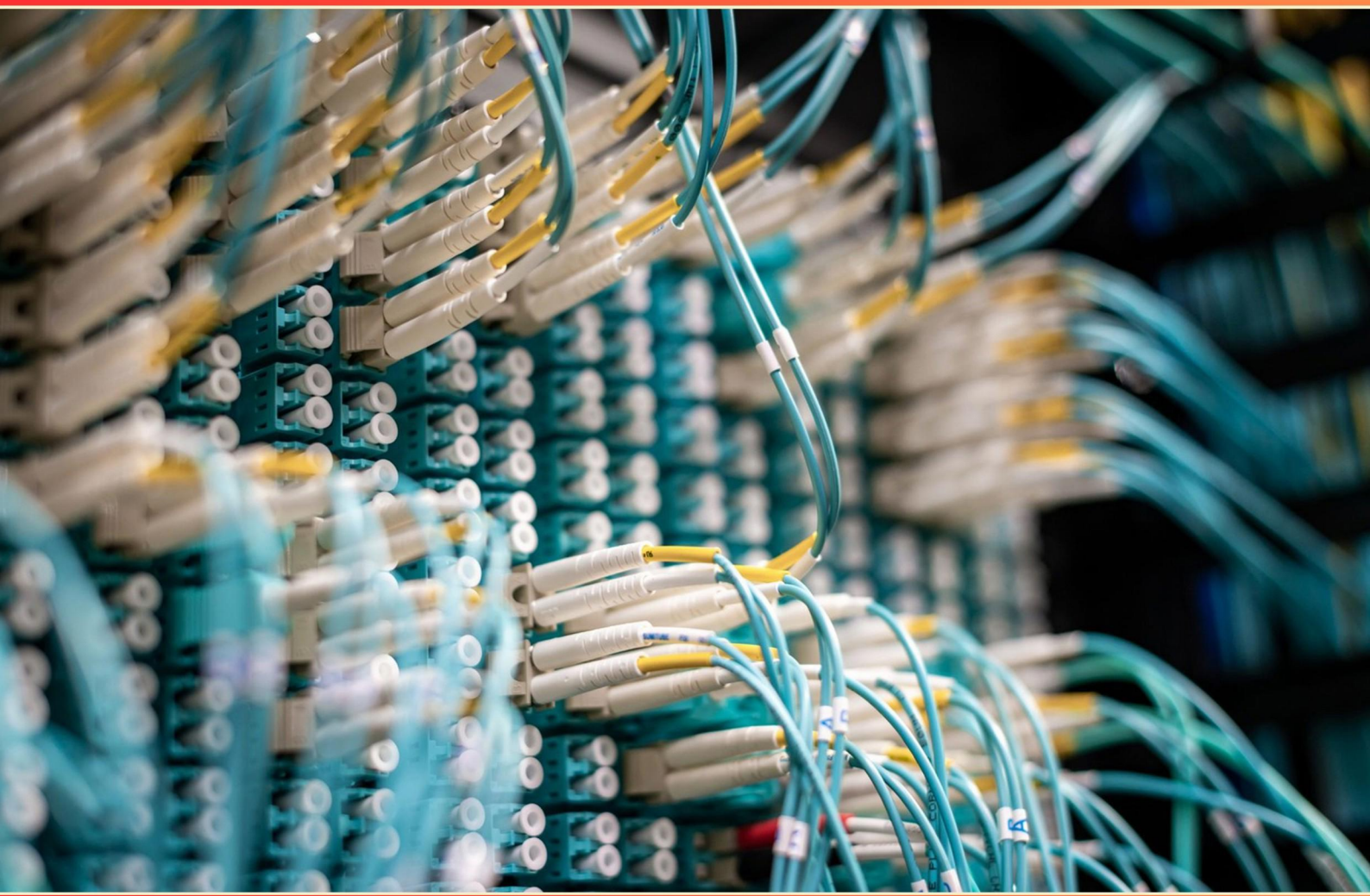
NETWORK SECURITY (NETSEC) 1 PRACTICE TEST (SAMPLE)

STUDY GUIDE



SAMPLE STUDY GUIDE WITH LIMITED QUESTIONS

VISIT US ONLINE FOR THE FULL VERSION STUDY GUIDE

https://netsec1.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. Cyberwar is described as attacks carried out by _____.

