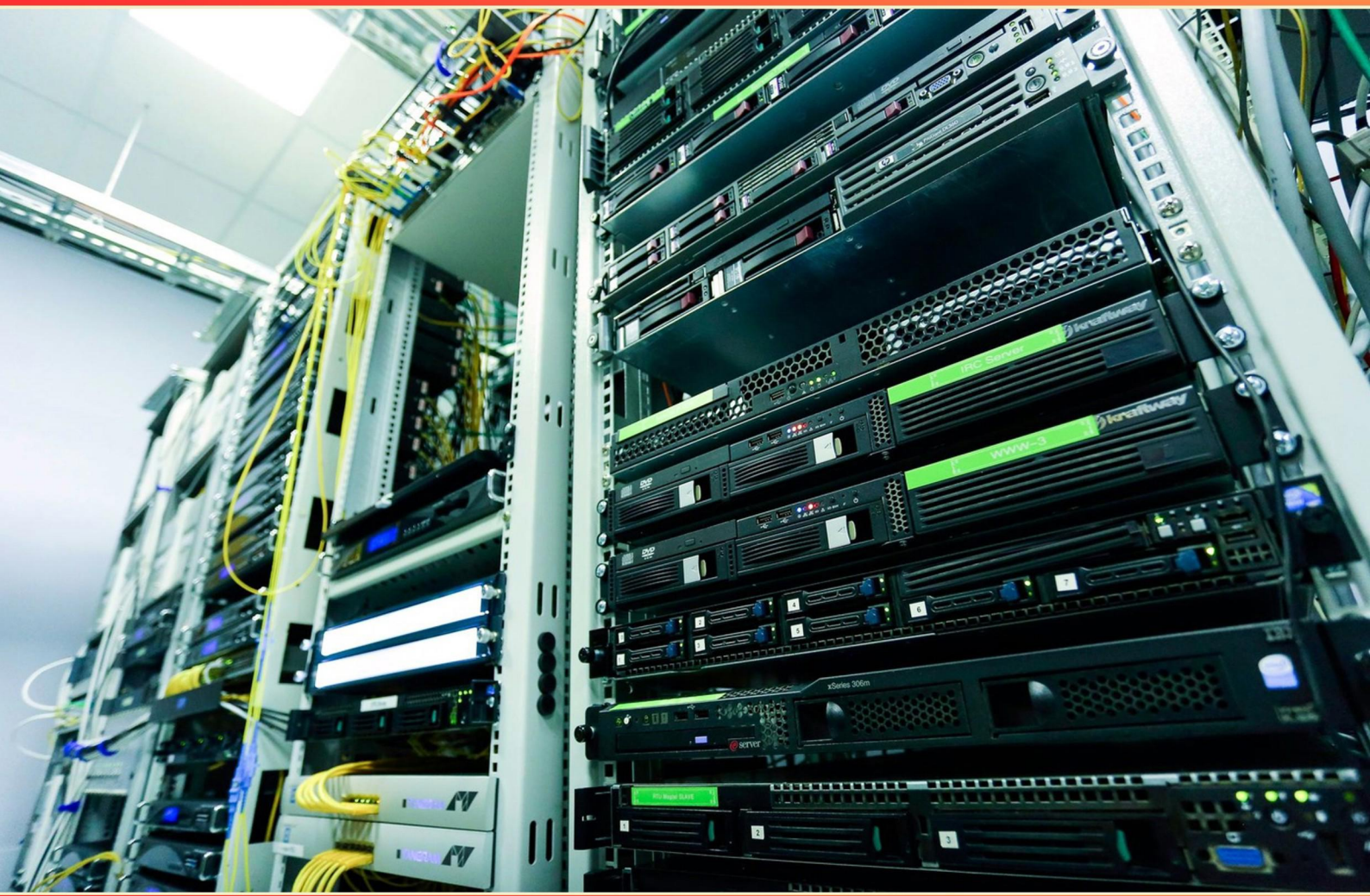
COMPTIA A+ CORE 2 (220-1102) PRACTICE EXAM (SAMPLE)

STUDY GUIDE



SAMPLE STUDY GUIDE WITH LIMITED QUESTIONS

VISIT US ONLINE FOR THE FULL VERSION STUDY GUIDE

https://comptiaapluscore22201102.examzify.com

Table of Contents

Introduction

Preparing for a certification exam can feel overwhelming, but with the right tools, it becomes an opportunity to build confidence, sharpen your skills, and move one step closer to your goals. At Examzify, we believe that effective exam preparation isn't just about memorization, it's about understanding the material, identifying knowledge gaps, and building the test-taking strategies that lead to success.

This guide was designed to help you do exactly that.

Whether you're preparing for a licensing exam, professional certification, or entry-level qualification, this book offers structured practice to reinforce key concepts. You'll find a wide range of multiple-choice questions, each followed by clear explanations to help you understand not just the right answer, but why it's correct.

