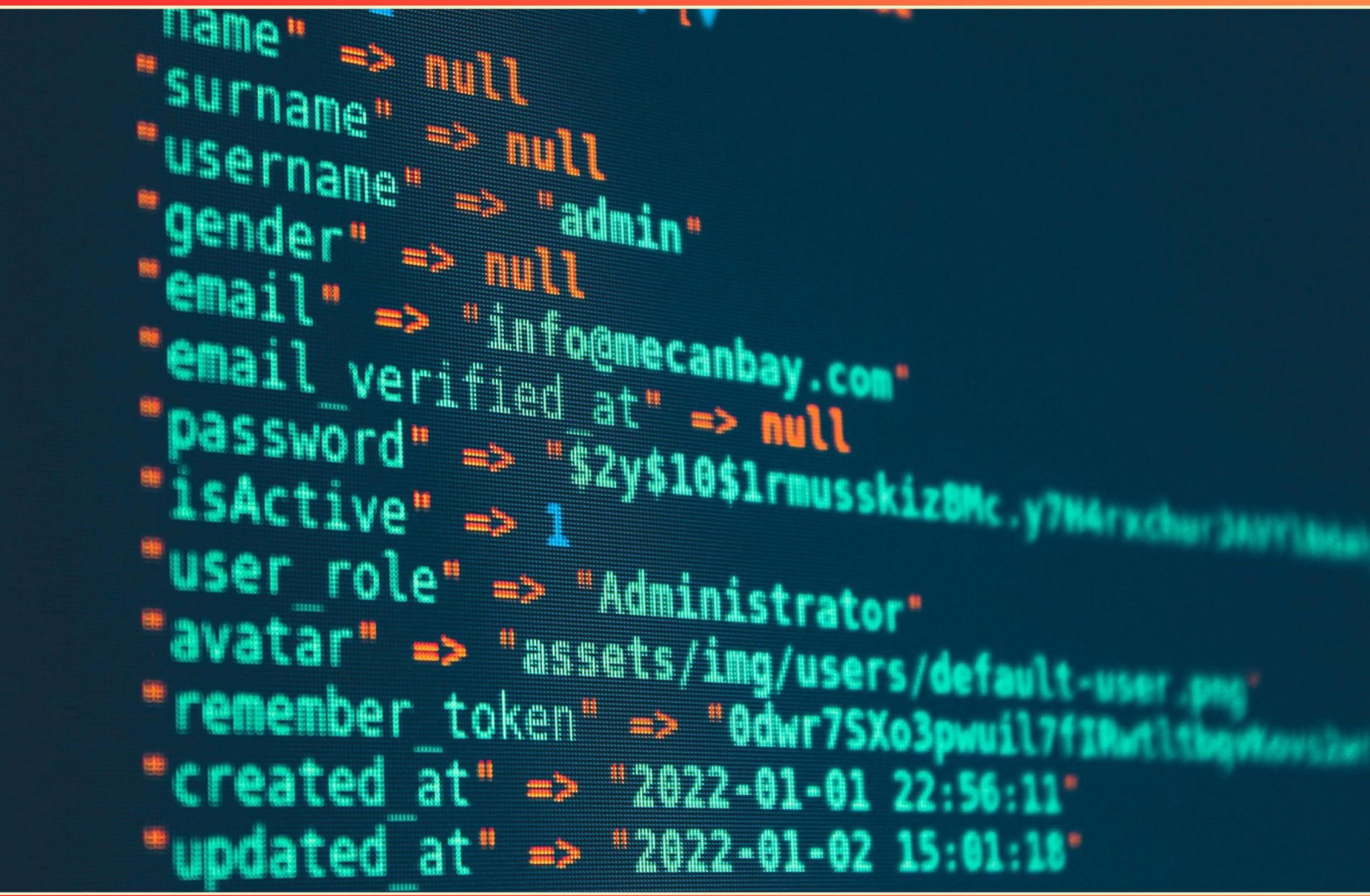
ELEARNSECURITY JUNIOR PENETRATION TESTER (EJPT) CLASS PRACTICE EXAM (SAMPLE)

STUDY GUIDE



SAMPLE STUDY GUIDE WITH LIMITED QUESTIONS

VISIT US ONLINE FOR THE FULL VERSION STUDY GUIDE

https://ejptclass.examzify.com

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

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 statement best describes IDS signatures?