A. National governments

B. Terrorists

C. Both A and B

D. Neither A nor B

2. Which of the following is true about the relationship between detective and preventative countermeasures?

A. Detective measures identify attacks; preventative measures stop them from succeeding.

B. Detective measures stop attacks; preventative measures only identify.

C. Both types are identical in function.

D. Neither type is used in modern networks.

3. Penalties for hacking are _____.

A. Limited only if a hacker stole $1000

B. Limited only if a hacker stole over $1,000,000

C. Irrelevant of the amount stolen

D. None of the above

4. It is true or false that rootkits replace legitimate programs and are a deeper threat than Trojan horses?

A. True

B. False

C. Cannot determine

D. Both

5. If you discover you can access someone else's files by hitting a certain key and you look around briefly, this is hacking.

A. True

B. False

C. It depends on intent

D. Not illegal

SAMPLE

6. Which term describes a targeted phishing attack aimed at a specific individual?

A. Social engineering

B. Hoax

C. Phishing

D. Spear phishing

7. Which of the following are types of countermeasures?

A. Preventative

B. Detective

C. Corrective

D. All Of The Above

8. _____ is a generic term for "evil software."

A. Virus

B. Worm

C. Malware

D. Threat

9. Which statement best captures the difference between a firewall and an IDS?

A. Firewall controls traffic flow; IDS detects and alerts on suspicious activity.

B. Firewall detects and alerts; IDS controls traffic flow.

C. They perform the same function; no difference.

D. Firewall authenticates users; IDS encrypts data.

10. Trade secret theft can occur through interception, hacking, and other traditional cybercrimes.

A. True

B. False

C. Not sure

D. Sometimes

SAMPLE

Answers

SAMPLE

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

SAMPLE

Explanations

SAMPLE

1. Cyberwar is described as attacks carried out by _____.

A. National governments

B. Terrorists

C. Both A and B

D. Neither A nor B

Cyberwar is framed as warfare in cyberspace conducted by nation-states using their governmental and military capabilities. The idea is that states, not non-state actors, wage wars in the digital realm to disrupt another country's critical systems, infrastructure, or military operations as an instrument of national power. While terrorist groups can and do carry out cyberattacks, those actions are typically categorized as cyberterrorism or cybercrime rather than formal cyberwar between states. Therefore, the best description is attacks carried out by national governments.

2. Which of the following is true about the relationship between detective and preventative countermeasures?

A. Detective measures identify attacks; preventative measures stop them from succeeding.

B. Detective measures stop attacks; preventative measures only identify.

C. Both types are identical in function.

D. Neither type is used in modern networks.

Detective and preventative countermeasures complement each other in a layered security approach. Preventive controls are designed to block unauthorized actions before they happen—firewalls, access controls, patching, and encryption all aim to stop attacks from succeeding. Detective controls monitor for signs of malicious activity, identify attacks as they occur or after they begin, and alert for containment and investigation—think intrusion detection systems, SIEMs, and log analysis. That distinction is why the statement is true: detective measures identify attacks, while preventative measures stop them from succeeding. In practice, you want both. Preventives reduce the attack surface and block many threats upfront, while detectives catch what slips past and enable quick response. Relying only on prevention risks missed or evasive attacks, and relying only on detection risks damage before you can respond. Together they provide effective defense-in-depth.

3. Penalties for hacking are _____.

A. Limited only if a hacker stole $1000

B. Limited only if a hacker stole over $1,000,000

C. Irrelevant of the amount stolen

D. None of the above

Penalties for hacking come from the illegal act itself, not from the dollar value involved. Unauthorised access, data exfiltration, or system damage triggers legal consequences regardless of how much money is stolen. The offense is punishable because the act destabilizes systems and violates laws, and the punishment can apply even if the stolen amount is small. While in some cases the amount stolen may influence sentencing, it does not restrict penalties to only certain dollar thresholds. This is why the statement that penalties are irrelevant of the amount stolen best captures how cybercrime penalties are typically structured.

SAMPLE

4. It is true or false that rootkits replace legitimate programs and are a deeper threat than Trojan horses?

A. True

B. False

C. Cannot determine

D. Both

Rootkits are built to hide the presence of malware and maintain control by manipulating how the system presents itself—often by intercepting system calls or altering kernel or other components. Their main goal is stealth and persistence, not necessarily to replace legitimate programs. Trojan horses rely on tricking users into thinking a malicious program is legitimate, and then delivering their payload. Because replacing legitimate programs is not a defining or universal trait of rootkits, and because the overall danger depends on what the malware does, the statement isn't accurate. Some Trojan horses can be just as harmful, and some rootkits mainly enable concealment for other threats rather than causing direct damage themselves. So this claim is false.

