SANS CYBER ACES PRACTICE TEST (SAMPLE)

STUDY GUIDE



SAMPLE STUDY GUIDE WITH LIMITED QUESTIONS

VISIT US ONLINE FOR THE FULL VERSION STUDY GUIDE

https://sanscyberaces.examzify.com

Copyright © 2026 by Examzify - A Kaluba Technologies Inc. product.

ALL RIGHTS RESERVED.

No part of this book may be reproduced or transferred in any form or by any means, graphic, electronic, or mechanical, including photocopying, recording, web distribution, taping, or by any information storage retrieval system, without the written permission of the author.

Notice: Examzify makes every reasonable effort to obtain accurate, complete, and timely information about this product from reliable sources.

SAMPLE

Table of Contents

Copyright 1

Table of Contents 2

Introduction 3

How to Use This Guide 4

Questions 5

Answers 8

Explanations 10

Next Steps 16

SAMPLE

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.

SAMPLE

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!

SAMPLE

Questions

SAMPLE

1. What does a subnet mask do in a network?

A. Identifies the device's MAC address

B. Defines the network and host portions of an IP address

C. Secures the network from unauthorized access

D. Connects devices to the internet

2. Which command will list the files on a remote share?

A. ls \\servername\share

B. dir \\servername\share

C. list \\servername\share

D. show \\servername\share

3. In which section of the Local Security Policy can you grant a user permission to change the time zone?

A. Security Options

B. User Rights Assignments

C. Account Policies

D. Audit Policy

4. If a user belongs to a group with explicit "ALLOW" and another with explicit "DENY" for reading a file, what will be the outcome?

A. The user will be able to read the file

B. The user will not be able to read the file

C. The user's access will be determined by the group with more permissions

D. The user will receive a prompt for permission

5. What are the main components of an intrusion detection system (IDS)?

A. Firewalls, routers, and switches

B. Sensors, management server, and user interface

C. Encryption, authentication, and logging

D. Data storage, routing, and analysis

SAMPLE

6. Which command can be used in Windows to display a list of network connections?

A. ipconfig

B. netstat

C. tracert

D. nslookup

7. What does the tasklist command do in Windows?

A. Lists system configurations

B. Lists currently running processes

C. Displays network settings

D. Monitors disk usage

8. Which command is NOT used to either create or delete directories?

A. mkdir

B. rmdir

C. del

D. ren

9. At which layer do switches operate within the OSI model?

A. Layer 2

B. Layer 1

C. Layer 3

D. Layer 4

10. What is the output of 'Write-Output "Hello World"'?

A. Prints "Hello World" to the console

B. Creates a new variable

C. Returns "Hello World" without printing

D. Errors out with a message

SAMPLE

Answers

SAMPLE

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

SAMPLE

Explanations

SAMPLE

1. What does a subnet mask do in a network?

A. Identifies the device's MAC address

B. Defines the network and host portions of an IP address

C. Secures the network from unauthorized access

D. Connects devices to the internet

A subnet mask plays a critical role in facilitating network communication by defining which portion of an IP address indicates the network and which part identifies the host within that network. In IP addressing, every device must be aware of its place within the overall network structure. The subnet mask accomplishes this by employing a binary representation that separates the two segments of the IP address. For example, consider an IP address of 192.168.1.10 with a subnet mask of 255.255.255.0. The subnet mask informs the device that the first three octets (192.168.1) represent the network part, while the last octet (.10) identifies the specific device or host. This arrangement enables routers and switches to efficiently manage traffic and data transmission within the network, ensuring that packets are appropriately directed to their destination. The other choices do not align with the primary function of a subnet mask. Identifying a device's MAC address involves different protocols and methods that operate at layer 2 of the OSI model, while securing the network relates to firewalls and authentication measures rather than segmentation of IP addresses. Lastly, connecting devices to the internet generally involves routers and gateways, and is not a direct function of the subnet mask itself.

2. Which command will list the files on a remote share?

A. ls \\servername\share

B. dir \\servername\share

C. list \\servername\share

D. show \\servername\share

The command that effectively lists the files on a remote share is "dir \\servername\share." This command is used in the Windows command-line interface to display a list of files and directories in the specified location. When you provide the path to a network share using this command format, it queries the remote server for its contents and prints them to the screen. Using "dir" is appropriate here because it is the standard command for listing directory contents in DOS, Windows, and compatible operating systems. It allows users to see not only the names of the files but also additional details like file sizes and creation dates depending on the options specified. Other options, while they seem plausible, are not correct. "ls" is a command used in Unix/Linux systems for listing directory contents, not typically used for Windows shares. "list" and "show" are not recognized commands in command-line interfaces for listing files and directories. Thus, the choice of "dir" aligns perfectly with the requirements for accessing and displaying files from a remote share in a Windows environment.

SAMPLE

3. In which section of the Local Security Policy can you grant a user permission to change the time zone?

A. Security Options

B. User Rights Assignments

C. Account Policies

D. Audit Policy

The section of the Local Security Policy that allows you to grant a user permission to change the time zone is found within User Rights Assignments. This part of the Local Security Policy deals with the various privileges that can be assigned to users or groups, allowing them to perform specific actions on the system. Changing the time zone is considered a system-level function that falls under the category of user rights because it affects how the operating system manages time and interacts with time-sensitive tasks and services. Therefore, only users with the appropriate permissions should have the ability to make such changes. In contrast, Security Options typically include a variety of security-specific settings, such as account lockout policies and user authentication methods, while Account Policies focus primarily on password requirements and user account settings. Audit Policy is concerned with defining what system events should be logged for monitoring and compliance purposes. None of these sections directly handle user rights related to system-level operations like changing the time zone.