A. Signatures enable detection of known threats; without them, detection may fail

B. Signatures eliminate all false positives

C. Signatures are used to encrypt traffic

D. Signatures make IDS immune to tampering

2. What does HTTP status code 301 Moved Permanently indicate?

A. Resource is found at a new permanent URI

B. Resource is temporarily under another URI

C. Client does not have privileges

D. Server error

3. In promiscuous mode, which statement best describes the NIC's behavior?

A. Discard only packets addressed to this NIC.

B. Discard any packet addressed to another NIC.

C. Accept and process every packet it receives.

D. Filter packets by protocol and port.

4. What does HTTP status code 403 Forbidden indicate?

A. Resource not found

B. Client does not have enough privileges

C. Resource is temporarily unavailable

D. Server encountered an error

5. What does the payload of a packet represent?

A. The actual information

B. The header

C. The encoding

D. The metadata

6. Which layer is responsible for transporting data between processes (server and client programs)?

A. Application layer

B. Network layer

C. Physical layer

D. Transport layer

7. Which header fields participate in the TCP three-way handshake?

A. Sequence number, Acknowledgement numbers, SYN/ACK flags

B. Source IP address, Destination IP address, TTL

C. Window size, Checksum, URG flag

D. Options field

8. TTL in networking stands for what?

A. Time to Live

B. Time to Link

C. Total Time Latency

D. Transmission Time Limit

9. What is the primary purpose of port scanning in a penetration test?

A. To identify open ports and services, determine attack surfaces, and map network topology.

B. To exploit vulnerabilities directly.

C. To erase logs.

D. To encrypt traffic.

10. What is SQL injection and why is it important for web app testing?

A. SQL injection is a defense mechanism.

B. SQL injection is input manipulation to execute malicious SQL, enabling data access or modification; critical to test for data leakage.

C. SQL injection is a technique to bypass FTP.

D. SQL injection is about injecting HTML into SQL.

Answers

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

Explanations

1. Which statement best describes IDS signatures?

A. Signatures enable detection of known threats; without them, detection may fail

B. Signatures eliminate all false positives

C. Signatures are used to encrypt traffic

D. Signatures make IDS immune to tampering

Signatures in an IDS are predefined patterns that match known malicious activity. This is what allows the system to recognize and alert on known threats: if the traffic or payload fits one of the signatures, an alert is triggered. Without these patterns, the IDS would lack specific indicators to identify those attacks, so detection of known techniques could fail. Think of signatures as a catalog of known bad behaviors—the exact payload strings, sequence of bytes, or protocol abuses that have been observed before. They're essential for fast, accurate detection of those known threats, but they're not a magic shield against everything. They require regular updates to cover new exploits, and they don't catch novel, unknown attacks. They can also produce false positives when legitimate activity matches a signature, and they do not provide encryption or tamper-proofing for the IDS itself.

2. What does HTTP status code 301 Moved Permanently indicate?

A. Resource is found at a new permanent URI

B. Resource is temporarily under another URI

C. Client does not have privileges

D. Server error

A 301 Moved Permanently tells you the resource has a new permanent URI. The server responds with the new URL in the Location header, and clients should use that address for all future requests. Caches and search engines will update to the new location, treating this as a long-term change. This is different from temporary redirects, which indicate the move isn't permanent, and from error or access-denied responses. So the best description is that the resource is found at a new permanent URI.

3. In promiscuous mode, which statement best describes the NIC's behavior?

A. Discard only packets addressed to this NIC.

B. Discard any packet addressed to another NIC.

C. Accept and process every packet it receives.

D. Filter packets by protocol and port.

Promiscuous mode removes the NIC's usual destination-based filtering, so the adapter passes all frames it sees up to the host rather than discarding those not addressed to it. This allows packet sniffers to capture traffic not intended for this machine. Because of this behavior, the NIC effectively accepts and processes every packet it receives. The other statements describe normal filtering or selective processing, which is not what promiscuous mode does.

4. What does HTTP status code 403 Forbidden indicate?

A. Resource not found

B. Client does not have enough privileges

C. Resource is temporarily unavailable

D. Server encountered an error

HTTP status code 403 Forbidden means the server understood the request but refuses to authorize access due to insufficient permissions. Even if your credentials are valid, the action or resource is not allowed for your account or context. It's about authorization rules, not about the resource being missing or the server being down. This differs from a 401, which signals authentication is required or has failed. In practice, you'd see this when trying to reach an admin-only page, a restricted file, or an API endpoint your user role isn't allowed to access. To resolve, you'd need the appropriate privileges or an ACL/permission change from an administrator.

