SANS Cyber Aces Practice Test (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. What is the main function of anti-virus software?

- **A. To delete all files on a computer**
- **B. To monitor network traffic**
- **C. To detect and remove malware**
- **D. To create backup copies of files**

2. What is the primary use of the 'ren' command?

- **A. Remove a file**
- **B. Rename a file**
- **C. Render a file**
- **D. Return file properties**

3. What noun is used in cmdlets to manage the execution policy for scripts?

- **A. ScriptPolicy**
- **B. ExecutionPolicy**
- **C. PolicyControl**
- **D. ScriptExecution**

4. What is a cybersecurity incident?

- **A. A planned maintenance activity**
- **B. An unauthorized access attempt to information systems**
- **C. Any security software update**
- **D. A regular audit of network security**

5. What is the purpose of patch management?

- **A. To install new hardware**
- **B. To keep software updated and fix vulnerabilities**
- **C. To delete outdated data**
- **D. To enhance user interface**

6. What does the acronym MFA stand for in cybersecurity?

- **A. Multi-Factor Authentication**
- **B. Micro-Focused Analysis**
- **C. Major Firewall Access**
- **D. Multi-Frequency Algorithm**

7. What is the primary function of antivirus software?

A. To track user online activity

B. To create backups of files

C. To detect, prevent, and remove malicious software (malware)

D. To improve system performance

8. What defines an access control list (ACL)?

A. A set of user passwords

B. A database of network devices

C. A set of rules governing user access to resources

D. A security protocol for wireless networks

9. What information does the netstat command provide in Windows?

A. Current user accounts

B. Active network connections, ports, routing table

C. Last boot time

D. File system permissions

10. What does the command 'cat' do in Linux?

A. Display the contents of a file

B. Edit a file

C. Change directory

D. Archive files

Answers

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

Explanations

1. What is the main function of anti-virus software?

A. To delete all files on a computer

B. To monitor network traffic

C. To detect and remove malware

D. To create backup copies of files

The primary function of anti-virus software is to detect and remove malware. This includes various types of malicious software such as viruses, worms, trojans, ransomware, and spyware. Anti-virus programs use signature-based detection, heuristics, and behavior-based detection techniques to identify and neutralize threats. By regularly scanning the system and protecting it in real-time, anti-virus software helps to safeguard your data and maintain system integrity against potential attacks. In contrast, deleting all files on a computer would not be a viable function of anti-virus software, as this action is destructive and undermines the purpose of protecting data. Monitoring network traffic is typically handled by other security solutions, such as intrusion detection systems or firewalls, rather than anti-virus software. Creating backup copies of files is usually the function of backup software, not anti-virus, although some security suites may offer limited backup features as part of a broader set of tools.

2. What is the primary use of the 'ren' command?

A. Remove a file

B. Rename a file

C. Render a file

D. Return file properties

The primary use of the 'ren' command is to rename a file. This command allows users to change the name of an existing file or directory within the command-line interface of operating systems like Windows. When using 'ren', you specify the current name of the file followed by the new name you want to assign to it. This operation is fundamental for file management, enabling users to maintain organized files and directories, which can help prevent confusion and improve workflow. While other commands might relate to files, such as deleting or checking properties, 'ren' is specifically designed for renaming, making it the correct answer in this context.

3. What noun is used in cmdlets to manage the execution policy for scripts?

A. ScriptPolicy

B. ExecutionPolicy

C. PolicyControl

D. ScriptExecution

The noun used in cmdlets to manage the execution policy for scripts is "ExecutionPolicy." In PowerShell, the execution policy is a security feature that determines whether scripts can run on the system and what permissions they require. It helps to protect users from running potentially harmful scripts. The cmdlets associated with setting and retrieving the execution policy, such as `Get-ExecutionPolicy` and `Set-ExecutionPolicy`, specifically utilize "ExecutionPolicy" as a parameter to define the policy levels. This includes options like Restricted, AllSigned, RemoteSigned, Unrestricted, and Bypass, which offer varying degrees of restriction on script execution. The other options, while they may sound relevant, do not represent the correct terminology used in PowerShell for managing script execution. "ScriptPolicy," "PolicyControl," and "ScriptExecution" are not recognized terms in the context of PowerShell's execution policy management, making "ExecutionPolicy" the appropriate choice in this scenario.

4. What is a cybersecurity incident?

A. A planned maintenance activity

B. An unauthorized access attempt to information systems

C. Any security software update

D. A regular audit of network security

A cybersecurity incident refers specifically to events that pose a threat to the confidentiality, integrity, or availability of information systems. It typically involves unauthorized access or attempted access to systems, data breaches, or any activities that compromise the security posture of an organization. The option that defines a cybersecurity incident accurately is one that highlights unauthorized access attempts. Such incidents can include hacking attempts, malware infections, or data theft, which are serious concerns for any organization that manages sensitive data. The other options describe activities that are part of routine operations or maintenance. Planned maintenance activities, security software updates, and regular audits are all essential components of maintaining a secure environment, but they do not fall under the definition of a cybersecurity incident since they don't involve a breach or threat to security. Understanding the distinction between routine activities and incidents is crucial in the field of cybersecurity to ensure appropriate responses and defenses are in place.