4. If a user belongs to a group with explicit "ALLOW" and another with explicit "DENY" for reading a file, what will be the outcome?

A. The user will be able to read the file

B. The user will not be able to read the file

C. The user's access will be determined by the group with more permissions

D. The user will receive a prompt for permission

When a user is part of two different groups that have conflicting permissions, the general rule in access control lists (ACLs) is that the "DENY" permission takes precedence over an "ALLOW" permission. Therefore, if a user belongs to a group which has been given explicit "ALLOW" for reading a file, but is also part of another group that has explicit "DENY," the user will not be able to read the file. This prioritization of "DENY" over "ALLOW" helps in maintaining strict security protocols, ensuring that if there is any doubt around a user's access rights, the most restrictive access control is applied to protect sensitive data. Hence, when resolving conflicting permissions, the presence of an explicit denial effectively overrides any explicit allowance that may exist for the same resource, resulting in denied access in this scenario.

SAMPLE

5. What are the main components of an intrusion detection system (IDS)?

A. Firewalls, routers, and switches

B. Sensors, management server, and user interface

C. Encryption, authentication, and logging

D. Data storage, routing, and analysis

An intrusion detection system (IDS) is primarily focused on monitoring network traffic for suspicious activities and potential threats. The main components of an IDS include sensors, which are responsible for collecting data from the network or host systems to detect any malicious activities. The management server processes the data received from these sensors, analyzing signs of intrusion and taking notes of any actionable threats. Finally, the user interface allows operators and security analysts to interact with the IDS, view reports, and manage the system effectively. Understanding this architecture is crucial because it highlights how the IDS operates as a cohesive unit that relies on each component to fulfill its purpose of threat detection and response. Components such as firewalls, routers, and switches, while important in network security, do not specifically pertain to the IDS function. Similarly, encryption, authentication, and logging, while relevant for overall security, are not integral parts of the IDS framework itself. The focus on data storage, routing, and analysis in other options reflects general network management and security practices rather than the specific structure and operational workflow of an IDS.

6. Which command can be used in Windows to display a list of network connections?

A. ipconfig

B. netstat

C. tracert

D. nslookup

The command that can be used in Windows to display a list of network connections is netstat. This command provides information about active connections, including the local and remote IP addresses, the ports being used, and the current status of each connection. It is particularly useful for network troubleshooting and monitoring, as it allows users to see what connections are established and any open ports that may be listening for incoming traffic. In contrast, ipconfig is designed to display the current network configuration of the computer, including the IP address, subnet mask, and default gateway, but does not show connection statuses. Tracert is used to determine the path that packets take to a specific host, showing each hop along the way, rather than listing active connections. Nslookup is a command-line tool used for querying DNS to obtain domain name or IP address mapping information, which is unrelated to displaying network connections. Therefore, netstat is the appropriate command for viewing active network connections.

SAMPLE

7. What does the tasklist command do in Windows?

A. Lists system configurations

B. Lists currently running processes

C. Displays network settings

D. Monitors disk usage

The tasklist command in Windows is specifically designed to display a list of all currently running processes on the system. This command provides valuable information such as the process name, its Process ID (PID), and uses memory, among other details. You can utilize this command to troubleshoot issues, monitor application performance, or kill processes, as needed, using additional commands. Other choices focus on different functionalities: system configurations or settings are not provided by the tasklist command, network settings would be displayed using another command like ipconfig, and disk usage monitoring falls under commands like dir or checking system properties rather than the purpose of tasklist. Therefore, the primary function of tasklist is to enumerate active processes, making the correct answer clear.

8. Which command is NOT used to either create or delete directories?

A. mkdir

B. rmdir

C. del

D. ren

The command that is NOT used to either create or delete directories is the one referred to as ren. The ren command, short for "rename," is specifically designed to alter the name of existing files or directories rather than creating or removing them. This command enables users to change the names of files or directories without affecting their content or structure. It serves a different purpose, focusing on the organization and labeling of files rather than their existence. In contrast, mkdir is used to create new directories, while rmdir is employed to delete empty directories. The del command, typically associated with deleting files, can also impact directories but generally operates on the files contained within them. Understanding these commands helps users manage their file systems effectively by knowing which commands pertain to creating, deleting, or renaming file system objects.

9. At which layer do switches operate within the OSI model?

A. Layer 2

B. Layer 1

C. Layer 3

D. Layer 4

Switches primarily operate at Layer 2 of the OSI model, which is known as the Data Link layer. This layer is responsible for node-to-node data transfer and for handling error correction from the physical layer. Switches use MAC addresses to forward data frames between devices within the same local area network (LAN). By analyzing the destination MAC address in a frame, a switch decides which port to forward the frame to, facilitating efficient communication between devices. Layer 1, the Physical layer, is concerned with the actual hardware and transmissions of the bits over media such as cables, while Layer 3, the Network layer, involves routing and forwarding packets based on IP addresses. Layer 4, the Transport layer, deals with end-to-end communication and error recovery between two hosts. Therefore, switch functionalities, which include the operation based on MAC addresses and frame switching, clearly align with the responsibilities designated to Layer 2.

SAMPLE

10. What is the output of 'Write-Output "Hello World"'?

A. Prints "Hello World" to the console

B. Creates a new variable

C. Returns "Hello World" without printing

D. Errors out with a message

The output of the command 'Write-Output "Hello World"' is that it prints "Hello World" to the console. The 'Write-Output' cmdlet in PowerShell is specifically designed to send output to the pipeline, and if it is the last command in a script or if it is in the console, it displays the output on the screen. This means that when this command is executed, you will see "Hello World" appear in the console, confirming the intended outcome of the command. Notably, this behavior is typical in many scripting environments where output commands are executed to provide feedback directly to the user.

SAMPLE

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!

SAMPLE