Black box, gray box, white box. Three ways to scope a pentest.

Black box, gray box, and white box describe how much information the tester has at the start of the engagement. Black box is the realistic outside-attacker simulation: no internal access, no documentation, find everything from scratch. White box is the maximum-coverage approach: source code, architecture diagrams, internal accounts, full credentials. Gray box sits in the middle: partial credentials and limited documentation, mirroring what an attacker who has compromised a typical user account would see. Most pentests are gray box because it is the best trade-off between realism and coverage.

HOW IT WORKS

01 How does each approach change what gets found?

- Black box finds weaknesses an outside attacker would actually reach. Misses anything that requires authenticated access the tester could not obtain in the engagement window. Slower per finding because of the discovery overhead.
- Gray box finds the broadest realistic mix: outside attacker paths plus the authenticated paths a compromised user would have. The combination most useful for most applications.
- White box finds the most weaknesses overall, including ones that would never be reached by an outside attacker but matter for defence in depth. Code-review and architecture-review findings appear here that would not appear in black box.

02 Which approach should you choose?

Three rules of thumb that hold for most engagements:

- Default to gray box. Best trade-off between realism and coverage. Most engagements should be gray box unless there is a specific reason to choose otherwise.
- Choose white box when you are testing before launch (you want maximum coverage in a short window), when the application is complex with significant business logic, or when source code review is in scope.

SOURCES

[1] NIST SP 800-115

[2] OWASP Web Security Testing Guide

[3] PTES Pre-engagement Interactions

- Choose black box when you specifically want to know what an outside attacker would reach (often for board reporting or after a near-miss incident), or when external attack-surface measurement is the goal.

A few engagements combine approaches: an initial black box phase for realism, transitioning to gray box once the tester has reached internal access through legitimate exploitation.

03 Common misconceptions

- Black box is not more thorough. It is more realistic but covers less ground in the same time window. The tester spends a large fraction of the engagement on reconnaissance the customer already has documented.
- White box is not 'cheating'. It is the most efficient way to cover the system in a fixed window. The realism trade-off is the cost, not a quality issue.
- Gray box does not need to be perfectly defined. A typical user account plus an admin account is enough for most engagements. The tester does not need every credential up front.
- Authenticated vs unauthenticated is a separate question. Authenticated testing means the tester has a working account in the application. White box means the tester also has source and architecture. They are not the same axis.

04 What about compliance and procurement?

Most compliance frameworks (PCI DSS, SOC 2, ISO 27001, HIPAA) do not mandate which approach to use. They require that penetration testing happens against the scope at the required cadence. The choice of approach is left to the customer and the tester to agree.

Procurement and customer-due-diligence questions sometimes ask 'was this a black box test?' as a proxy for 'how realistic'. The honest answer is usually 'gray box' for most engagements, with a clear explanation of what that means. Black box claims that are not actually black box (because the tester got documentation halfway through) damage credibility.

Default to gray box. Refine with us.

securelayer7.net/learn/pentest/black-box-vs-gray-box-vs-white-box-pentest

Open online