OSCP LINUX PRACTICE EXAM (SAMPLE)

STUDY GUIDE

SAMPLE STUDY GUIDE WITH LIMITED QUESTIONS

VISIT US ONLINE FOR THE FULL VERSION STUDY GUIDE

https://oscplinux.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. **If you're trying to redirect stdout or stderr AND throw a long command that's been piped multiple times and includes multiple commands into the background, how do you need to do it?**

   A. (command | commands; commands) > /dev/null 2>&1 &

   B. (command | commands; commands) 2> /dev/null/ &

   C. (command | commands; commands) &

   D. (command; commands | commands) > /dev/null 2>&1 &

2. **Where is the Linux kernel stored?**

   A. /root

   B. /home

   C. /var

   D. /boot

3. **If a diff shows '2,4c2,4', what does this indicate about the change?**

   A. Append after line 2

   B. Delete lines 2-4

   C. Replace lines 2-4 in the original with lines 2-4 from the new file

   D. Copy lines 2-4 from the first file to the second

4. **In the following sed command what is the g used for? sed 's/bob/jake/g'**

   A. It means that if there are more instances of 'bob' on one line, more than the first will be replaced; normally only the first 'bob' on each line would be replaced.

   B. It disables global replacement

   C. It applies replacement to the next line only

   D. It makes the replacement case-insensitive

5. **To delete a file, what permissions do you need?**

   A. Write and execute for the file

   B. Read and write for the directory

   C. Write and execute for the directory

   D. Execute and read for the directory

6. What are the basic regular expression characters?

A. ^ $. * [ ]

B. g

C. ( ) { } | ? +

D. Digits and letters

7. If you wanted to edit /etc/passwd, /etc/shadow, /etc/group, and /etc/gshadow safely, which sequence of commands would you run respectively?

A. vipw, vipw -s, vigr, vigr -s

B. vipw -s; vipw; vigr; vigr -s

C. vipw; vipw -s; vigr; vigr -s

D. vipw; vipw; vigr; vigr

8. Which option do you add to netstat to resolve hostnames to IP addresses in the output?

A. -p

B. -n

C. -a

D. -t

9. Which filter shows all TCP and ICMP packets?

A. tcp or icmp

B. tcp || icmp

C. tcp and icmp

D. tcp and not icmp

10. What does the loop for ((i=0;i<5;++i)); do echo $i; done print?

A. It runs forever.

B. It prints 1 through 5.

C. It prints 0 through 4, each on a new line.

D. It prints 0 through 4, on a single line.

Answers

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

Explanations

1. If you're trying to redirect stdout or stderr AND throw a long command that's been piped multiple times and includes multiple commands into the background, how do you need to do it?

A. (command | commands; commands) > /dev/null 2>&1 &

B. (command | commands; commands) 2> /dev/null/ &

C. (command | commands; commands) &

D. (command; commands | commands) > /dev/null 2>&1 &

The key idea is to treat the whole multi-part command as a single job, so you can redirect both outputs for the entire block and run it in the background. Wrapping the entire sequence in a subshell and then redirecting and backgrounding that subshell ensures stdout and stderr from every part of the long command are sent to /dev/null, not just a piece of it. The syntax shown does exactly that: the long sequence (including an initial simple command followed by a pipeline) is grouped, then its stdout is redirected to /dev/null and 2>&1 sends stderr there as well, and finally the ampersand backgrounds the entire grouped job. This avoids partial redirection and guarantees the whole job runs quietly in the background. In contrast, options without proper grouping or with an incorrect redirection path would either fail to redirect both streams for all parts or would not reliably background the entire composite command.

2. Where is the Linux kernel stored?

A. /root

B. /home

C. /var

D. /boot

The kernel image and its boot files are kept in the /boot directory. This location holds the compressed kernel binary (like vmlinuz-<version>) and related items such as the initial ramdisk (initramfs) and System.map, which the bootloader uses to start the system. The bootloader, for example GRUB, reads these files from /boot during startup and loads the kernel into memory. In contrast, /root is the root user's home directory, /home stores regular users' home directories, and /var contains variable data like logs and caches, none of which are where the kernel image resides.

3. If a diff shows '2,4c2,4', what does this indicate about the change?

A. Append after line 2

B. Delete lines 2-4

C. Replace lines 2-4 in the original with lines 2-4 from the new file

D. Copy lines 2-4 from the first file to the second

In diff notation, a change operation signals that a section of the original file is being replaced by content from the new file. The two ranges show which parts are involved: the portion from the original that will be replaced, and the portion from the new file that will replace it. So a change instruction means you take the specified block from the new file and substitute it for the corresponding block in the original. It is not an append or a simple delete, and there isn't a separate copy operation here. This is why the interpretation is that the original segment is replaced by the new content.

