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

Study Guide

Everything you need from our exam experts!

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. **A user's phone contains customer's PII. Which of the following is the best method for securing the phone?**

   A. Fingerprint lock

   B. Passcode lock

   C. Swipe lock

   D. PIN lock

2. **What does the acronym IPv4 stand for?**

   A. Internet Protocol version 2

   B. Internet Protocol version 3

   C. Internet Protocol version 4

   D. Internet Protocol version 5

3. **During a DDoS attack, which types of infections are the source of traffic most likely infected?**

   A. Spyware

   B. Zombies

   C. Virus

   D. Ransomware

4. **What compliance is required for businesses using credit cards in both physical and web locations?**

   A. PHI certification

   B. PCI compliance

   C. POTS implementation

   D. PII filtering

5. **What could be a potential reason for a network share to return an "Access Denied" message despite correct user permissions?**

   A. Insufficient user privileges

   B. Disabled network adapter

   C. Invalid session tokens

   D. Incorrectly configured sharing settings

6. During a planned router OS upgrade, what essential part of the change request must an administrator document?

A. Inform management of the anticipated downtime

B. Document a backout plan to roll back changes

C. Configure a redundant data path to eliminate downtime

D. Make the downtime window larger than expected

7. 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

8. What is the function of a proxy server?

A. To store data for offline access

B. To act as an intermediary for requests from clients

C. To provide local network access

D. To encrypt user data

9. A user finds that their web browser opens to an unrecognized search engine and shows irrelevant results. What should a technician do?

A. Reset the browser to default settings

B. Reboot and install antivirus

C. Encourage using a different browser

D. Update the user's web browser

10. What is the most important action a technician can take to protect a server from possible infection when remote access is requested?

A. Create a policy to remove Internet access from the server during off hours

B. Set the local antivirus software on the server to update and scan daily

C. Ensure the server is patched with the latest security updates

D. Educate the manager on safe Internet browsing practices

Answers

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

Explanations

1. A user's phone contains customer's PII. Which of the following is the best method for securing the phone?

A. Fingerprint lock

B. Passcode lock

C. Swipe lock

D. PIN lock

Using a fingerprint lock is considered the best method for securing the phone in a scenario where it contains personally identifiable information (PII) such as customer data. Fingerprint locks provide a high level of security because they rely on biometric authentication, which means that access is granted based on unique physical characteristics of the user. This makes it significantly harder for unauthorized individuals to gain access to the device compared to other methods. Biometric locks, like fingerprint scanning, also offer convenience because users can unlock their phones quickly and easily without the need to remember and input a passcode or PIN. In a situation where sensitive information is involved, such as customer PII, having a more robust security measure in place can help protect this data from potential breaches or unauthorized access. While passcodes and PINs are strong security measures as well, they can be more easily compromised through techniques like social engineering or brute-force attacks. Swipe locks are generally the least secure option among those listed, as they do not require any specific authentication and can be easily bypassed. Thus, a fingerprint lock is optimal for safeguarding sensitive information stored on the phone.

2. What does the acronym IPv4 stand for?

A. Internet Protocol version 2

B. Internet Protocol version 3

C. Internet Protocol version 4

D. Internet Protocol version 5

The acronym IPv4 stands for Internet Protocol version 4. This version of the Internet Protocol is one of the core protocols for the operation of the internet, responsible for addressing and routing packets of data so that they can travel across networks. IPv4 was introduced in the early 1980s and continues to be widely used, even as newer versions like IPv6 have been developed to address issues such as the limited number of available IP addresses in IPv4. In summary, IPv4 specifically refers to the fourth version of the Internet Protocol, marking it as a distinct and critical foundation for networking as we know it today.

3. During a DDoS attack, which types of infections are the source of traffic most likely infected?

A. Spyware

B. Zombies

C. Virus

D. Ransomware

In a Distributed Denial of Service (DDoS) attack, the source of traffic is primarily comprised of "zombies." Zombies refer to devices that have been compromised and are under the control of an attacker, often as part of a botnet. These devices are typically infected by malware and can be used to send large volumes of malicious traffic to a targeted server or network, overwhelming it and causing disruption. Zombies are particularly significant in DDoS attacks because they can encompass a large number of infected devices, allowing attackers to leverage their combined resources to generate a significant amount of traffic. This capability is what makes DDoS attacks effective, as the distributed nature of the attack complicates efforts to mitigate the incoming traffic. Other types of malware mentioned, such as spyware, viruses, and ransomware, do not serve the same role in generating traffic for DDoS attacks. Spyware typically focuses on spying on user activity or stealing information; viruses aim to replicate and spread but are not specifically designed for DDoS attacks; and ransomware's purpose is to encrypt files and demand payment for recovery, rather than generating outbound traffic to a target. Thus, the nature of zombies directly aligns with the mechanisms of a DDoS attack.

4. What compliance is required for businesses using credit cards in both physical and web locations?

A. PHI certification

B. PCI compliance

C. POTS implementation

D. PII filtering

Businesses that handle credit card transactions in both physical and online environments must adhere to PCI compliance, which stands for Payment Card Industry Data Security Standard (PCI DSS). This set of security standards is designed to ensure that all companies that accept, process, store, or transmit credit card information maintain a secure environment. PCI compliance is crucial for protecting cardholder data and helps to reduce the risk of data breaches and fraud. The standards outlined by PCI DSS include requirements for maintaining a secure network, implementing strong access control measures, regularly monitoring and testing networks, and maintaining an information security policy. Achieving PCI compliance not only protects customers' sensitive information but also helps businesses avoid potential fines and legal issues that may arise from data breaches. The other options do not pertain to credit card processing. For instance, PHI certification relates to Protected Health Information, important in the healthcare sector. POTS implementation refers to Plain Old Telephone Service, which is not relevant to credit card transactions. PII filtering focuses on Personally Identifiable Information, which while important, does not specifically address the requirements for handling credit card data. Thus, emphasizing PCI compliance is crucial for any business involved in credit card transactions.

