eLearnSecurity Junior Penetration Tester (eJPT) Class Practice Exam (Sample)

Study Guide

Everything you need from our exam experts!

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 **16**

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 of the following could be payload data in a packet?

A. The packet header

B. The checksum

C. The electrical signal

D. Part of an email message

2. Give an example of a Linux privilege escalation vector commonly checked during pentests.

A. Using password spraying to gain root access.

B. Exploiting cron jobs to escalate privileges.

C. Enumerating kernel modules for privilege escalation.

D. Listing and examining SUID binaries for misconfigurations that could grant elevated privileges.

3. Which statement best captures the primary distinction between authenticated and unauthenticated scanning?

A. Authenticated scans reveal internal exposure by using valid credentials; unauthenticated scans test from an external perspective without credentials.

B. Authenticated scans are always faster than unauthenticated scans.

C. Unauthenticated scans require root access.

D. Authenticated scans test only DNS configuration.

4. IP:Port pair is used to identify a single network process on a machine. Which component forms the IP:Port pair?

A. IP address

B. Subnet mask

C. Gateway

D. Port

5. On Linux, which command can be used to view the neighboring hardware address table (ARP cache)?

A. ip neighbour

B. arp -a

C. ifconfig

D. ip addr

6. HTTPS is HTTP delivered over which cryptographic protocol?

A. TLS/SSL

B. SSH

C. IPsec

D. S/MIME

7. Which is a best practice for logging and evidence collection during a pentest?

A. Delete logs after testing to minimize exposure.

B. Maintain a clear, tamper-evident chain of custody for all evidence and document each action taken.

C. Publicly share raw logs to increase transparency.

D. Do not document actions to speed up testing.

8. Which does the Host header field specify?

A. The host's IP address only

B. The internet hostname and port number of the resource being requested

C. The user account to access the resource

D. The server's supported HTTP versions

9. In a packet-filtering firewall, which rule causes the packet to be dropped without diagnostic message?

A. Allow: allow packet to pass

B. Drop: drops the packet without any diagnostic message to the packet source host

C. Deny: Do not let the packet pass, but notify the source host

D. Reject: Do not let the packet pass and send an ICMP error

10. What is 'safe harbor' in the context of a penetration test?

A. The agreed-upon authorization, scope, and boundaries that protect both tester and client legally.

B. A type of legal shield that prevents any liability.

C. An internal policy requiring testers to share vulnerabilities publicly.

D. The agreed-upon authorization, scope, and boundaries that protect both tester and client legally.

Answers

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

Explanations

1. Which of the following could be payload data in a packet?

A. The packet header

B. The checksum

C. The electrical signal

D. Part of an email message

In a network packet, the payload is the actual user data being carried, the content from higher-layer protocols, not the metadata used for routing or error checking. The packet header contains routing and control information, so it isn't payload. The checksum is used for error detection and typically lives in the header or trailer, not in the user data. The electrical signal is simply the physical representation of bits on the wire, not the data itself. An email message's content—its body and attachments—fits as the payload because it is the actual data the packet is delivering to the destination.

2. Give an example of a Linux privilege escalation vector commonly checked during pentests.

A. Using password spraying to gain root access.

B. Exploiting cron jobs to escalate privileges.

C. Enumerating kernel modules for privilege escalation.

D. Listing and examining SUID binaries for misconfigurations that could grant elevated privileges.

Privilege escalation on Linux often hinges on how programs run with elevated rights. A set-user-ID (SUID) program runs with the owner's privileges (typically root) regardless of who executes it. If such a binary is insecure or misconfigured, a non-privileged user can exploit it to gain root access. That makes SUID binaries a go-to focus during a pentest: they're directly tied to how privileges are granted and can reveal clear paths to elevation. Searching for SUID binaries and then inspecting them is a core step because many systems inadvertently expose risky SUID programs or wrappers. You'd typically locate them with a broad scan and then analyze each candidate for weaknesses, such as a binary that invokes a shell, uses unvalidated input, or calls system functions in unsafe ways. If you find a misconfigured or vulnerable SUID binary, it often provides a straightforward route to escalate privileges. Other options describe legitimate credential or persistence concepts, or require specific misconfigurations or kernel-level bugs to be exploitable. While cron job misconfigurations or kernel module vulnerabilities can enable privilege escalation, they're less universal as a baseline tactic compared to the standard, widely applicable check of SUID binaries.

3. Which statement best captures the primary distinction between authenticated and unauthenticated scanning?

A. Authenticated scans reveal internal exposure by using valid credentials; unauthenticated scans test from an external perspective without credentials.

B. Authenticated scans are always faster than unauthenticated scans.

C. Unauthenticated scans require root access.

D. Authenticated scans test only DNS configuration.

Authenticated scans use valid credentials to log into the target, giving the scanner access to internal pages, configurations, and services that aren't exposed to unauthenticated users. This allows you to see how the system behaves under a legitimate user account, verify access controls, inspect software versions and patch levels, and identify issues like insecure defaults, weak permissions, or hidden admin interfaces that only appear after login. Unauthenticated scans run without credentials and mimic an external attacker, so they can only see publicly accessible surfaces, exposed services, and misconfigurations visible without logging in. They won't reveal internal data or internal-facing controls, and they may miss issues that require access to authenticated areas. So the key distinction is the perspective and depth of visibility: authenticated scanning provides deeper, internal insight, while unauthenticated scanning assesses what an external observer can reach without credentials.