4. In the following sed command what is the g used for? sed 's/bob/jake/g'

A. It means that if there are more instances of 'bob' on one line, more than the first will be replaced; normally only the first 'bob' on each line would be replaced.

B. It disables global replacement

C. It applies replacement to the next line only

D. It makes the replacement case-insensitive

The g flag in a sed substitution enables global replacement. In the command sed 's/bob/jake/g', sed looks for every occurrence of bob on each input line and replaces all of them with jake. Without the g flag, only the first bob on each line would be replaced, leaving others unchanged. This flag operates per line, since sed processes input one line at a time. Other flags exist for different behaviors, but g specifically makes the substitution apply to all matches within a single line.

5. To delete a file, what permissions do you need?

A. Write and execute for the file

B. Read and write for the directory

C. Write and execute for the directory

D. Execute and read for the directory

Deleting a file is a change to the directory's contents, not a change to the file itself. To remove an entry, you must be able to modify the directory, which requires write permission on the directory. You also need execute permission on the directory to access or traverse it and reach the entry you want to delete. The file's own permissions don't control whether you can delete it. (Note: a sticky bit on a directory, common on shared dirs like /tmp, can restrict deletion of files owned by others even if you have write/execute on the directory.) So, the necessary permissions are write and execute on the directory.

6. What are the basic regular expression characters?

A. ^ $. * [ ]

B. g

C. ( ) { } | ? +

D. Digits and letters

Regular expressions rely on metacharacters that carry special meaning beyond literal characters. The foundational ones include the caret for the start of a string, the dollar sign for the end, the dot which matches any single character, the asterisk indicating zero-or-more repetition of the preceding element, and the square brackets that define a character class. Together, these five provide the essential tools to anchor patterns, broaden matching, repeat, and specify acceptable sets of characters. Other symbols like grouping, alternation, or additional quantifiers are useful but represent more advanced constructs beyond this basic set, and letters or digits by themselves aren't special regex characters.

7. If you wanted to edit /etc/passwd, /etc/shadow, /etc/group, and /etc/gshadow safely, which sequence of commands would you run respectively?

A. vipw, vipw -s, vigr, vigr -s

B. vipw -s; vipw; vigr; vigr -s

C. vipw; vipw -s; vigr; vigr -s

D. vipw; vipw; vigr; vigr

Editing these critical authentication files must be done with the system's safe, locked editing tools. vipw opens the password file in a protected environment, ensuring the file isn't corrupted by partial writes. When you need to modify the shadow data, vipw -s edits the shadow file in the same safe way, targeting the correct file. For the group database, vigr provides a safe editing session for /etc/group, and vigr -s does the same for the gshadow file. Using the appropriate tool for each file, and the -s option to reach the corresponding shadow or gshadow file, keeps the edits atomic and properly formatted. This sequence—vipw for passwd, vipw -s for shadow, vigr for group, and vigr -s for gshadow—ensures you modify the right files safely.

8. Which option do you add to netstat to resolve hostnames to IP addresses in the output?

A. -p

B. -n

C. -a

D. -t

Netstat can resolve addresses to hostnames by default, showing friendly names instead of raw IPs. To display the numeric IP addresses in the output, you use the numeric option, which disables name resolution. This makes the addresses appear as IPs directly, which is why this option is the best fit. The other options serve different purposes: one shows the owning process, one lists all sockets, and one restricts output to TCP connections, none of which change how hostnames are resolved.

9. Which filter shows all TCP and ICMP packets?

A. tcp or icmp

B. tcp || icmp

C. tcp and icmp

D. tcp and not icmp

Using a logical OR to combine simple protocol checks is the way to show all TCP and ICMP packets. One check matches TCP packets, the other matches ICMP packets. By combining them with OR, a packet passes if it is either TCP or ICMP, so you see every packet of those two protocols. If you used AND, you'd require a packet to be both TCP and ICMP at the same time, which doesn't happen, so that would yield nothing. If you used TCP with AND NOT ICMP, you'd end up filtering to TCP packets only and explicitly excluding ICMP, which misses ICMP traffic entirely. The form with an alternative OR symbol (like ||) can work in some tools, but the clear, standard way is to use or.

10. What does the loop for ((i=0;i<5;++i)); do echo $i; done print?

A. It runs forever.

B. It prints 1 through 5.

C. It prints 0 through 4, each on a new line.

D. It prints 0 through 4, on a single line.

This uses a C-style for loop in Bash. It starts with i=0, checks i<5 before each iteration, and after each iteration runs the increment ++i. The body prints the current value of i. Since the increment happens after the body, the values seen and printed are 0, 1, 2, 3, 4. When i becomes 5, the condition i<5 is false, so the loop stops. Echo prints each value on its own line, giving 0 through 4, each on a new line.

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://oscplinux.examzify.com

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