Wireshark Traffic Analysis Practice Exam (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. Which option is a protocol suite that provides end-to-end encryption for web traffic?

A. SSH

B. HTTPS/TLS encryption

C. Tor

D. IPsec VPN

2. Which of the following can you see in TLS encrypted traffic?

A. IP addresses, domains (SNI), and packet sizes

B. Payload data

C. Certificates

D. User credentials

3. To decrypt TLS traffic in Wireshark, which input is required?

A. You must install a decryption plugin

B. You must use the server's private key

C. You must provide the appropriate keys via SSLKEYLOGFILE or pre-master secret

D. TLS cannot be decrypted

4. When must keys be captured?

A. During the session

B. Before handshake

C. After the session

D. At the start of capture

5. In the client-side steps of the handshake, which method finalizes the connection after receiving a SYN/ACK?

A. The client ends the handshake by sending a FIN

B. The client ends the handshake by sending an ACK after receiving a SYN/ACK

C. The client ends the handshake by sending a SYN

D. The client ends the handshake by sending a RST

6. Which factor makes DNS attractive for abuse?

A. It is encrypted by default.

B. It is trusted and rarely blocked.

C. It never uses subdomains.

D. It requires VPN to access.

7. What is NBNS used for?

A. Resolving hostnames in local networks.

B. Resolving domain names on the public internet.

C. Mapping MAC addresses to IPs.

D. Resolving hostnames using DNS.

8. Which statement about ICMP is true?

A. It is not used for reachability checks.

B. It is never trusted by networks.

C. It is only used on IPv6.

D. It is often trusted and allowed through firewalls.

9. Which approach filters the capture to TLS handshake messages?

A. Use a TLS/SSL filter such as tls and then inspect handshake-related messages

B. Filter by http and then TLS handshake messages

C. Filter by tcp.port == 443 only

D. Use dns filter

10. Which technique enables MITM?

A. ARP spoofing

B. DNS spoofing

C. IP spoofing

D. Port scanning

Answers

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

Explanations

1. Which option is a protocol suite that provides end-to-end encryption for web traffic?

A. SSH

B. HTTPS/TLS encryption

C. Tor

D. IPsec VPN

End-to-end protection for web traffic comes from using TLS within HTTPS. When a browser connects to a website over HTTPS, TLS authenticates the server with a certificate, negotiates a session key, and then uses that key to encrypt all the data exchanged. This means the content stays confidential and intact from your device to the server, and the server can be verified as legitimate. Other options serve different purposes. SSH is aimed at secure remote access and file transfers, not typical web-page traffic. Tor focuses on anonymity by routing traffic through multiple relays, which may hide who you are but isn't the standard end-to-end encryption for a web request unless TLS is also used. IPsec VPN encrypts at the network level for the connection between endpoints, not specifically the web traffic inside a browser session. So, HTTPS/TLS encryption is the protocol suite that provides end-to-end encryption for web traffic.

2. Which of the following can you see in TLS encrypted traffic?

A. IP addresses, domains (SNI), and packet sizes

B. Payload data

C. Certificates

D. User credentials

In TLS, the payload you send and receive is encrypted, but some surrounding information stays visible. You can observe the IP addresses involved in the connection (source and destination) and the sizes of the TLS records that are sent, even though you can't read the actual application data inside those records. The server name requested by the client is typically carried in the SNI field of the ClientHello and is sent in the clear, so observers can often see which domain is being contacted. Packet or record sizes give you an idea of how much data is being exchanged without revealing the content. The actual application data isn't readable, and user credentials in the application layer aren't exposed in the encrypted stream. Certificates are exchanged as part of the handshake, but that exchange isn't the encrypted application data, so it's not what's meant by "TLS encrypted traffic" in this context. Therefore, the elements that are visible are the IPs, the domain via SNI, and the TLS record sizes, matching the best answer.

3. To decrypt TLS traffic in Wireshark, which input is required?

A. You must install a decryption plugin

B. You must use the server's private key

C. You must provide the appropriate keys via SSLKEYLOGFILE or pre-master secret

D. TLS cannot be decrypted

Decrypting TLS in Wireshark requires access to the session keys that were used to encrypt the data. In practice, you provide these keys from the client side—typically as the pre-master secret or the derived session keys—so Wireshark can reconstruct the encryption keys and decrypt the traffic. This is usually done by supplying a key log (such as SSLKEYLOGFILE) that logs the pre-master secret for each TLS session, or by otherwise providing the pre-master secret to Wireshark. Merely using the server's private key isn't sufficient in most modern TLS connections because of forward secrecy (ephemeral key exchange). Without the correct keys, the traffic remains encrypted, and decrypting isn't possible.

