Network Security (NETSEC) 4 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. **A firm can be its own certificate authority for internal users.**

   A. False

   B. Not sure

   C. Depends

   D. True

2. **Which feature is commonly included in a unified threat management (UTM) firewall besides antivirus and spam filtering?**

   A. NAT

   B. SPI

   C. VPN

   D. DDoS protection

3. **An EAP message begins with an _____ message.**

   A. EAP request

   B. EAP accept

   C. EAP start

   D. EAP response

4. **In military security, SBU documents are unclassified.**

   A. True

   B. False

   C. Not defined

   D. Depends

5. **An internal firewall sits at the boundary between the corporate site and the Internet.**

   A. True

   B. False

   C. Sometimes

   D. Not specified

6. Flooding the frequency of a wireless network is one method attackers use to affect the network. True or False?

A. TRUE

B. FALSE

C. Not applicable

D. Indeterminate

7. If you will proxy 8 different applications, you will need _____ proxy programs.

A. 2

B. 4

C. 6

D. 8

8. In Kerberos, which item is sent from the Kerberos server to the verifier?

A. ticket granting ticket

B. service ticket

C. Neither A nor B

D. Both A and B

9. Firewalls do not stop provable attack packets.

A. True

B. False

C. Both

D. Neither

10. Which term describes looking over someone's shoulder to capture a password?

A. Shadowing

B. Trailing

C. Shoulder surfing

D. Piggybacking

Answers

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

Explanations

1. A firm can be its own certificate authority for internal users.

A. False

B. Not sure

C. Depends

D. True

The idea being tested is that an organization can run its own certificate authority to issue and manage certificates for internal users and devices. This is a standard practice in enterprise security: a private PKI lets a firm issue certificates for VPN access, Wi-Fi, email encryption, code signing, and server authentication without relying on public CAs. To make this work, the organization distributes the root certificate of its private CA to all internal clients so they trust certificates issued by that CA. Security best practices include keeping the root CA offline, using a hierarchy with subordinate CAs, protecting private keys, and implementing revocation via CRLs or OCSP. This arrangement gives the organization control over certificate policies, issuance, renewal, and revocation, while reducing reliance on external authorities.

2. Which feature is commonly included in a unified threat management (UTM) firewall besides antivirus and spam filtering?

A. NAT

B. SPI

C. VPN

D. DDoS protection

Unified threat management devices integrate multiple protective functions into a single appliance, and a key capability they rely on is inspecting traffic with awareness of connection state. This stateful packet inspection tracks ongoing sessions and ensures that only packets that belong to valid, established connections are allowed through. That ongoing monitoring gives the firewall context about each packet, helping to block spoofed traffic, unusual connection attempts, and other forms of abuse, which is why it's a staple feature alongside antivirus and anti-spam in UTMs. NAT translates addresses and helps with routing, but it isn't primarily a security inspection feature. VPN support is common on UTMs for providing secure remote access, but it's more about creating encrypted tunnels than inspecting traffic for each packet's legitimacy. DDoS protection is less universally included as a core feature of UTMs, often offered as an optional or higher-end capability. The stateful inspection capability is the one that most directly complements antivirus and spam filtering to improve overall inline security.

3. An EAP message begins with an _____ message.

A. EAP request

B. EAP accept

C. EAP start

D. EAP response

An EAPOL authentication session starts when the supplicant sends an EAP start frame to the authenticator. This Start signal tells the authenticator to begin the EAP negotiation. After this, the authenticator usually issues an EAP-Request (often for identity), and the dialogue continues with EAP-Response messages and further requests until authentication completes. The Start message is the initiating step, whereas requests and responses occur as the exchange progresses; there isn't a defined EAP message called "accept." So the best fit is the EAP start.