The content in this guide is based on real-world exam objectives and aligned with the types of questions and topics commonly found on official tests. It's ideal for learners who want to:

- Practice answering questions under realistic conditions,
- Improve accuracy and speed,
- Review explanations to strengthen weak areas, and
- Approach the exam with greater confidence.

We recommend using this book not as a stand-alone study tool, but alongside other resources like flashcards, textbooks, or hands-on training. For best results, we recommend working through each question, reflecting on the explanation provided, and revisiting the topics that challenge you most.

Remember: successful test preparation isn't about getting every question right the first time, it's about learning from your mistakes and improving over time. Stay focused, trust the process, and know that every page you turn brings you closer to success.

Let's begin.

How to Use This Guide

This guide is designed to help you study more effectively and approach your exam with confidence. Whether you're reviewing for the first time or doing a final refresh, here's how to get the most out of your Examzify study guide:

1. Start with a Diagnostic Review

Skim through the questions to get a sense of what you know and what you need to focus on. Your goal is to identify knowledge gaps early.

2. Study in Short, Focused Sessions

Break your study time into manageable blocks (e.g. 30 – 45 minutes). Review a handful of questions, reflect on the explanations.

3. Learn from the Explanations

After answering a question, always read the explanation, even if you got it right. It reinforces key points, corrects misunderstandings, and teaches subtle distinctions between similar answers.

4. Track Your Progress

Use bookmarks or notes (if reading digitally) to mark difficult questions. Revisit these regularly and track improvements over time.

5. Simulate the Real Exam

Once you're comfortable, try taking a full set of questions without pausing. Set a timer and simulate test-day conditions to build confidence and time management skills.

6. Repeat and Review

Don't just study once, repetition builds retention. Re-attempt questions after a few days and revisit explanations to reinforce learning. Pair this guide with other Examzify tools like flashcards, and digital practice tests to strengthen your preparation across formats.

There's no single right way to study, but consistent, thoughtful effort always wins. Use this guide flexibly, adapt the tips above to fit your pace and learning style. You've got this!

Questions

1. **What should a user check first if their WiFi connection shows limited connectivity?**

   A. Network cable connections

   B. SSID visibility

   C. Firewall settings

   D. Router placement

2. **What password practice should a technician implement to secure a private PC in a public workspace?**

   A. Remove the guest account from the administrators group

   B. Disable single sign-on

   C. Issue a default strong password for all users

   D. Require authentication on wake-up

3. **What best practice could have prevented a corporate network from being infected by a malicious application on a flash drive?**

   A. Implementing strong passwords

   B. Changing default credentials

   C. Disabling AutoRun

   D. Removing Guest account

4. **What is an essential practice after removing malware from a user's system?**

   A. Creating a backup

   B. Reinstalling the operating system

   C. Educating the user

   D. Running a diagnostic check

5. **What type of attacks attempts to overload a server with traffic?**

   A. Man-in-the-Middle attack

   B. Phishing attack

   C. Denial of Service (DoS) attack

   D. Brute Force attack

6. What is the function of a captive portal in network security?

A. To configure access control lists

B. To provide guest access to an unsecured network

C. To redirect users for authentication before granting network access

D. To monitor network logs

7. Which command allows a junior Linux administrator to gain necessary permissions to update system software?

A. sudo

B. chmod

C. grep

D. pwd

8. What is the difference between a public IP address and a private IP address?

A. Public IP addresses are only for email

B. Private IP addresses are routable on the internet

C. Public IP addresses are routable on the internet

D. Private IP addresses are used globally

9. What role does a network switch play in a Local Area Network (LAN)?

A. To store network passwords

B. To connect wirelessly to devices

C. To receive, process, and forward data to destination devices

D. To act as a firewall for network protection

10. What is the function of a screensaver password in a workstation security policy?

A. To enhance performance

B. To protect screen visibility

C. To secure access when the user is away

D. To provide entertainment

Answers

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

Explanations

1. What should a user check first if their WiFi connection shows limited connectivity?

A. Network cable connections

B. SSID visibility

C. Firewall settings

D. Router placement

When troubleshooting limited connectivity issues with a WiFi connection, the first step should be checking the SSID visibility. The SSID, or Service Set Identifier, is the name of the wireless network. If the SSID is not visible, it indicates that the wireless network may be hidden or turned off, which prevents devices from connecting to it. Ensuring that the SSID is broadcasting allows the user to see and connect to the correct network. In scenarios where the SSID is not visible, devices may try to connect to other available networks, leading to limited or no connectivity. By confirming that the SSID is visible, the user can ensure they are attempting to connect to the correct network and diagnose further if issues persist. Checking network cable connections is important for wired connections but may not be applicable in a WiFi troubleshooting context. Similarly, while firewall settings can impact connectivity, they typically do so after a device has connected to the network. Lastly, router placement can affect signal strength and coverage, but it is often not the first factor to check when a device shows limited connectivity. Ensuring the SSID is visible is a direct and immediate step to resolve connection issues.