5. What could be a potential reason for a network share to return an "Access Denied" message despite correct user permissions?

A. Insufficient user privileges

B. Disabled network adapter

C. Invalid session tokens

D. Incorrectly configured sharing settings

The potential reason for a network share to return an "Access Denied" message, despite correct user permissions, is due to incorrectly configured sharing settings. When a share is set up, there are numerous configuration options available that determine who can access the share and what type of access they have (read, write, etc.). If these settings are misconfigured—such as not granting access to the specific user or group, or if an exclusion rule overrides allowed permissions—users may encounter an "Access Denied" message even if their individual user permissions appear to be correct. This emphasizes the importance of reviewing both the share permissions and the underlying NTFS permissions on the directory being shared. It's possible for a user to have the necessary permissions to access a file or folder at the NTFS level, but if the sharing settings explicitly deny access to those permissions, the user will be blocked, resulting in the "Access Denied" message. Understanding the distinction between these levels of permission is crucial for troubleshooting access issues effectively.

6. During a planned router OS upgrade, what essential part of the change request must an administrator document?

A. Inform management of the anticipated downtime

B. Document a backout plan to roll back changes

C. Configure a redundant data path to eliminate downtime

D. Make the downtime window larger than expected

Documenting a backout plan to roll back changes is critical during a router OS upgrade. This plan serves as a safeguard, ensuring that if the upgrade encounters issues or does not perform as expected, the administrator can efficiently revert the system to its previous state. The backout plan should include specific steps for reverting changes, system configurations, and any necessary precautions to restore service with minimal disruption. Having this strategy in place not only minimizes downtime but also helps to maintain network stability and performance. In the event of unforeseen complications, an effective backout plan enables swift action, ensuring that the organization can continue to operate without extensive outages. While informing management of anticipated downtime is important for communication, it does not directly impact the technical execution of the upgrade. Configuring a redundant data path can reduce downtime, but it may not be feasible for every upgrade situation. Making the downtime window larger than expected could lead to unnecessary resource use and may frustrate users, but it fails to address the core backup strategy necessary for a smooth changeover. This highlights the importance of having a sound backout plan as part of any upgrade process.

7. 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.

8. What is the function of a proxy server?

A. To store data for offline access

B. To act as an intermediary for requests from clients

C. To provide local network access

D. To encrypt user data

A proxy server functions as an intermediary between a client and another server, handling requests made by clients and relaying those requests to the appropriate destination server. When a client, such as a computer or application, makes a request for a resource on the internet, the proxy server processes this request, potentially modifying it based on various rules, and forwards it to the target server. Once the target server responds, the proxy server receives the data and sends it back to the client. This functionality provides several benefits, including improved performance through caching, enhanced security features by hiding the client's IP address, and the ability to enforce access control over the network by filtering requests. The role of a proxy server is crucial in network management and is widely used in both personal and organizational settings. The other options refer to different technologies or concepts that serve other purposes—storing data for offline access pertains to local storage solutions, providing local network access relates to networking devices like routers or switches, and encrypting user data is typically the role of security protocols rather than a proxy server.

9. A user finds that their web browser opens to an unrecognized search engine and shows irrelevant results. What should a technician do?

A. Reset the browser to default settings

B. Reboot and install antivirus

C. Encourage using a different browser

D. Update the user's web browser

The most effective action in this scenario is resetting the browser to default settings. This process typically removes any unwanted changes made to the browser, which can often occur due to browser hijacking or the installation of suspicious software. By resetting the browser, the technician will eliminate any alterations to the home page, default search engine, and any extensions or plugins that may have been added without the user's consent. This approach is essential for addressing issues such as an unrecognized search engine and irrelevant search results, as it restores the browser to its original state, thereby ensuring the user has a clean slate. After the reset, the user can then configure their browser settings according to their preferences without the interference of potentially harmful changes. Rebooting and installing antivirus can indeed be helpful in some cases, especially if malware is suspected, but it may not directly resolve the immediate issue of the browser's settings. Encouraging the use of a different browser does not address the underlying problem and simply avoids the issue instead of fixing it. Updating the browser is important for security and functionality but will not correct the altered settings that have led to the symptoms described. Thus, resetting to default settings directly targets and resolves the problem effectively.

10. What is the most important action a technician can take to protect a server from possible infection when remote access is requested?

A. Create a policy to remove Internet access from the server during off hours

B. Set the local antivirus software on the server to update and scan daily

C. Ensure the server is patched with the latest security updates

D. Educate the manager on safe Internet browsing practices

The most important action a technician can take to protect a server from potential infection when remote access is requested is to ensure the server is patched with the latest security updates. Applying security patches is crucial because these updates often contain fixes for vulnerabilities that could be exploited by attackers. Servers, as critical components of IT infrastructure, are common targets for malware and other cyber threats. Regularly updating these systems minimizes the risk of exploitation through known vulnerabilities, providing a foundational layer of security against infections. While other actions such as updating antivirus software, creating internet access policies, and educating managers about safe browsing practices contribute to the overall security posture, they are typically secondary measures compared to the impact of patch management. Patching directly addresses vulnerabilities that could be targeted during remote access sessions, making it a priority for any technician tasked with protecting server environments.

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!