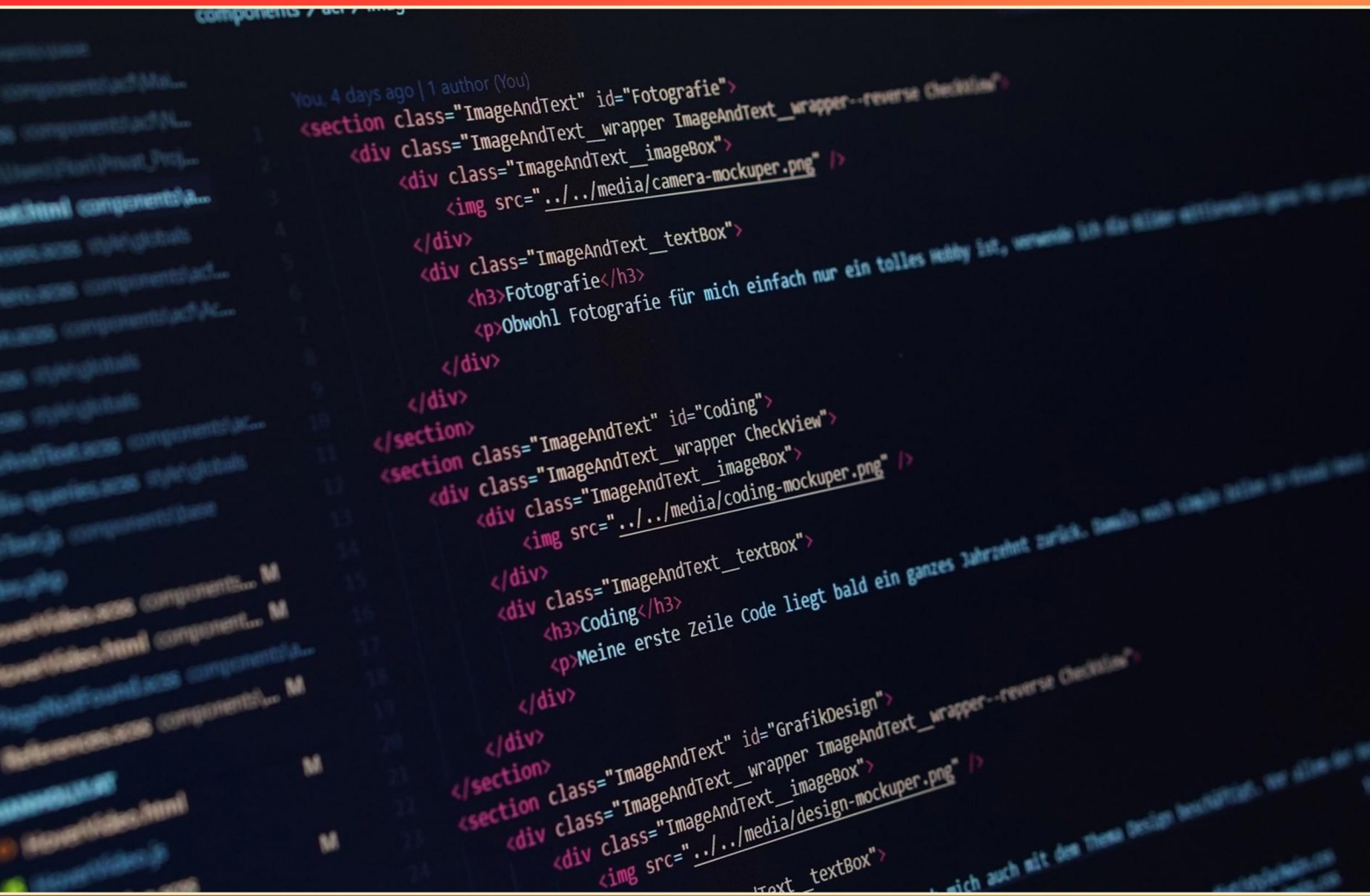
EC-COUNCIL NETWORK DEFENSE ESSENTIALS (NDE) PRACTICE TEST (SAMPLE)

STUDY GUIDE



SAMPLE STUDY GUIDE WITH LIMITED QUESTIONS

VISIT US ONLINE FOR THE FULL VERSION STUDY GUIDE

https://excouncilnde.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 15

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. A wireless modem is a device that allows PCs to connect to a wireless network and access the Internet through an ISP, commonly including USB sticks. What is this device called?