4. IP:Port pair is used to identify a single network process on a machine. Which component forms the IP:Port pair?

A. IP address

B. Subnet mask

C. Gateway

D. Port

An endpoint on a device is defined by the host's IP address and a port number. The IP address identifies the machine, while the port identifies a specific process or service running on that machine. Together, they form the IP:Port pair used by TCP/UDP sockets to deliver data to the correct application. Routing details like the subnet mask or gateway aren't part of the endpoint. The port is the component that completes the IP:Port pair, pointing to a single process.

5. On Linux, which command can be used to view the neighboring hardware address table (ARP cache)?

A. ip neighbour

B. arp -a

C. ifconfig

D. ip addr

Viewing the ARP cache on Linux is done with the ip command's neighbor subcommand. The kernel keeps a neighbor table that maps IP addresses to MAC addresses for devices the host has recently communicated with. The modern, recommended way to inspect this table is ip neigh (also shown as ip neighbor on some systems). It lists each entry with the IP, the corresponding MAC (lladdr), the interface, and the entry state (such as REACHABLE or STALE). This approach is preferred because iproute2 consolidates networking tasks in one toolset and is kept up to date. The older arp -a option can show the ARP cache, but it relies on the legacy net-tools package, which is less commonly installed and not as actively maintained, while ifconfig or ip addr focus on interface configuration rather than the ARP cache.

6. HTTPS is HTTP delivered over which cryptographic protocol?

A. TLS/SSL

B. SSH

C. IPsec

D. S/MIME

HTTPS is HTTP delivered over TLS/SSL, the cryptographic protocol that provides encryption, integrity, and authenticating the server. When you connect to a secure website, a TLS handshake runs first to agree on encryption algorithms and to exchange keys, then the actual HTTP data is sent through this secure channel. This is what keeps web traffic confidential and protected from tampering. Other protocols serve different purposes: SSH handles secure remote login and file transfer, IPsec protects IP packets at the network layer (often used for VPNs), and S/MIME encrypts email messages. None of these secure the plain HTTP traffic the way TLS does, which is why HTTPS relies on TLS/SSL.

7. Which is a best practice for logging and evidence collection during a pentest?

A. Delete logs after testing to minimize exposure.

B. Maintain a clear, tamper-evident chain of custody for all evidence and document each action taken.

C. Publicly share raw logs to increase transparency.

D. Do not document actions to speed up testing.

The key idea here is preserving evidence in a way that keeps it trustworthy and traceable. In a pentest, logs capture what you did, when you did it, and with what tools, so they must be protected from tampering and clearly linked to who performed each action. A tamper-evident chain of custody guarantees that evidence remains in its original state and that every item can be authenticated later. Coupled with thorough documentation of every action taken, this creates a reliable trail that can be reviewed, audited, or even challenged in a legal or contractual context. Implementing this means preserving logs securely, time-stamping events, and using methods to verify integrity, such as checksums or hashes. Store evidence in access-controlled, write-once or append-only media when feasible, and maintain clear records of what was done, why it was done, the tools used, commands executed, outputs observed, and any data touched. This level of discipline ensures findings are credible and reproducible, and that stakeholders can trust the results. Deleting logs would erase the record of what occurred, breaking traceability. Publicly sharing raw logs can expose sensitive information and violate privacy or contractual terms. Not documenting actions eliminates accountability and makes it impossible to reproduce or validate findings.

8. Which does the Host header field specify?

A. The host's IP address only

B. The internet hostname and port number of the resource being requested

C. The user account to access the resource

D. The server's supported HTTP versions

In HTTP, the Host header identifies the target host by its internet hostname and an optional port. This is crucial for virtual hosting, where one IP may serve multiple domains. The header looks like Host: example.com or Host: example.com:8080, and the server uses this value to select the correct website and route the request. If the port is omitted, the default port for the scheme is assumed (80 for HTTP, 443 for HTTPS). The Host header does not convey user credentials or authentication, nor does it specify which HTTP versions the server supports; those details come from other parts of the request/response.

9. In a packet-filtering firewall, which rule causes the packet to be dropped without diagnostic message?

A. Allow: allow packet to pass

B. Drop: drops the packet without any diagnostic message to the packet source host

C. Deny: Do not let the packet pass, but notify the source host

D. Reject: Do not let the packet pass and send an ICMP error

In packet-filtering firewalls, actions determine how a matching packet is treated: it can be allowed to pass, dropped silently, denied with a notification, or rejected with an ICMP error. The option that drops the packet without any diagnostic message is the silent drop. When a packet hits a drop rule, the firewall simply discards it and sends no reply or error back to the sender, which makes the source unaware that the packet was blocked. This contrasts with rejecting, which would send an ICMP error back, and with deny/notify, which implies some form of feedback to the source. Allow simply forwards the packet.

10. What is 'safe harbor' in the context of a penetration test?

A. The agreed-upon authorization, scope, and boundaries that protect both tester and client legally.

B. A type of legal shield that prevents any liability.

C. An internal policy requiring testers to share vulnerabilities publicly.

D. The agreed-upon authorization, scope, and boundaries that protect both tester and client legally.

Safe harbor in a penetration test refers to the pre-approved authorization, scope, and boundaries that protect both tester and client legally. This framework, often captured in a rules of engagement or engagement letter, spells out what systems can be tested, what methods are allowed, the testing window, data handling, and how findings will be reported. When testing stays within these agreed limits, actions are considered authorized, reducing legal risk for the tester and clarifying expectations for the client. It's not a blanket shield that eliminates all liability, and it doesn't authorize public disclosure or actions outside the defined scope. It provides a controlled, lawful environment for the assessment so vulnerabilities can be identified and reported responsibly.

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!