4. When must keys be captured?

A. During the session

B. Before handshake

C. After the session

D. At the start of capture

Keys used to decrypt TLS traffic are created during the TLS handshake and are then used for the rest of that session. The session keys (including the secret material derived in the handshake) are what unlock each record in the captured data. Because these keys are produced as part of establishing the session, you need to obtain or export them while the handshake is happening so they can be applied to the subsequent traffic. If you try to provide them before the handshake, they don't exist yet; if you try to decrypt data from a session after the handshake without having captured the keys, the data remains unreadable. In practice, you enable a key export or TLS key log during the handshake, and then load those keys into Wireshark so it can decrypt the traffic from that session. Therefore, the keys must be captured during the session.

5. In the client-side steps of the handshake, which method finalizes the connection after receiving a SYN/ACK?

A. The client ends the handshake by sending a FIN

B. The client ends the handshake by sending an ACK after receiving a SYN/ACK

C. The client ends the handshake by sending a SYN

D. The client ends the handshake by sending a RST

TCP connections are established using a three-way handshake. After the client receives the server's SYN-ACK, the final step is for the client to send an ACK. This ACK confirms receipt of the server's response (acknowledging the server's sequence number) and completes the handshake, allowing data transfer to begin. Sending a FIN would terminate an existing connection, not finalize a new one. Sending another SYN would be out of place—it's effectively trying to start a new connection before finishing the current one. Sending a RST would abruptly reset the connection rather than completing the setup.

6. Which factor makes DNS attractive for abuse?

A. It is encrypted by default.

B. It is trusted and rarely blocked.

C. It never uses subdomains.

D. It requires VPN to access.

DNS is attractive for abuse because it is trusted and rarely blocked. It underpins almost all Internet activity, so security controls typically allow DNS traffic to pass; blocking it would disrupt normal services. That permissiveness lets malicious actors use DNS for hosting, command-and-control, or data exfiltration while blending in with legitimate domain lookups, making it a low-friction channel for abuse.

7. What is NBNS used for?

A. Resolving hostnames in local networks.

B. Resolving domain names on the public internet.

C. Mapping MAC addresses to IPs.

D. Resolving hostnames using DNS.

NBNS is used to resolve NetBIOS names to IP addresses within a local network. This lets Windows machines find each other by NetBIOS names (for example, a computer named SERVER or WORKSTATION) on the LAN, enabling NetBIOS-based services like file sharing. It operates as part of NetBIOS over TCP/IP and typically uses UDP port 137. This is different from DNS, which resolves domain names on the public Internet, and from ARP, which maps MAC addresses to IPs.

8. Which statement about ICMP is true?

A. It is not used for reachability checks.

B. It is never trusted by networks.

C. It is only used on IPv6.

D. It is often trusted and allowed through firewalls.

ICMP exists to provide feedback about the delivery of IP packets, including reachability and error information. Because networks rely on these signals for diagnostics and for functions like path MTU discovery, many operators configure firewalls to allow some ICMP traffic to pass. This is why the statement that ICMP is often trusted and allowed through firewalls is accurate: you typically see rules that permit essential ICMP types (like Echo Request/Reply and certain error messages) while still using rate limiting or type-based filtering to reduce abuse. Understanding the other options helps solidify this: ICMP is indeed used for reachability checks (ping is the classic example), so saying it's not used for reachability checks is false. ICMP is not IPv6-only; it exists in IPv4 as well (with ICMPv4) and remains a vital part of IPv6 (ICMPv6) too, so claiming it's exclusive to IPv6 is incorrect. While some networks may block ICMP for security, in practice it's often tolerated or selectively allowed to preserve troubleshooting capabilities and proper network operation.

9. Which approach filters the capture to TLS handshake messages?

A. Use a TLS/SSL filter such as tls and then inspect handshake-related messages

B. Filter by http and then TLS handshake messages

C. Filter by tcp.port == 443 only

D. Use dns filter

TLS handshake messages are the set of messages that establish a secure session within the TLS protocol. To study them, start by filtering for TLS traffic so you only see TLS records, then zero in on the handshake messages themselves. In Wireshark, you can narrow further with a handshake-specific filter (for example, tls.handshake) to display only the handshake messages like ClientHello, ServerHello, Certificate, and so on. Filtering by HTTP won't catch the TLS handshake, since the HTTP layer comes after the handshake, and filtering by a port like 443 is not precise to handshake content and can include other TLS records or miss nonstandard cases. DNS is unrelated to TLS handshakes. So, applying a TLS filter first and then inspecting the handshake messages is the direct, precise approach.

10. Which technique enables MITM?

A. ARP spoofing

B. DNS spoofing

C. IP spoofing

D. Port scanning

Man-in-the-middle on a local network is achieved by making traffic pass through the attacker’s device. ARP spoofing does this by poisoning ARP caches: a attacker sends forged ARP replies so that the victim and/or the gateway associate the attacker’s MAC address with the other device’s IP. As a result, traffic meant for the gateway (or the other host) is sent to the attacker, who can sniff or modify it before forwarding it on. While DNS spoofing can redirect a host to a malicious server and IP spoofing can impersonate another device, neither by itself reliably places the attacker in the middle of traffic on the LAN, and port scanning has no role in intercepting traffic. So the technique that directly enables MITM in this context is ARP spoofing.

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://wiresharttrafficanalysis.examzify.com

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