Penetration Tester interview questions

careertips.com.au: common questions and what they're really testing

What to expect

Penetration tester interviews test three things at once: whether you actually know how to break systems methodically, whether you can be trusted with access to sensitive environments, and whether you can explain what you found to people who don't read exploit code. Expect a mix of methodology questions, hands-on or scenario-based problem solving, and direct questions about scope and ethics.

- **Technical methodology:** Questions asking you to walk through how you'd actually approach testing a specific system, tool by tool and phase by phase.
- **Scenario / judgement:** Hypothetical situations that test how you'd react to unexpected findings, scope creep or ethical grey areas mid-engagement.
- **Behavioural:** Past-experience questions about handling difficult stakeholders, disagreements over findings, or pressure to soften a report.
- **Client-facing communication:** Questions on translating technical findings into business risk for executives who aren't technical.
- **Safety and ethics:** Questions probing your understanding of rules of engagement, legal boundaries and the Privacy Act when handling data you shouldn't retain.

Most processes start with a recruiter or HR screen on background and clearances, followed by a technical interview with a senior tester or security lead covering methodology and possibly a live or take-home practical exercise (a mini CTF or log analysis task). A final round often includes a client-facing or panel interview where communication style and ethical judgement are assessed alongside technical depth.

1. Walk me through your methodology for a black-box web application penetration test, from kickoff to report.

Why they ask

This checks whether you follow a repeatable, defensible process rather than testing ad hoc, which matters both for coverage and for legal defensibility of the engagement.

How to structure your answer

Walk through it phase by phase: scoping and rules of engagement, reconnaissance, mapping the attack surface, exploitation, post-exploitation and evidence capture, then reporting and retesting.

Example answer

“I start by confirming scope and rules of engagement in writing, including what's out of bounds. Then I do reconnaissance with Nmap to map open ports and services, and manually crawl the application to understand its functionality. I use Burp Suite to intercept and test requests, focusing on authentication, session handling and input validation, and I'll bring in Metasploit if I find a service-level vulnerability worth exploiting further. Throughout, I keep detailed notes and screenshots as evidence. Once testing is done I rate each finding by severity, write remediation advice specific to the tech stack, and offer a retest window once fixes are applied.”

2. During a test you gain access to a production database containing customer personal information, which is outside the agreed scope. What do you do?

Why they ask

This tests judgement under pressure around legal boundaries, the Privacy Act, and whether you'll stick to rules of engagement when a more interesting path opens up.

How to structure your answer

Explain the immediate decision, the reasoning behind it, and the follow-up actions, in that order, rather than jumping straight to the resolution.

Example answer

“I'd stop testing that path immediately rather than pull or view any records, because accessing data outside scope creates legal and privacy exposure for both me and the client. I'd document exactly how I got there and what I could see without extracting anything, then flag it urgently to my engagement lead so the client can be notified. Depending on the rules of engagement, this might warrant an out-of-cycle report given the severity, since unrestricted access to customer PII is a critical finding regardless of scope.”

3. Tell me about a time you found a critical vulnerability that stakeholders were reluctant to fix.

Why they ask

Testers regularly deliver unwelcome news. This checks whether you can hold your ground on a finding without damaging the working relationship.

How to structure your answer

Use STAR: describe the situation, the specific task or finding, the action you took to get it taken seriously, and the result.

Example answer

“During an internal network assessment I found a legacy server still using an outdated authentication protocol that allowed credential relay attacks. The infrastructure team pushed back, saying the server was scheduled for decommission anyway. I explained the actual exploit path and demonstrated, in a controlled way, how it could lead to domain compromise, then linked the finding to the ASD Essential Eight patching guidance to give it business context. That reframing got it prioritised for an interim mitigation ahead of the full decommission.”

4. How would you test whether an API's authentication tokens can be manipulated to escalate privileges?

Why they ask

API security is central to modern penetration testing, and this checks specific technical knowledge beyond generic web testing.

How to structure your answer

Walk through the technical steps in order: what you'd inspect first, what you'd try, and how you'd confirm the finding.

Example answer

“I'd start by decoding the token structure, checking if it's a JWT and whether claims like role or user ID are trusted without server-side revalidation. Using Burp Suite I'd intercept requests and try modifying those claims or swapping tokens between test accounts of different privilege levels to see if the API accepts the tampered token. I'd also check token expiry handling and whether signature verification can be bypassed, for example through an 'alg: none' downgrade. Any successful escalation gets captured with a full request and response trail as evidence.”

5. How do you explain a critical finding to a non-technical executive who's mainly worried about the cost of fixing it?

Why they ask

Reports get read by people who control budget, not just engineers. This tests whether you can translate technical risk into business language without dumbing it down.

How to structure your answer

Describe your general approach to framing risk, then give a concrete example of language you'd use.

Example answer

“I avoid leading with technical detail. I lead with impact: what could happen, how likely it is, and what it would cost the business if it went wrong versus the cost of the fix. For example, rather than describing a SQL injection flaw in detail, I'd say it lets an attacker read the entire customer database without needing a password, and that regulators would expect this fixed before it's exploited. I keep the technical writeup available for their engineers but frame the executive conversation around business risk and comparative cost.”

6. How do you make sure your testing stays within the agreed rules of engagement, especially when a new opportunity to escalate access presents itself mid-test?

Why they ask

This directly probes professional discipline and legal awareness, both essential given the access testers are trusted with.

How to structure your answer

Explain your process and safeguards rather than a single anecdote: what you check before testing, and what you do in the moment when tempted to go further.

Example answer

“Before any engagement I confirm the written scope and get sign-off from a client contact who has authority to approve it. During testing I keep a running log against that document, and if I find a path that would take me outside agreed systems or IP ranges, I stop and raise it rather than proceeding, even if it looks like a quick win. It's a judgement call sometimes, but the rule I follow is that anything not explicitly in scope needs explicit approval before I touch it.”