A. Wireless bridge

B. Dipole antenna

C. Wireless modem

D. Bluetooth dongle

2. Standpipe systems provide water to hose lines by connecting to the water supply. Which statement is true?

A. True

B. False

C. Not specified

D. Not applicable

3. Which statement about the statistics toolbar is true?

A. It can be customized by the user

B. It shows only flow graphs

C. It is the same as the main toolbar

D. It cannot be customized by the user

4. Which Docker networking option allows a container to use the host's network namespace?

A. Bridge

B. MACVLAN

C. Overlay

D. Host Driver

5. Which function is a cryptographic hash function developed by NIST and included in the Secure Hash Standard?

A. SHA

B. DES

C. AES

D. MD5

SAMPLE

6. Which window displays the protocol hierarchy statistics?

A. IO Graphs

B. Protocol Hierarchy Statistics

C. Summary of Captured Packets

D. Flow Graphs

7. The Device-to-Cloud model extends data sharing to authorized third parties. Which option best describes this access?

A. Authorized third parties

B. Local administrators

C. The cloud service provider

D. The device itself

8. Which standard defines the Digital Signature Algorithm (DSA) used in the Digital Signature Standard (DSS)?

A. FIPS 180

B. FIPS 197

C. FIPS 200

D. FIPS 186

9. Windows Information Protection provides endpoint DLP capabilities and can be configured to store business data only on approved devices and applications. Which technology is this?

A. DLP

B. LOIC

C. HOIC

D. WIP

10. Which principle applies to the IoT communication layer, focusing on machine-to-machine identification, authentication, and encryption rather than human credentials?

A. Device autonomy and local processing.

B. User-based access control for dashboards.

C. Identification, authentication, and encryption for machines.

D. Physical tamper resistance of devices.

SAMPLE

Answers

SAMPLE

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

SAMPLE

Explanations

SAMPLE

1. A wireless modem is a device that allows PCs to connect to a wireless network and access the Internet through an ISP, commonly including USB sticks. What is this device called?

A. Wireless bridge

B. Dipole antenna

C. Wireless modem

D. Bluetooth dongle

The essential idea here is identifying the device that connects your local network to your Internet Service Provider. A wireless modem is the piece of hardware that terminates the ISP connection and, when equipped for wireless, lets devices share that Internet access over Wi Fi. USB sticks mentioned are a common form of mobile broadband modems that plug into a computer to provide Internet access via a cellular network, which fits the description perfectly. Why this fits over the others: a wireless bridge connects two networks but isn't the endpoint that talks to the ISP for Internet access; a dipole antenna is just an RF radiator used to improve signal, not to provide Internet connectivity; a Bluetooth dongle adds Bluetooth for short-range device communication, not Internet access.

2. Standpipe systems provide water to hose lines by connecting to the water supply. Which statement is true?

A. True

B. False

C. Not specified

D. Not applicable

Standpipe systems are designed to deliver water through hose lines from a dedicated water supply. They run piping to hose outlets in the building and are fed by the water supply—either as a wet system where water is already in the pipes under pressure, or as a dry system where water enters the pipes when a valve is opened and pressurized by the fire department or a pump. Because the purpose is to provide a readily available water source to hose lines via a connection to the water supply, the statement is true.

3. Which statement about the statistics toolbar is true?

A. It can be customized by the user

B. It shows only flow graphs

C. It is the same as the main toolbar

D. It cannot be customized by the user

The idea being tested is whether the statistics toolbar is customizable by the user. In many monitoring interfaces, the statistics toolbar is meant to provide a stable, at-a-glance view of key metrics, so operators can rely on seeing the same data in the same place across sessions. Because of this consistency, it's designed to be non-customizable by the user, ensuring that critical statistics remain visible and in predictable locations. This toolbar isn't limited to flow graphs; it usually displays a mix of numerical readouts and small graphs that summarize system or network performance, not just a single type of visualization. It isn't the same as the main toolbar, which typically houses controls and commands rather than data displays. So the statement that the statistics toolbar cannot be customized by the user is the correct one.

SAMPLE

4. Which Docker networking option allows a container to use the host's network namespace?

A. Bridge

B. MACVLAN

C. Overlay

D. Host Driver

The option in use here is the one that makes the container share the host's network stack. Using the host driver places the container in the host's network namespace, so it uses the host's IP address and can access services on localhost directly. There's no separate network namespace, no NAT between the container and the host, and no port mapping needed. This setup can improve performance and simplify some configurations, but it sacrifices isolation and portability—containers become tightly tied to the host's network environment. Bridge creates an independent, isolated network for containers behind a virtual bridge. MACVLAN gives each container its own MAC address on the physical network, appearing as a separate device. Overlay builds a network that spans multiple hosts (useful in Swarm) but still uses container-specific namespaces.