4. In military security, SBU documents are unclassified.

A. True

B. False

C. Not defined

D. Depends

SBU stands for Sensitive But Unclassified, a label used for information that isn't assigned a formal classification level like Secret or Top Secret but still needs protection. In military security practice, such documents are considered unclassified in terms of classification, yet they require controlled handling: restricted distribution, proper marking, secure storage, and secure transmission. So the statement is correct because SBU denotes information that is not classified, but must be safeguarded due to its sensitivity. This distinction matters because not all unclassified information can be freely shared; SBU signals that even though there's no formal classification, disclosure could still cause harm and thus should be treated with care. The other options don't fit because the designation exists precisely to denote unclassified but sensitive material, not something undefined or dependent on context, and it's not inaccurate to say it's unclassified.

5. An internal firewall sits at the boundary between the corporate site and the Internet.

A. True

B. False

C. Sometimes

D. Not specified

Firewalls are placed based on their role in network protection. The boundary between the corporate network and the Internet is typically secured by a perimeter (edge) firewall, which controls traffic entering and leaving the trusted network. An internal firewall, on the other hand, sits inside the network to segment internal zones (for example, between departments or between a DMZ and the core network) and to enforce policies within the organization. While you can have multiple layers of defense, the device at the border to the Internet is usually a perimeter firewall, not an internal one. So the statement is false.

6. Flooding the frequency of a wireless network is one method attackers use to affect the network. True or False?

A. TRUE

B. FALSE

C. Not applicable

D. Indeterminate

In wireless networks, flooding the channel with noise or frames is a denial-of-service tactic. By saturating the airwaves or occupying the channel with excessive traffic, legitimate transmissions struggle to get through. Devices back off more often, collisions rise, throughput drops, and connections can be dropped, which directly harms availability. This is a well-known way attackers disrupt wireless networks, such as through jamming or deauthentication floods, making the statement true. While other threats target confidentiality or integrity, flooding the frequency specifically undermines access to the network.

7. If you will proxy 8 different applications, you will need _____ proxy programs.

A. 2

B. 4

C. 6

D. 8

Each application's traffic is typically routed through a dedicated proxy instance. Running a separate proxy program for each app provides isolation and allows you to customize filtering, logging, and access controls per app. Therefore, to proxy eight different applications, you would deploy eight proxy programs—one for each application. In practice, you could route multiple apps through one proxy by configuring separate rules, but the straightforward approach given here is eight separate proxies.

8. In Kerberos, which item is sent from the Kerberos server to the verifier?

A. ticket granting ticket

B. service ticket

C. Neither A nor B

D. Both A and B

In Kerberos, tickets are issued by the Key Distribution Center and then carried by the client, not pushed directly to the service (verifier). The client first obtains a Ticket-Granting Ticket, and later a service ticket for the requested service. That service ticket is sent to the client by the KDC, and the client then presents it to the verifier. The verifier does not receive either a TGT or a service ticket directly from the Kerberos server; it only receives the service ticket from the client as part of the authentication handshake.

9. Firewalls do not stop provable attack packets.

A. True

B. False

C. Both

D. Neither

Firewalls enforce access control by inspecting traffic and dropping packets that match rules or known threat signatures. When a packet aligns with a configured rule—such as an exploit signature, a forbidden port, or unusual connection patterns—the firewall can stop it before it reaches its destination. This is a core defense role: filtering out provable attack attempts based on policy and signatures, especially with stateful inspection and IPS features. Of course, there are limitations: encrypted payloads can hide malicious content from inspection, new or obfuscated attacks may not be covered by existing signatures, and misconfigurations can allow harmful traffic through. Still, the idea that firewalls do not stop provable attack packets is not correct; they do block such packets when they match the protections in place.

10. Which term describes looking over someone's shoulder to capture a password?

A. Shadowing

B. Trailing

C. Shoulder surfing

D. Piggybacking

Observing someone enter a password by looking over their shoulder is called shoulder surfing. It's a direct observation of credentials being entered or displayed, often in public or shared spaces, and the attacker relies on visibility rather than breaking in or stealing devices. This term precisely captures the act of watching someone type a password to capture it. The other terms describe different behaviors: shadowing or trailing implies following someone over time rather than specifically watching password input, and piggybacking refers to gaining physical access by accompanying someone through a secured entry, not observing credentials.

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://netsec4.examzify.com

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