CompTIA A+ Core 2 (220-1002) Certification 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. **Which protocol is commonly used to secure communications over the internet?**

   A. HTTP

   B. FTP

   C. HTTPS

   D. TELNET

2. **Which of the following characteristics defines a secure password?**

   A. It should be long, complex, and include a mix of letters, numbers, and symbols

   B. It should be easy to remember and contain only letters

   C. It should be short and include birthdays

   D. It should consist of only special characters

3. **You want to prevent a user from accessing your phone while you step away from your desk. What should you do?**

   A. Implement remote backup

   B. Set up a remote wipe program

   C. Configure a screen lock

   D. Install a locator application

4. **What is the most likely cause of excessive pop-up windows and a particular website showing in searches?**

   A. Spam

   B. Virus

   C. Social engineering

   D. Spyware

5. **What system is indicated if a technician saved a file as a .sh?**

   A. PowerShell

   B. Linux

   C. JavaScript

   D. Python

6. To make the bootmgr file visible in the C: root of a hard drive, which settings should you configure? (Select two best answers)

- **A. Hidden files and folders**
- **B. Extensions for known file types**
- **C. Encrypted or compressed NTFS files in color**
- **D. Protected operating system files**

7. What is the key difference between IPv4 and IPv6?

- **A. IPv4 uses 128-bit addresses, while IPv6 uses 32-bit addresses**
- **B. IPv4 uses 32-bit addresses, while IPv6 uses 128-bit addresses**
- **C. IPv4 addresses are textual only, while IPv6 addresses are numerical**
- **D. IPv4 is no longer in use, while IPv6 is the only version available**

8. A user clicked a link in an e-mail that appeared to be from his bank. The link led him to a page that requested he charge his password to access his bank account. What is this an example of?

- **A. Impersonation**
- **B. Dumpster diving**
- **C. Phishing**
- **D. Shoulder surfing**

9. What is two-factor authentication (2FA)?

- **A. A process requiring a password only**
- **B. A security process using a single form of identification**
- **C. A verification method using two different forms of identification**
- **D. A physical security measure for hardware protection**

10. Which command can be used to display all active network connections and listening ports?

- **A. netstat**
- **B. ipconfig**
- **C. ping**
- **D. arp**

Answers

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

Explanations

1. Which protocol is commonly used to secure communications over the internet?

A. HTTP

B. FTP

C. HTTPS

D. TELNET

The reason C, HTTPS, is the correct answer is that it is specifically designed to secure communications over the internet by using encryption. HTTPS stands for Hypertext Transfer Protocol Secure and combines HTTP (which is used for transferring web pages) with additional security layers, usually through the use of SSL/TLS (Secure Sockets Layer/Transport Layer Security). This encryption ensures that all data exchanged between the client (such as a web browser) and the server is secure, protecting it from eavesdropping, tampering, and other forms of cyber threats. In contrast, HTTP is the standard protocol for transmitting data over the web but does not include any encryption, making it vulnerable to interception. FTP (File Transfer Protocol) is commonly used for file transfers but lacks built-in security features. Telnet is a protocol used for remote access to devices over a network, but like HTTP, it transmits data in plaintext and is not secure for sensitive communications. Thus, HTTPS is the preferable choice when security is a priority in internet communications.

2. Which of the following characteristics defines a secure password?

A. It should be long, complex, and include a mix of letters, numbers, and symbols

B. It should be easy to remember and contain only letters

C. It should be short and include birthdays

D. It should consist of only special characters

A secure password is best defined as one that is long, complex, and includes a mix of letters, numbers, and symbols. This combination enhances its strength and makes it much more difficult for unauthorized users to guess or crack the password. A longer password generally provides a greater number of potential combinations, making it exponentially harder for attackers to brute-force into an account. Including a variety of character types—such as uppercase and lowercase letters, numbers, and special characters—further increases the complexity and unpredictability of the password. This multifaceted approach to password creation is recommended by security experts and organizations as an essential practice to safeguard sensitive information. In contrast, options that suggest passwords should be easy to remember and consist only of letters, be short and include birthdays, or consist solely of special characters represent less secure practices. Easy-to-remember passwords often lead to simpler, more predictable combinations that can be easily exploited. Short passwords limit the number of possible variations, making them vulnerable to attacks. Using identifiable information, like birthdays, is also risky because such data can often be found or guessed. Meanwhile, passwords made up only of special characters may not be practical for users and can also create compatibility issues across different systems and applications.