2. What password practice should a technician implement to secure a private PC in a public workspace?

A. Remove the guest account from the administrators group

B. Disable single sign-on

C. Issue a default strong password for all users

D. Require authentication on wake-up

Requiring authentication on wake-up is a crucial practice for securing a private PC in a public workspace. This means that when the computer goes into sleep or hibernation mode, it will need a password or some form of authentication to be re-accessed. This effectively prevents unauthorized access to the system when the owner is away from their desk, which is particularly important in a public environment where others can easily approach the unattended device. Implementing this measure significantly enhances security by ensuring that sensitive data remains protected, even in situations where the device is temporarily left unattended. Without this requirement, anyone could simply wake the computer and access potentially sensitive information. This practice is a standard recommendation for security in both personal and professional environments. While the other options might improve security in different contexts, they do not specifically address the immediate risk of unauthorized access when a computer is left unattended in a public area.

3. What best practice could have prevented a corporate network from being infected by a malicious application on a flash drive?

A. Implementing strong passwords

B. Changing default credentials

C. Disabling AutoRun

D. Removing Guest account

Disabling AutoRun is a key best practice for preventing a corporate network from being infected by malicious applications on a flash drive. When AutoRun is enabled, any media such as a USB flash drive can automatically execute executables stored on it as soon as it is plugged into a computer. This feature can quickly lead to the unintentional propagation of malware without any user interaction, making it easier for malicious software to infect systems. By disabling AutoRun, an organization can ensure that plugged-in flash drives do not automatically launch programs, thereby providing an additional layer of security. This requires users to manually access the contents of the flash drive, giving them an opportunity to inspect files before executing any software, and reducing the risk of malware spreading across the network. Other practices, such as implementing strong passwords, changing default credentials, or removing guest accounts, focus on securing access controls and user accounts, but they do not specifically address the threat posed by malicious files on external drives. While important for overall security, they do not directly mitigate the risk of malware execution from a USB flash drive, making disabling AutoRun the most effective preventive measure in this context.

4. What is an essential practice after removing malware from a user's system?

A. Creating a backup

B. Reinstalling the operating system

C. Educating the user

D. Running a diagnostic check

After removing malware from a user's system, educating the user is an essential practice. This step is crucial because it helps the user understand how the malware might have infiltrated their system and what preventative measures they can take in the future. It empowers users by enhancing their awareness of safe browsing habits, recognizing phishing attempts, avoiding suspicious downloads, and maintaining robust security practices, such as using antivirus software and keeping their operating system and applications updated. The knowledge gained through education not only aids the individual but also promotes a culture of cybersecurity awareness, reducing the likelihood of future infections for that user, as well as for the broader network or organization. By fostering a more informed user base, IT professionals can bolster the overall security posture of the systems they manage. Options such as creating a backup, reinstalling the operating system, and running a diagnostic check are all valid actions to consider in the context of system maintenance or recovery, but they do not address the fundamental aspect of preventing future malware infections as effectively as user education does.

5. What type of attacks attempts to overload a server with traffic?

A. Man-in-the-Middle attack

B. Phishing attack

C. Denial of Service (DoS) attack

D. Brute Force attack

A Denial of Service (DoS) attack is specifically designed to overwhelm a server with excessive traffic, making it difficult or impossible for legitimate users to access the services provided by that server. This type of attack floods the target with so many requests that it cannot handle the load, leading to service degradation or complete shutdown. In a DoS attack, malicious actors may use various methods to generate fake traffic or send numerous requests to the server. The intent is to exhaust the server's resources, such as bandwidth, memory, or CPU, effectively denying access to real users. This can be particularly damaging for websites and online services, as it can result in loss of business and trust. Other attack types mentioned do not primarily focus on overwhelming servers with traffic. A Man-in-the-Middle attack involves intercepting communication between two parties without their knowledge, while a Phishing attack aims to deceive individuals into providing sensitive information. A Brute Force attack tries to gain unauthorized access by systematically guessing passwords but does not involve overloading a server with traffic. Therefore, the nature of a Denial of Service attack aligns directly with the concept of overloading servers.

6. What is the function of a captive portal in network security?

A. To configure access control lists

B. To provide guest access to an unsecured network

C. To redirect users for authentication before granting network access

D. To monitor network logs

A captive portal serves a specific function in network security by requiring users to authenticate before they are granted access to the network. When a device connects to a network that uses a captive portal, the user is typically redirected to a web page where they must enter credentials, agree to terms of service, or perform some other verification. This process ensures that only authorized users can access the network and can help prevent unauthorized access, protect sensitive data, and manage user activity on the network. For instance, captive portals are often used in public Wi-Fi networks to ensure that individuals using the network agree to certain usage policies or display advertisements before they can gain full access. This mechanism not only enhances security but also allows network administrators to control who is using their network and under what conditions.

