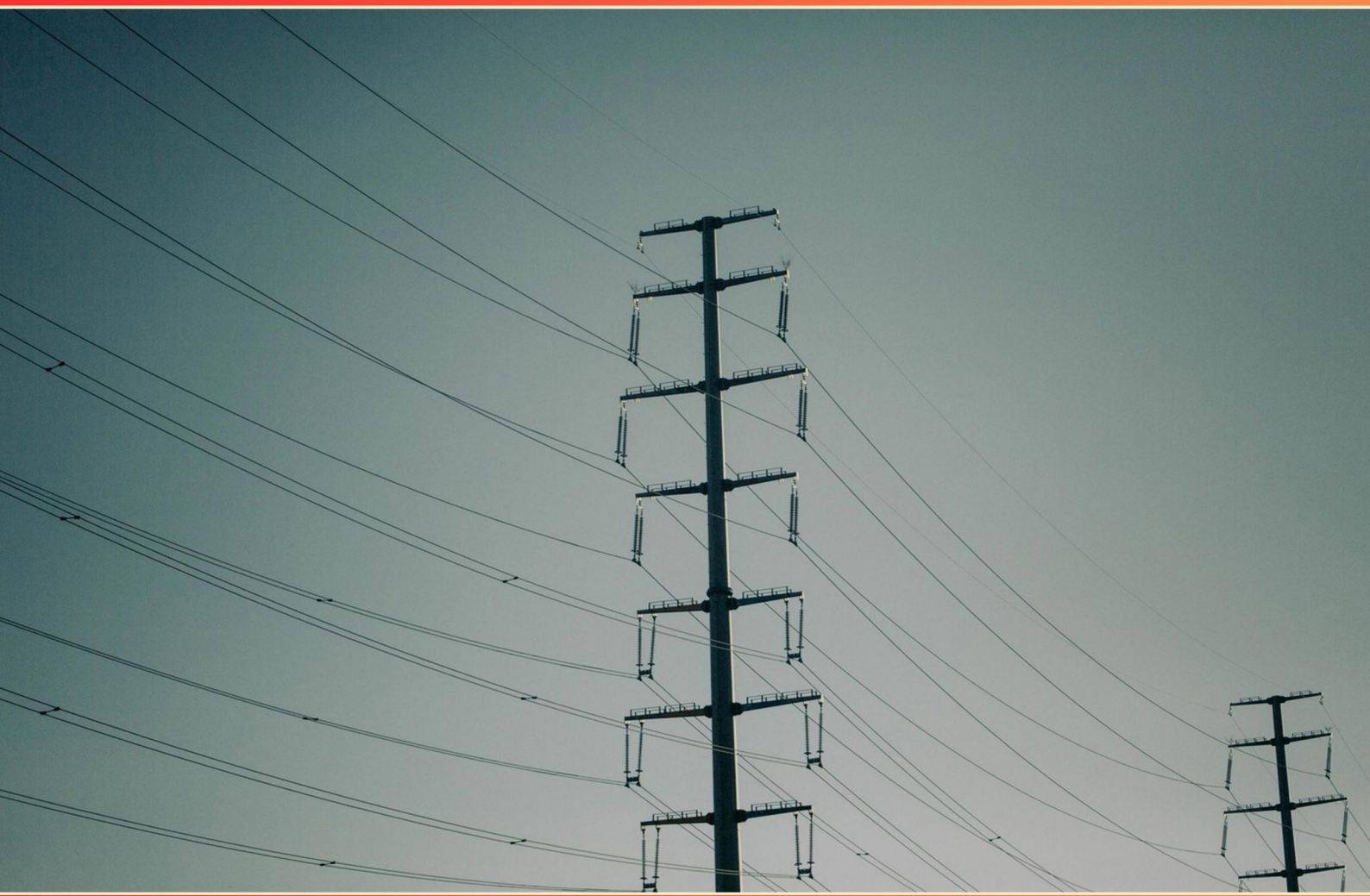
KHAN ACADEMY THE INTERNET PRACTICE TEST (SAMPLE)

STUDY GUIDE



SAMPLE STUDY GUIDE WITH LIMITED QUESTIONS

VISIT US ONLINE FOR THE FULL VERSION STUDY GUIDE

https://khanacademytheinternet.examzify.com

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 purpose of a CDN for a global audience?