5. What does the payload of a packet represent?

A. The actual information

B. The header

C. The encoding

D. The metadata

The payload is the actual information carried by the packet. In networking, a packet has a header and a data portion. The header holds addressing and control information—source and destination addresses, protocol, sequencing, and similar fields—to route and deliver the packet. The payload is the part that carries the user or application data—the content the sender wants the receiver to process. Encoding refers to how bits are represented or transformed for transmission (such as encryption) and isn't the payload itself. Metadata is supplementary information about the data, not the data itself. So, the payload represents the actual information being transmitted, such as an HTTP request/response or the contents of a file.

6. Which layer is responsible for transporting data between processes (server and client programs)?

A. Application layer

B. Network layer

C. Physical layer

D. Transport layer

End-to-end communication between processes on different machines is handled by the transport layer. It uses port numbers to multiplex multiple conversations on a single host and ensures data is delivered to the correct process on the remote end. The transport layer can provide reliable, connection-oriented delivery (as with TCP) or lightweight, best-effort delivery (as with UDP), handling segmentation, reassembly, error detection, and flow control. The network layer is responsible for routing packets between hosts, the application layer defines the actual data and protocols used by programs, and the physical layer deals with the hardware signaling. In a server–client interaction, the transport layer ensures the data from a client process reaches the intended server process via the appropriate port, making it the layer that transports data between processes.

7. Which header fields participate in the TCP three-way handshake?

A. Sequence number, Acknowledgement numbers, SYN/ACK flags

B. Source IP address, Destination IP address, TTL

C. Window size, Checksum, URG flag

D. Options field

The key idea is that the TCP three-way handshake uses specific header information to establish and synchronize a connection. The essential elements are the sequence number, the acknowledgment number, and the flags that indicate SYN and ACK. In the first segment, the client starts the connection by sending a request with its initial sequence number and the SYN flag set. The server replies with a segment that has both the SYN and ACK flags set, uses its own initial sequence number, and acknowledges the client's SYN by setting the acknowledgment number to the client's ISN plus one. Finally, the client sends a final segment with the ACK flag set, acknowledging the server's ISN plus one, and the connection is established. Other header fields, like the source and destination IP addresses or TTL, belong to other layers or are always present in all TCP segments but aren't specific to performing the handshake. The window size and checksum are important for data transfer and integrity in all segments, not just the handshake, and the options field may carry optional parameters but is not essential to establishing the connection.

8. TTL in networking stands for what?

A. Time to Live

B. Time to Link

C. Total Time Latency

D. Transmission Time Limit

TTL stands for Time to Live. It is a field in the IP header that acts as a hop limit to prevent packets from looping forever. Each router that forwards the packet decreases this value by one; when it reaches zero, the packet is discarded and often an ICMP Time Exceeded message is sent back to the sender. This mechanism keeps networks from wasting bandwidth on misrouted or looping traffic. While the name suggests elapsed time, in practice TTL is a count of hops, not an exact time measurement. (Note: TTL is also used in DNS with a related but separate meaning—the caching duration for a DNS record—but that is a different context.)

9. What is the primary purpose of port scanning in a penetration test?

A. To identify open ports and services, determine attack surfaces, and map network topology.

B. To exploit vulnerabilities directly.

C. To erase logs.

D. To encrypt traffic.

Port scanning is all about uncovering what is exposed on a network. It helps you identify which ports are open on target systems, what services are listening on those ports, and by doing so, you map out the attack surface and the overall network topology. This information is essential for planning a penetration test because it shows where an attacker could potentially gain access and which hosts and services to study further. Exploitation is a later step that uses found vulnerabilities to gain access, not the discovery itself. Erasing logs is about evading detection and is not part of identifying entry points. Encrypting traffic is about protecting data in transit, not about discovering exposed services.

10. What is SQL injection and why is it important for web app testing?

A. SQL injection is a defense mechanism.

B. SQL injection is input manipulation to execute malicious SQL, enabling data access or modification; critical to test for data leakage.

C. SQL injection is a technique to bypass FTP.

D. SQL injection is about injecting HTML into SQL.

SQL injection happens when an application builds SQL queries using input from users without treating that input as data. By injecting specially crafted input into forms, query strings, or parameters, an attacker can alter the logic of the SQL being executed, potentially retrieving, modifying, or deleting data, or even bypassing authentication. This matters for web app testing because it directly affects the integrity and confidentiality of the database. A tester looks for places where input is interpolated into SQL and verifies that queries are parameterized or properly escaped, that inputs are validated, and that the application uses least-privilege database accounts. Typical tests try inputs that would alter the query's meaning, to see if the app leaks data or grants access incorrectly; successful prevention hinges on using prepared statements, parameterized queries, and robust input handling. Other options don't fit because this vulnerability is not a defense mechanism, not related to bypassing FTP, and not about injecting HTML into SQL.

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://ejptclass.examzify.com

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