5. If you discover you can access someone else's files by hitting a certain key and you look around briefly, this is hacking.

A. True

B. False

C. It depends on intent

D. Not illegal

Accessing files you're not authorized to view is hacking because it bypasses protective controls and exposes data that should be protected. Even if you discover a way to access and only glance at a few files, the act of viewing those files without permission is unauthorized access. Intent or how briefly you look does not erase the breach. While intent can affect how a situation is treated in practice, the action itself remains hacking. So the statement is true. The idea that it's not illegal ignores the core issue of accessing someone's data without permission, and saying it depends on intent doesn't change the fact that access was gained without authorization.

6. Which term describes a targeted phishing attack aimed at a specific individual?

A. Social engineering

B. Hoax

C. Phishing

D. Spear phishing

Single-target manipulation is the hallmark here. When an attacker crafts a message that seems to come from a trusted colleague or supervisor and uses personal details about a specific person to persuade them to reveal credentials or perform an action, that is spear phishing. The personalization and narrow focus make it more persuasive and harder to detect than generic phishing sent to many people, which is why it's considered a targeted phishing attack. In contrast, broader phishing tries to hit lots of people, social engineering covers the broader tactic of manipulating people rather than specific content, and a hoax is just a false claim or prank not necessarily tied to a targeted credential-braud attempt.

SAMPLE

7. Which of the following are types of countermeasures?

A. Preventative

B. Detective

C. Corrective

D. All Of The Above

Countermeasures in security are controls designed to reduce risk by preventing, detecting, or correcting security incidents. Preventative countermeasures aim to stop threats before they cause harm, such as implementing strong authentication, least-privilege access, timely patch management, secure configurations, and network segmentation. Detective countermeasures focus on finding incidents as they occur or after they happen, with tools like intrusion detection systems, security monitoring, log analysis, and regular audits. Corrective countermeasures come into play after an incident to restore normal operations and minimize impact, including backups and restoration, disaster recovery planning, remediation steps, and incident response procedures. When you combine preventive, detective, and corrective measures, you achieve a more resilient security posture through defense in depth. All of these are valid types of countermeasures, which is why the best choice is that all of the above.

8. _____ is a generic term for "evil software."

A. Virus

B. Worm

C. Malware

D. Threat

Malware is the broad term used for any software designed to cause harm or perform unauthorized actions on a computer. It covers many specific types, including viruses, worms, trojans, ransomware, and spyware. So when the description is "evil software," the umbrella term that fits best is malware. A virus is a particular kind of malware that attaches to files and replicates, while a worm is another type that spreads on its own across networks. A threat, meanwhile, is a broader term referring to potential danger, not the software itself.

9. Which statement best captures the difference between a firewall and an IDS?

A. Firewall controls traffic flow; IDS detects and alerts on suspicious activity.

B. Firewall detects and alerts; IDS controls traffic flow.

C. They perform the same function; no difference.

D. Firewall authenticates users; IDS encrypts data.

The key idea is prevention versus detection. A firewall actively governs traffic between networks by applying rules and blocking or permitting packets, effectively controlling the flow of traffic. An IDS, by contrast, watches for signs of malicious or abnormal activity, analyzes the data, and raises alerts to notify administrators; it doesn't block traffic by itself. If blocking is needed, that's typically handled by a firewall (or an IPS if automatic blocking is integrated). So the statement that describes the firewall as controlling traffic flow and the IDS as detecting and alerting on suspicious activity best captures their distinct roles. In practice there can be overlap on some devices, but the fundamental distinction remains: prevention/control versus detection/notification.

SAMPLE

10. Trade secret theft can occur through interception, hacking, and other traditional cybercrimes.

A. True

B. False

C. Not sure

D. Sometimes

Trade secrets can be stolen through cyber means just as through physical means. In the digital world, confidential information is vulnerable to interception and unauthorized access. Interception occurs when data in transit is captured, such as if traffic is not properly encrypted or is exposed on insecure networks, enabling eavesdropping or tampering. Hacking involves breaking into systems, databases, or cloud storage to exfiltrate sensitive files and designs. Additionally, cybercrime techniques like phishing to obtain credentials, malware or remote access tools to covertly move data, and insider misuse can all lead to theft of trade secrets. Because these cyber methods can and do result in the unauthorized disclosure of confidential information, the statement is true.

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://netsec1.examzify.com

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

SAMPLE