A. It reduces latency by serving content from servers closer to users, improving load times.

B. It increases the size of the origin server.

C. It eliminates the need for DNS resolution.

D. It forces all users to download content from a single server.

2. Which of the following is the correct unit for upload speed?

A. 50 MBps

B. 50 Mbps

C. 50 GBps

D. 50 KBps

3. What information does a typical data packet contain?

A. A header with routing information and a payload with the actual data.

B. Only the payload with no header.

C. A list of connected devices.

D. The password for the receiving site.

4. What does a 200 status code indicate?

A. The request was successful and the server returned the requested resource.

B. The resource was not found on the server.

C. The server encountered an error while processing the request.

D. The request was redirected to a different URL.

5. Which threat involves redirecting users to fake sites by tampering with DNS or hosts files?

A. Pharming

B. Phishing

C. Malware

D. Social engineering

6. How can you identify trustworthy websites?

A. HTTP only, no certificate, no privacy policy.

B. HTTPS, a valid site certificate, a reputable domain, privacy policies, and credible contact information.

C. Any site with pop-up ads.

D. Sites with questionable contact info.

7. Why does each IP packet contain a sequence number?

A. To determine the original order of the packets.

B. To identify the sender's device.

C. To indicate the total number of packets in the transmission.

D. To encrypt the payload.

8. For the described three-step symmetric encryption (in-word letter swap, A/E swap, then a Caesar shift of 14), what would be the best key to explain the method to a friend?

A. The original plaintext before encryption.

B. A random number used to seed the random generator.

C. A diagram of Caesar shift by 7.

D. A 3-step explanation of how he encrypted the message (the in-word letter swap, the A and E swap, and the Caesar shift of 14).

9. What does HTTP stand for?

A. Hyperlink Transport Protocol.

B. Hypertext Transfer Protocol and Secure.

C. Hypertext Transfer Procedure.

D. Hypertext Transfer Protocol.

10. What is a digital certificate and who issues it?

A. It binds a public key to a domain and is issued by a Certificate Authority.

B. It certifies a user's identity in a social network and is issued by the platform.

C. It encrypts emails end-to-end and does not require an issuer.

D. It stores passwords securely in the browser.

Answers

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

Explanations

1. What is the main purpose of a CDN for a global audience?

A. It reduces latency by serving content from servers closer to users, improving load times.

B. It increases the size of the origin server.

C. It eliminates the need for DNS resolution.

D. It forces all users to download content from a single server.

A CDN works by bringing content closer to users to speed things up. It places copies of your static resources on many servers around the world, so when someone in another country requests a page, the CDN serves from the closest server. That shortens the distance data has to travel, reduces the number of network hops, and lowers the time it takes for the page to start loading. This leads to faster load times and a better user experience for people worldwide. A CDN also helps by taking some of the load off the origin server, especially during traffic spikes, and it can improve reliability. It doesn't increase the size of the origin server; in fact, it reduces direct requests to it. DNS resolution is still used to locate the nearest edge server, not eliminated. And it doesn't force everyone to download from a single server—they're distributed across many edge locations.

2. Which of the following is the correct unit for upload speed?

A. 50 MBps

B. 50 Mbps

C. 50 GBps

D. 50 KBps

When we talk about internet upload speeds, the rate is measured in bits per second, not bytes per second. The standard unit for consumer speeds is megabits per second, abbreviated Mbps. So 50 Mbps means 50 million bits transmitted every second, which is how internet providers describe upload (and download) speeds. Other units would describe data in bytes per second. Megabytes per second (MBps) is eight times larger than Mbps, since 1 byte equals 8 bits, so 50 MBps would be 400 Mbps in the same scale. Gigabytes per second (GBps) would be far faster than typical home internet, and kilobytes per second (KBps) is a much slower rate. Because upload speed is conventionally expressed in megabits per second, the correct choice is the unit Mbps.

3. What information does a typical data packet contain?

A. A header with routing information and a payload with the actual data.

B. Only the payload with no header.

C. A list of connected devices.

D. The password for the receiving site.

Data is sent over networks in small chunks called packets, and each packet carries two main parts: a header and a payload. The header holds routing and control information that helps the network move the packet from the sender to the correct recipient, including addresses, sequencing data, and error-checking fields. The payload is the actual data you want to deliver, like part of a file or a piece of a web page. Without a header, routers wouldn't know where to send the packet or how to reassemble the message, and without a payload there would be no useful data to deliver. Choices that suggest only the data or that include unrelated items (like a list of devices or a password) don't describe how standard packets are structured.

4. What does a 200 status code indicate?

A. The request was successful and the server returned the requested resource.

B. The resource was not found on the server.

C. The server encountered an error while processing the request.

D. The request was redirected to a different URL.

A 200 status code means the request was successful and the server returned the requested resource. This signals that everything went through as intended and you can expect the response body to contain the data you asked for. It's part of the 2xx family that covers successful responses; 200 is the most common form when you fetch something, like a web page or data. Sometimes a request is successful but doesn't need to return content, in which case you might see a 204 No Content. Other status codes describe different outcomes: 404 indicates the resource isn't found; 5xx codes mean the server ran into an error; 3xx codes indicate a redirect to another URL.

5. Which threat involves redirecting users to fake sites by tampering with DNS or hosts files?

A. Pharming

B. Phishing

C. Malware

D. Social engineering

Pharming is the tactic of redirecting you to fraudulent websites by tampering with how domain names are resolved. Attackers can alter DNS records or modify the host file on your computer so that a legitimate URL resolves to an attacker controlled IP address. Even if you type the correct address or click a normal link, you'll end up at a fake site, which can steal credentials or deliver malware. This network- or machine-level redirection is unique to pharming. Phishing relies on tricking you into visiting a malicious site via deceptive messages, malware is software that causes harm, and social engineering is the broader manipulation of people to reveal information or take action. The described scenario matches pharming because it centers on redirecting users through DNS or hosts-file changes.

