

Vulnerability Testing vs. Penetration Testing (and Why the ROE Comes First)

Thu, Aug 13, 4:00 PM EDT · <https://scottslab.io/posts/vulnerability-testing-vs-penetration-testing>



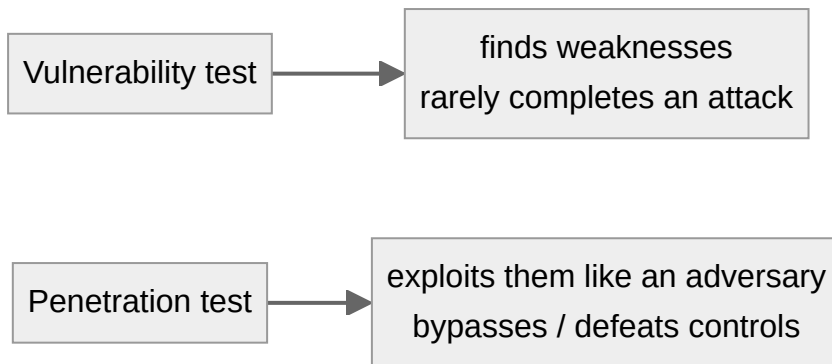
TL;DR

A vulnerability test finds weaknesses; a penetration test proves them by actually exploiting them like an attacker would. That difference is the point: a scanner says "port 445 looks vulnerable," a pentester walks through it, pivots, and shows you what it costs. None of it starts without documented Rules of Engagement. The knowledge level, white, grey, or black box, decides which attacker you're simulating.

These two get lumped together and they are not the same job. A vulnerability test probes for weaknesses and stops there. It tells you what looks exploitable. A penetration test simulates a real attack: the tester acts as an adversary and actually tries to bypass or defeat your controls, chaining findings into a working intrusion. The scanner hands you a list; the pentester hands you a story of how far they got with it. Both are useful, but only one tells you whether a "medium" finding is actually a path to the crown jewels.

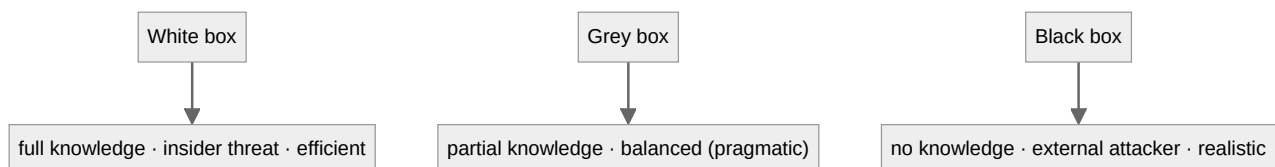
Because a pentest is a real attack by consent, nothing happens until the Rules of Engagement are written down. The ROE defines what's in scope, which systems are fair game, and which techniques are allowed: no social engineering, no denial of service, only these IP ranges, only these hours. It's

the document that keeps an authorized test from becoming an incident (or a crime), and skipping it is how well-meaning tests take down production and end careers.



Vulnerability Testing vs. Penetration Testing (and Why the ROE Comes First)

Then there's how much the tester knows going in, which decides which threat you're modeling. White box means full knowledge of the network: architecture, credentials, source. It simulates an insider, or a determined attacker who's already done the homework, and it's efficient because no time is burned on discovery. Black box is the opposite: no prior knowledge, the tester starts from the outside like a stranger on the internet, which is realistic but spends real effort just mapping the attack surface. Grey box splits the difference with partial knowledge, and it's usually the pragmatic pick: an external attacker's perspective without paying full price for reconnaissance.



Vulnerability Testing vs. Penetration Testing (and Why the ROE Comes First)

The takeaway is to match the engagement to the question you're actually asking. Want to know whether you'd survive a random internet attacker? Black box. Want to know how bad a compromised employee could get, fast? White box. Want a realistic result on a budget? Grey box. And whichever you pick, the ROE is written and signed before anyone touches a keyboard.