5. What is the purpose of patch management?

A. To install new hardware

B. To keep software updated and fix vulnerabilities

C. To delete outdated data

D. To enhance user interface

The purpose of patch management primarily revolves around keeping software updated and fixing vulnerabilities. In the realm of cybersecurity, software patches are essential for addressing security flaws that could be exploited by attackers. When vulnerabilities are discovered, software vendors typically release patches to correct these issues. By implementing a robust patch management process, organizations ensure that their systems are fortified against known threats, thus reducing the risk of breaches or other security incidents. Additionally, patch management helps maintain software performance and stability, as updates often include improvements and optimizations, but the core focus remains on the security aspect. Keeping systems patched and updated is a critical component of a comprehensive cybersecurity strategy, ensuring that known vulnerabilities are mitigated as part of proactive defense efforts.

6. What does the acronym MFA stand for in cybersecurity?

A. Multi-Factor Authentication

B. Micro-Focused Analysis

C. Major Firewall Access

D. Multi-Frequency Algorithm

The acronym MFA stands for Multi-Factor Authentication in the context of cybersecurity. Multi-Factor Authentication is a security measure that requires users to provide two or more verification factors to gain access to a resource, such as an application, online account, or database. This approach enhances security by adding an additional layer of defense beyond just a username and password. Typically, MFA combines something the user knows (like a password), something the user has (such as a smartphone app that generates a one-time code), or something the user is (biometric factors like fingerprints or facial recognition). The importance of MFA lies in its ability to significantly reduce the risk of unauthorized access, even if one of the factors (like a password) is compromised. Other options listed do not reflect established concepts in cybersecurity. For instance, Micro-Focused Analysis is not recognized as a security principle, Major Firewall Access does not align with common terminology in the field, and Multi-Frequency Algorithm does not pertain to authentication processes. Thus, Multi-Factor Authentication stands out as the correct and relevant term in cybersecurity practices.

7. What is the primary function of antivirus software?

A. To track user online activity

B. To create backups of files

C. To detect, prevent, and remove malicious software (malware)

D. To improve system performance

The primary function of antivirus software is to detect, prevent, and remove malicious software (malware). Antivirus programs are designed to identify various types of malware, including viruses, worms, trojans, ransomware, and spyware, which can compromise computer systems and user data. By continuously scanning files and monitoring system activity, antivirus software can provide real-time protection, alert users to potential threats, and execute the necessary actions to mitigate risks, such as quarantining infected files or removing malware altogether. This core functionality is essential for maintaining the integrity and security of a computer system, allowing users to operate without the fear of malicious attacks compromising their information or system performance.

8. What defines an access control list (ACL)?

A. A set of user passwords

B. A database of network devices

C. A set of rules governing user access to resources

D. A security protocol for wireless networks

An access control list (ACL) is fundamentally defined as a set of rules that govern which users or systems have access to particular resources and what operations they can perform on those resources. This can include permissions such as reading, writing, or executing files or services. ACLs are commonly used in network security to control access to resources, such as files and directories, ensuring that only authorized individuals can access sensitive information or perform critical operations. In network devices, ACLs are also utilized to manage traffic control and enhance the security posture by allowing or denying the flow of traffic based on specified conditions, such as IP addresses or protocols. This structure is crucial for establishing a clear access framework within various environments, ensuring that protections are in place to prevent unauthorized access or misuse. In short, an ACL is designed specifically to articulate and enforce access controls, making option C the correct definition.

9. What information does the netstat command provide in Windows?

A. Current user accounts

B. Active network connections, ports, routing table

C. Last boot time

D. File system permissions

The netstat command in Windows is a powerful networking tool that provides information about active network connections, listening ports, and the routing table. When executed, it displays details about the current state of network traffic on the system, including both incoming and outgoing connections, along with information on the status of each connection such as established, listening, or closed. This command is crucial for troubleshooting network issues and monitoring network performance, as it allows users to see which applications or services are using network resources and to identify any potentially unauthorized connections that may pose a security risk. Therefore, the correct answer highlights the primary functionality of netstat as it pertains to monitoring network-related information.

10. What does the command 'cat' do in Linux?

A. Display the contents of a file

B. Edit a file

C. Change directory

D. Archive files

The command 'cat' in Linux is primarily used to display the contents of a file in the terminal or command-line interface. It reads data from the specified file and outputs it, allowing users to view the text directly without opening an editor. This command is quite versatile; for example, it can also be used to concatenate multiple files and display their combined contents. However, its fundamental purpose is to show file contents to the user, making it an essential tool for quick file checks and data examination. The other options focus on actions that are not associated with the 'cat' command. Editing a file requires different commands or tools designed for that purpose, such as 'nano' or 'vim.' Changing directories is performed using the 'cd' command, while archiving files involves utilities like 'tar' or 'zip.' Thus, the functionality of 'cat' as a file viewer is what distinctly sets it apart in this context.

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://sanscyberaces.examzify.com

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