3. You want to prevent a user from accessing your phone while you step away from your desk. What should you do?

A. Implement remote backup

B. Set up a remote wipe program

C. Configure a screen lock

D. Install a locator application

Configuring a screen lock is the best way to prevent unauthorized access to a phone while you are away from your desk. A screen lock requires a user to enter a passcode, password, or use biometric authentication (such as a fingerprint or facial recognition) to unlock the device. This effectively protects the data and privacy of the user, as it ensures that anyone who attempts to access the phone without the correct credentials will be denied entry. Having a screen lock in place is crucial in maintaining security, especially in a work environment where sensitive information might be stored on the device. It acts as a first line of defense against unauthorized access. Implementing remote backup, setting up a remote wipe program, or installing a locator application do not directly prevent physical access to the device while you are away. Remote backup and remote wipe are useful for data recovery and security in cases of theft or loss, but they would not secure the device itself when simply stepping away. A locator application helps track the device's location but does not prevent access. Therefore, configuring a screen lock is the most effective immediate solution to keep your phone secure.

4. What is the most likely cause of excessive pop-up windows and a particular website showing in searches?

A. Spam

B. Virus

C. Social engineering

D. Spyware

The presence of excessive pop-up windows and a specific website repeatedly appearing in searches is most commonly associated with spyware. Spyware is malicious software designed to gather information from a user's computer without their knowledge, which often results in unwanted pop-ups and redirects to certain websites as part of advertising schemes or data collection purposes. When spyware infects a device, it can manipulate the browser's behavior, leading to the display of unwanted ads and pop-ups. This behavior occurs because spyware typically tracks browsing habits, which can then be exploited to generate revenue for cybercriminals through ad impressions or clicks. Additionally, such software can alter browser settings or the default homepage, further causing users to encounter pop-ups and redirects to specific sites. In contrast, spam generally refers to unsolicited messages, often in the form of emails or unwanted notifications, which do not specifically cause pop-up windows in the browser environment. Viruses, while capable of causing significant harm to a system, usually manifest in other ways rather than merely producing excessive pop-ups. Social engineering refers to tactics that manipulate individuals into revealing personal information; it does not inherently involve the technical aspects of pop-up windows or search behaviors.

5. What system is indicated if a technician saved a file as a .sh?

A. PowerShell

B. Linux

C. JavaScript

D. Python

The indication that a file has been saved with a .sh extension strongly points to a Linux operating system. Files with the .sh extension are typically shell scripts used in Unix-based systems, which include various distributions of Linux. These scripts often contain a series of commands and are executed within a terminal that utilizes a shell, such as bash (Bourne Again SHell). The naming convention of file extensions is essential in identifying the purpose and associated environment of a file. In this case, .sh files are universally recognized in the context of Linux systems. This contrasts with the other options, which have different file types and extensions associated with them. For example, PowerShell scripts typically have a .ps1 extension, JavaScript files use .js, and Python scripts are generally saved with a .py extension. Therefore, the .sh extension distinctly identifies the file as a shell script intended for use within a Linux operating system.

6. To make the bootmgr file visible in the C: root of a hard drive, which settings should you configure? (Select two best answers)

A. Hidden files and folders

B. Extensions for known file types

C. Encrypted or compressed NTFS files in color

D. Protected operating system files

The process of making the bootmgr file visible in the C: root of a hard drive involves configuring certain settings that control the visibility of files on the system. To see the bootmgr file, it is essential to adjust the visibility options related to hidden files and system files. Configuring the setting for hidden files and folders allows you to view files and directories that the operating system normally keeps hidden to prevent accidental deletion or modification. Bootmgr is a hidden system file, so enabling this setting will ensure that it is displayed in the file explorer. Moreover, another key setting that needs to be configured is the visibility of protected operating system files. By default, these files, which include critical boot files like bootmgr, are hidden to safeguard the operating system's integrity. Adjusting this setting will allow you to view bootmgr alongside other important system files. Together, adjusting both the hidden files and folders setting and the protected operating system files setting will enable you to see the bootmgr file that is necessary for the Windows boot process.