5. Which function is a cryptographic hash function developed by NIST and included in the Secure Hash Standard?

A. SHA

B. DES

C. AES

D. MD5

The question tests knowledge of which cryptographic hash function is standardized by NIST within the Secure Hash Standard. SHA is the hash function family developed by NIST and included in SHS, meaning it's the one defined and standardized for hashing purposes by this standard. The other options are not part of SHS for hashing: DES and AES are encryption algorithms (not hashes), and MD5 is an older hash function not part of SHS and is considered insecure today. So SHA is the best answer because it is the NIST-developed hash function officially included in the Secure Hash Standard.

6. Which window displays the protocol hierarchy statistics?

A. IO Graphs

B. Protocol Hierarchy Statistics

C. Summary of Captured Packets

D. Flow Graphs

The main idea here is to identify which view shows how the captured traffic is distributed across protocols, organized in a hierarchy. The Protocol Hierarchy Statistics window in a packet analyzer presents a tree of protocols and subprotocols, with counts and percentages for each, so you can see exactly how the traffic is composed and how protocols nest within each other. This is why it's the best match for "protocol hierarchy statistics." IO Graphs plot traffic over time, useful for spotting bursts or throughput trends. Summary of Captured Packets (often just "Summary") shows overall capture stats like total packets and duration. Flow Graphs visualize conversations between endpoints. None of these display the hierarchical breakdown of protocols like the Protocol Hierarchy Statistics window does.

SAMPLE

7. The Device-to-Cloud model extends data sharing to authorized third parties. Which option best describes this access?

A. Authorized third parties

B. Local administrators

C. The cloud service provider

D. The device itself

In Device-to-Cloud setups, data moves from devices up into cloud services, and sometimes you extend access beyond your own organization to external entities that are explicitly allowed to use that data. The term that best describes this is authorized third parties—external partners, vendors, or external analytics services that have been granted permission and credentials to access the data stored in the cloud. This keeps sharing controlled and auditable, using mechanisms like tokens, roles, and API permissions tied to formal data-sharing arrangements. Local administrators are internal personnel managing systems, so their access isn't the external, third-party sharing many Device-to-Cloud scenarios involve. The cloud service provider runs the platform but isn't the external partner being described here; the focus is on who outside the organization is allowed to access the data. The device itself is simply the data producer and push source, not a party that's granted ongoing access to the data in the cloud.

8. Which standard defines the Digital Signature Algorithm (DSA) used in the Digital Signature Standard (DSS)?

A. FIPS 180

B. FIPS 197

C. FIPS 200

D. FIPS 186

DSA is the digital signature algorithm specified for use within the Digital Signature Standard. The document that defines how this algorithm works—covering the math, parameter sizes, key generation, signing, and verification—is FIPS 186. Hash functions used with the signature process are described in FIPS 180, which explains the digest that gets signed. The other standards listed cover different technologies (FIPS 197 defines AES, FIPS 200 outlines general security requirements, and FIPS 180 covers hash functions) and do not define the signature algorithm itself. So the standard that defines the DSA used in DSS is FIPS 186.

9. Windows Information Protection provides endpoint DLP capabilities and can be configured to store business data only on approved devices and applications. Which technology is this?

A. DLP

B. LOIC

C. HOIC

D. WIP

Endpoint data protection at the device level relies on Windows Information Protection. This Windows feature creates a boundary around corporate data so it can reside and be used only within approved, managed applications on enrolled devices. By labeling apps as work apps and enforcing which apps can access and save business information, WIP prevents corporate data from being stored in or opened by unmanaged or personal apps, and it can restrict actions like copy/paste or saving to personal cloud locations. Deploying these policies through management tools keeps business data on approved devices and apps, aligning with data loss prevention goals at the endpoint. The other options don't fit: LOIC and HOIC are tools for denial-of-service activities, and DLP is a broad concept rather than a specific technology name.

SAMPLE

10. Which principle applies to the IoT communication layer, focusing on machine-to-machine identification, authentication, and encryption rather than human credentials?

A. Device autonomy and local processing.

B. User-based access control for dashboards.

C. Identification, authentication, and encryption for machines.

D. Physical tamper resistance of devices.

In IoT, securing the communication layer means ensuring devices prove who they are to each other and that their messages are kept confidential and tamper-proof. This involves giving each device an identity, performing authentication between devices, and using encryption to protect data in transit. This machine-to-machine identification, authentication, and encryption focus is what keeps inter-device communications trustworthy without relying on human credentials. The other ideas touch on related security topics but aren't about the trust and confidentiality of device-to-device messaging: on-device processing speaks to capabilities of the device itself, user-based access control targets humans accessing dashboards, and physical tamper resistance deals with hardware hardening rather than the secure exchange of data between devices.

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://excouncilnde.examzify.com

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

SAMPLE