CERTLABZ CERTIFICATION BOARD

Certified Penetration Testing Professional (CPTP)

Ten Sample Questions

These ten questions are written at the difficulty of the live exam. Six carry a figure, a data table, a configuration or a code listing; four are plain scenario questions, as on the live paper. Every one is a scenario a working penetration tester would meet, and none of them appears in the live question bank.

The live exam is multistage adaptive: how you score on one stage selects the difficulty of the next, so no two candidates sit the same paper. It is a performance-based exam: each form can carry up to 5 to 12 performance-based questions alongside the multiple-choice questions, which means you build, sequence or complete something rather than only choosing from a list. Answers and full explanations follow each question here; the live exam does not disclose item-level answers.

Question 1

Domain 1: Penetration Testing Foundations

DATA

Sarah Miller matches each engagement document to its purpose, with one purpose missing.

Document	Purpose
Scope statement	Defines targets in bounds
Rules of engagement	(to choose)
Authorization letter	Grants written consent
Final report	Records findings and fixes

Table 1.1 Engagement documents.

What do the rules of engagement set?

A. The client budget
B. Testing limits and timing
C. The staff payroll
D. The office floor plan

Correct answer: B
The rules of engagement define the allowed methods, timing windows and limits agreed with the client before testing starts. The scope statement lists targets, the authorization letter grants consent, and the final report records outcomes.

Question 2

Domain 2: Reconnaissance and Scanning

CONFIG

James Carter reviews a redacted port scan summary taken during an authorized test.

```
PORT     STATE   SERVICE
22/tcp   open    ssh
80/tcp   open    http
443/tcp  open    https
3306/tcp open    mysql
```

Listing 2.1 Scan summary.

Which finding most warrants a closer review?

A. Exposed database port
B. Standard web on 80
C. Secure web on 443
D. Managed ssh on 22

Correct answer: A
A database service on 3306 reachable from the tested network is unusual and often should not face untrusted hosts, so it warrants a closer review. The web and ssh ports are common and expected on many servers.

Question 3

Domain 3: Exploitation

DATA

Emma Wilson maps each exploitation concept to its meaning, with one meaning missing.

Concept	Meaning
Vulnerability	A weakness in a system
Exploit	(to choose)
Payload	Action run after access
Proof of concept	Safe demonstration only

Table 3.1 Exploitation concepts.

What does an exploit describe?

A. A signed support contract
B. A routine backup job
C. A means to use a weakness

D A plan for staff training

Correct answer: C
An exploit is a means of taking advantage of a vulnerability to gain some unintended effect during authorized testing. A vulnerability is the weakness itself, the payload is what runs after access, and a proof of concept is a safe demonstration.

Question 4 — Domain 4: Web and Application Testing — DATA

David Brown maps each web weakness to its short description, with one description missing.

Weakness	Description
Injection	Untrusted input reaches a query
Broken access	(to choose)
Misconfiguration	Unsafe default settings left on
Weak session	Predictable session tokens

Table 4.1 Web weaknesses.

What does broken access control allow?

A Faster page loads
B Cleaner site design
C Lower hosting cost
D Reaching restricted data

Correct answer: D
Broken access control lets a user reach data or actions that should be restricted to others, such as viewing another accounts records. The other options describe performance, design or cost rather than an access flaw.

Question 5 — Domain 5: Post-Exploitation and Privilege Escalation — CONFIG

Olivia Davis reviews an account listing gathered on an authorized test host.

```
USER      GROUP
webapp    users
backup    operators
jsmith    users
svc_admin administrators
```

Listing 5.1 Local accounts.

Which account is the best escalation target?

A svc_admin
B webapp

C jsmith

D backup

Correct answer: A
The svc_admin account sits in the administrators group, so gaining it would grant the highest privilege on the host. The other accounts hold standard user or limited operator roles that offer less control.

Question 6

Domain 6: Reporting, Ethics and Standards

DATA

Ava Thompson orders findings by severity for the report, with one rating missing.

Finding	Severity
Exposed admin console	Critical
Missing security header	(to choose)
Weak password policy	Medium
Verbose error page	Low

Table 6.1 Findings by severity.

What severity fits a missing header?

A Critical

B Blocker level

C Low

D Beyond critical

Correct answer: C
A single missing security header raises risk only slightly on its own, so it fits a low rating in the report. The exposed admin console is critical, and a weak password policy sits in the middle at medium.

Question 7

Domain 1: Penetration Testing Foundations

A client asks a tester to begin work on a system that is not named in the signed scope or authorization. What is the correct action?

A Test it quietly first

B Ask another tester

C Guess the intent

D Pause and get written consent

Correct answer: D
Ethical testing requires written authorization for every target, so the tester must pause and get the scope and consent updated before touching the system. Testing without consent, guessing intent, or asking a colleague does not create authorization.

Question 8 Domain 2: Reconnaissance and Scanning

A tester wants to learn about a target using only public sources, without sending any packets to the target systems. Which approach fits?

A. Passive recon
B. Full port sweep
C. Loud vuln scan
D. Brute force login

Correct answer: A
Passive reconnaissance gathers information from public sources without interacting with the target, so no packets are sent to its systems. Port sweeps, vulnerability scans and brute force attempts all send traffic directly to the target.

Question 9 Domain 5: Post-Exploitation and Privilege Escalation

After gaining access during an authorized test, a tester wants to keep the environment safe and undamaged. What practice best supports this?

A. Delete the logs
B. Alter user records
C. Limit and document actions
D. Leave hidden backdoors

Correct answer: C
A professional tester limits actions to what the engagement needs and documents each step so the client can verify and clean up afterward. Deleting logs, altering records or leaving backdoors harms the environment and breaks the rules of engagement.

Question 10 Domain 6: Reporting, Ethics and Standards

A tester finds a serious flaw midway through an engagement that puts customer data at real risk. What is the sound reporting practice?

A. Post it publicly
B. Report it promptly
C. Wait until year end
D. Tell only a friend

Correct answer: B
A serious flaw that risks customer data should be reported promptly to the client contact so it can be addressed before the final report. Public disclosure, long delays or informal sharing breach confidentiality and leave the risk open.

CPTP-001. https://certlabz.com/certifications/certified-penetration-testing-professional.html