moment it is collected until it is presented in a legal context. Documentation serves multiple crucial purposes: it records who collected the evidence, where and how it was collected, the time of collection, and who has had access to it afterward. This detailed record prevents tampering or accidental alteration of the evidence and ensures that it can be legally accepted in court. A clear and comprehensive chain of documentation shows that the evidence has been handled properly and can strengthen its reliability during investigations or legal proceedings. While multiple technicians may assist in the forensic process, having their involvement does not automatically ensure the preservation of a proper chain of custody without adequate documentation. Verbal agreements lack the formality required in legal contexts, and independent verification by authorities can certainly bolster the process but relies upon the preceding documentation to prove that the evidence has been safeguarded through its entirety. Therefore, the foundation of a trustworthy chain of custody is built through meticulous and proper documentation.

10. What port numbers would a technician be looking for in the captured packets for SNMP traffic?

A. 161 and 162

B. 8080 and 443

C. 25 and 110

D. 53 and 67

The correct port numbers that a technician would look for in captured packets for SNMP (Simple Network Management Protocol) traffic are 161 and 162. Port 161 is used for SNMP operations, specifically for sending queries from a management system to a managed device, which is where monitoring begins. Port 162 is used for SNMP traps, which are automated alerts triggered by devices to notify the management system of issues or significant events, allowing for proactive management of the network. When capturing network packets for analysis, identifying traffic on these ports indicates active SNMP communication, which is crucial for network device monitoring and management. The use of these specific ports is standardized for SNMP, aiding technicians in diagnosing issues related to network management effectively. Other port numbers associated with different protocols, such as those listed in the other answer choices, do not pertain to SNMP and serve different purposes. For instance, ports 8080 and 443 are associated with HTTP and HTTPS traffic, respectively; 25 and 110 are used for email protocols like SMTP and POP3; while 53 and 67 pertain to DNS queries and DHCP. These distinctions highlight the importance of knowing specific port assignments for effective troubleshooting and network management.