7. Which command allows a junior Linux administrator to gain necessary permissions to update system software?

A. sudo

B. chmod

C. grep

D. pwd

The command that allows a junior Linux administrator to gain the necessary permissions to update system software is "sudo." This command stands for "superuser do" and is essential for executing commands with elevated privileges. In Linux and Unix-like systems, certain tasks, such as installing software or making system-wide changes, require administrative or root-level permissions. By preceding a command with "sudo," a user can temporarily elevate their permissions to complete these tasks without fully switching to the root user account. This is particularly important for maintaining system security and stability. It allows users to perform administrative functions while still operating under their standard user account, minimizing the risk of unintentional system-wide changes or damage that could occur if the user were logged in as the root. The other options do have specific functionalities, but they do not provide the necessary permissions for software updates. "chmod" is used for changing file permissions, "grep" is a command-line utility for searching text, and "pwd" displays the current working directory. None of these commands facilitate elevated permissions to perform administrative tasks like software updates.

8. What is the difference between a public IP address and a private IP address?

A. Public IP addresses are only for email

B. Private IP addresses are routable on the internet

C. Public IP addresses are routable on the internet

D. Private IP addresses are used globally

A public IP address is assigned to devices that need to communicate over the internet and is routable on the global internet. This means that any device configured with a public IP address can be reached from any other device on the internet, facilitating open communication. Public IP addresses are essential for the proper functioning of web servers, email servers, and other services that must be accessible to users outside of a local network. On the other hand, private IP addresses are designated for use within a local area network (LAN) and are not routable on the internet. They are meant for internal networking purposes, allowing devices within the same network to communicate with each other but preventing direct access from outside that network. Private IP addresses are defined by specific ranges set aside by the Internet Engineering Task Force (IETF) and are commonly used in home, office, and campus networks. Understanding this distinction is crucial for managing network configurations, including the setting up of networks that require access to internet resources while maintaining a secure internal structure.

9. What role does a network switch play in a Local Area Network (LAN)?

A. To store network passwords

B. To connect wirelessly to devices

C. To receive, process, and forward data to destination devices

D. To act as a firewall for network protection

A network switch is an essential component within a Local Area Network (LAN) that primarily functions to receive, process, and forward data to the appropriate destination devices. It operates at the data link layer (Layer 2) of the OSI model and makes decisions based on MAC (Media Access Control) addresses assigned to each device connected to it. When a data frame is received, the switch examines the destination MAC address and uses its internal MAC address table to determine which port to send the data through, ensuring that data packets reach their intended devices efficiently. This capability to intelligently forward data frames enhances the overall performance and scalability of the network, facilitating communication between devices such as computers, printers, and servers within the same local area. The switch minimizes unnecessary data traffic on the network, improving speed and reducing congestion. In contrast, other choices outline roles that are not typically associated with a switch. For example, storing network passwords is a function best suited for authentication servers or directory services, while connecting wirelessly pertains to access points or routers rather than switches. Lastly, acting as a firewall is a security feature commonly provided by dedicated firewall devices or specialized routers, rather than the primary function of a switch.

10. What is the function of a screensaver password in a workstation security policy?

A. To enhance performance

B. To protect screen visibility

C. To secure access when the user is away

D. To provide entertainment

The function of a screensaver password in a workstation security policy is primarily to secure access when the user is away. When a user steps away from their computer, the screensaver activates, and if it requires a password to deactivate, this serves as a security measure. It prevents unauthorized access to sensitive data and applications while the user is temporarily away from their workstation. This mechanism helps maintain data integrity and confidentiality, especially in environments where sensitive information is processed. By requiring a password to access the workstation again, it ensures that only authorized users can regain access, thereby enhancing overall security. Such policies are essential in safeguarding organizational resources and helping to mitigate the risk of data breaches when users are away from their devices. In contrast, while other aspects like performance enhancement or providing entertainment may be side effects or features of screensavers, they do not align with the primary security function of needing a password to prevent unauthorized access.

Next Steps

Congratulations on reaching the final section of this guide. You've taken a meaningful step toward passing your certification exam and advancing your career.

As you continue preparing, remember that consistent practice, review, and self-reflection are key to success. Make time to revisit difficult topics, simulate exam conditions, and track your progress along the way.

If you need help, have suggestions, or want to share feedback, we'd love to hear from you. Reach out to our team at hello@examzify.com.

Or visit your dedicated course page for more study tools and resources:

https://comptiaapluscore22201102.examzify.com

We wish you the very best on your exam journey. You've got this!