7. What is the key difference between IPv4 and IPv6?

A. IPv4 uses 128-bit addresses, while IPv6 uses 32-bit addresses

B. IPv4 uses 32-bit addresses, while IPv6 uses 128-bit addresses

C. IPv4 addresses are textual only, while IPv6 addresses are numerical

D. IPv4 is no longer in use, while IPv6 is the only version available

The correct answer highlights a fundamental characteristic of the two protocols: IPv4 utilizes 32-bit addresses, yielding a theoretical maximum of about 4.3 billion unique addresses. In contrast, IPv6 was developed to address the limitations of IPv4, particularly the exhaustion of available IP addresses due to the growth of the internet and connected devices. By using 128-bit addresses, IPv6 can accommodate an astronomical number of unique addresses—around 340 undecillion (3.4 x 10^38). This vast addressing capability is crucial for the expansion and sustainability of internet-connected devices. The remaining options contain inaccuracies regarding the characteristics of both protocols. For instance, the first choice misrepresents the bit lengths of the addresses, while the third option incorrectly describes the types of addresses; both IPv4 and IPv6 can be represented in both numerical and textual (dotted-decimal or hexadecimal) formats. The last option incorrectly suggests that IPv4 is no longer in use, whereas it is still widely utilized despite the gradual transition to IPv6. This distinction is vital for understanding networking concepts and the evolution of internet protocols.

8. A user clicked a link in an e-mail that appeared to be from his bank. The link led him to a page that requested he charge his password to access his bank account. What is this an example of?

A. Impersonation

B. Dumpster diving

C. Phishing

D. Shoulder surfing

This scenario is an example of phishing. Phishing is a malicious attempt to trick individuals into providing sensitive information, such as login credentials, by pretending to be a trustworthy entity—in this case, the user's bank. When the user clicked the link in the email, they were led to a fraudulent webpage that resembled the bank's official website. This tactic exploits social engineering techniques to create a sense of urgency or fear, prompting users to enter their information without realizing they are interacting with a harmful source. In contrast, impersonation refers to someone pretending to be another person but does not specifically involve the act of gathering sensitive data through fake electronic communications. Dumpster diving involves searching through trash to find confidential information, and shoulder surfing is the act of observing someone entering sensitive data, such as passwords, in real-time. Each of these terms represents a different type of security threat, with phishing being specifically focused on fraudulent online deception to harvest personal information.

9. What is two-factor authentication (2FA)?

A. A process requiring a password only

B. A security process using a single form of identification

C. A verification method using two different forms of identification

D. A physical security measure for hardware protection

Two-factor authentication (2FA) is a security process that requires users to present two different forms of identification before they can access an account or system. This method enhances security by requiring two separate components: something the user knows (like a password) and something the user has (like a smartphone, security token, or smart card). By combining these two factors, 2FA significantly reduces the risk of unauthorized access compared to relying solely on a password. The other options do not accurately describe 2FA. The process that requires just a password is a single-factor authentication method, which lacks the added layer of security. A single form of identification also pertains to one-factor authentication, which does not provide sufficient protection against potential threats. Lastly, while physical security measures can protect hardware, they do not specifically define the concept of two-factor authentication, which focuses on user verification methods rather than physical equipment.

10. Which command can be used to display all active network connections and listening ports?

A. netstat

B. ipconfig

C. ping

D. arp

The command that effectively displays all active network connections and listening ports is netstat. This command provides a detailed overview of current TCP/IP connections, including the local and remote IP addresses, port numbers, and the state of each connection (e.g., established, listening, etc.). It is a valuable tool for network troubleshooting and monitoring, as it allows users to identify any unauthorized or unexpected connections that may indicate security issues or performance problems. In contrast, the ipconfig command is primarily used to display and manage the configuration of network interfaces, including IP addresses, subnet masks, and default gateways, but does not show active connections. The ping command is utilized to test connectivity between devices on a network by sending ICMP echo requests and receiving echo replies, and it is not concerned with listing active connections. The arp command is used to display and manipulate the Address Resolution Protocol (ARP) cache, which maps IP addresses to MAC addresses, but it does not provide information on active connections or listening ports.