6. How can you identify trustworthy websites?

A. HTTP only, no certificate, no privacy policy.

B. HTTPS, a valid site certificate, a reputable domain, privacy policies, and credible contact information.

C. Any site with pop-up ads.

D. Sites with questionable contact info.

Identifying trustworthy websites comes down to signals that show both secure connections and responsible handling of your information. A site that uses HTTPS with a valid certificate helps protect any data you send or receive by encrypting it, and you can usually see this as a padlock icon in the address bar. But encryption alone isn't enough—it's important that the certificate is valid and issued by a trusted authority, and that the domain name matches the organization behind the site. Beyond security, trustworthy sites provide clear, accessible information about how they handle your data. A privacy policy explains what data is collected, how it's used, and who it's shared with. Credible contact information, such as a real physical address and a working phone number or customer support channel, shows accountability and gives you a way to reach the organization. So the best choice combines these signals: a secure HTTPS connection with a valid site certificate, a reputable domain, a transparent privacy policy, and credible contact details. The other options miss one or more of these important trust signals—such as relying on a site with no encryption, or sites that have misleading or absent contact information.

7. Why does each IP packet contain a sequence number?

A. To determine the original order of the packets.

B. To identify the sender's device.

C. To indicate the total number of packets in the transmission.

D. To encrypt the payload.

The idea being tested is how data that's split into packets can be put back together correctly. Packets may take different routes and arrive at different times, so the numbers that label each piece of data let the recipient place the bytes in the original order and notice if any piece is missing. That way the whole message can be reconstructed reliably, even if packets don't arrive in sequence. It's not about identifying the sender's device—that's handled by the address information. It's not about indicating how many packets were sent—the receiver doesn't rely on a total count to reassemble. And it's not about encryption—the sequence helps with order, not with encrypting the payload.

8. For the described three-step symmetric encryption (in-word letter swap, A/E swap, then a Caesar shift of 14), what would be the best key to explain the method to a friend?

A. The original plaintext before encryption.

B. A random number used to seed the random generator.

C. A diagram of Caesar shift by 7.

D. A 3-step explanation of how he encrypted the message (the in-word letter swap, the A and E swap, and the Caesar shift of 14).

A good key for explaining this encryption is a clear, three-step description of the method—covering the in-word letter swap, the A/E swap, and the Caesar shift by 14—so your friend can reproduce it. This kind of explanation directly conveys how to apply the system, which is what a key should do: it describes how the encryption is performed, not just what one part looks like. Revealing the original plaintext isn't a key at all because it exposes the message instead of teaching the method. A random seed is an implementation detail that doesn't describe the steps themselves, so it doesn't help someone understand how to encrypt and decrypt. A diagram of a Caesar shift by 7 gives only a single piece and even uses the wrong shift amount, so it wouldn't accurately convey the full three-step process. Describing the exact sequence of steps and the specific shift makes the method understandable and reproducible.

9. What does HTTP stand for?

A. Hyperlink Transport Protocol.

B. Hypertext Transfer Protocol and Secure.

C. Hypertext Transfer Procedure.

D. Hypertext Transfer Protocol.

HTTP stands for Hypertext Transfer Protocol. It is the set of rules that governs how a browser and a server communicate to fetch and display web pages. "Hypertext" refers to linked documents, "Transfer" describes moving data between your computer and the server, and "Protocol" means a defined method of communication. The other options mix up terms (Hyperlink instead of Hypertext, Transport vs Transfer, and including "Secure" which would point to HTTPS) or use the word "Procedure," which isn't the correct term for this standard. So the exact and standard name is Hypertext Transfer Protocol.

10. What is a digital certificate and who issues it?

A. It binds a public key to a domain and is issued by a Certificate Authority.

B. It certifies a user's identity in a social network and is issued by the platform.

C. It encrypts emails end-to-end and does not require an issuer.

D. It stores passwords securely in the browser.

Digital certificates are part of how the internet proves who a site or entity is. A certificate binds a public key to an identity (such as a domain) and is issued by a trusted Certificate Authority. The CA verifies the entity, signs the certificate with its private key, and publishes it so others can check the signature against the CA's public key. When you visit a site, your browser uses this certificate to confirm the domain matches and to establish an encrypted TLS connection, trusting the certificate because it chains back to a trusted CA. This is why the description that says it binds a public key to a domain and is issued by a Certificate Authority is the best answer. The other descriptions describe different concepts (social identity on a platform, end-to-end encryption without an issuer, or browser-stored passwords) and don't capture what a digital certificate actually is.

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://khanacademytheinternet.examzify.com

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