What is penetration testing?

Penetration testing (often called a pentest) is a controlled attack on a system performed by a security professional, with permission, to find out what an unauthorised attacker could actually achieve. A useful pentest produces a report that names every weakness the tester reproduced, ranks each by realistic impact, shows the request or evidence that proves it, and recommends the fix. It is different from automated scanning, different from a bug bounty programme, and different from a red team engagement.

HOW IT WORKS

01 What does a pentest actually cover?

Scope is decided by the customer, not the tester. A typical engagement covers one or more of:

- A web application (the customer-facing site, the admin portal).
- APIs (REST, GraphQL, gRPC, the endpoints behind the mobile app).
- A mobile application (the iOS or Android binary plus its backend).
- A cloud environment (the AWS / Azure / GCP account and what runs in it).
- A network perimeter (the externally reachable IPs and services).
- An internal network (an attacker who is already inside).
- A specific feature (the payment flow, the new AI assistant, the SSO integration).

What is in scope determines the engagement type. A web pentest looks very different from a network pentest, which looks different from a smart contract audit, even though they all share the same overall methodology.

02 Why do organisations run penetration tests?

Four reasons come up most often:

- Find what is exploitable before someone else does. The blunt and original purpose. A pentest in advance is much cheaper than an incident.

SOURCES

[1] NIST SP 800-115 Technical Guide to Information Security Testing

[2] PTES Penetration Testing Execution Standard

[3] OSSTMM Open Source Security Testing Methodology Manual

[4] OWASP Web Security Testing Guide

- Compliance requires it. PCI DSS, SOC 2, ISO 27001, HIPAA, FedRAMP, CERT-In, and most large enterprise procurement processes require an external penetration test, usually annually plus after major changes.
- Before a release or after a major change. A new feature, a re-architecture, a cloud migration, a third-party integration. Major change is when defects ship.
- Independent verification for stakeholders. Investors, board members, customers, and auditors want a third party (not the team that built the system) to assess the security posture.

03 How is a pentest different from other security activities?

The four most-confused terms in security buying:

- Vulnerability assessment. Wide, automated, frequent. Finds known weaknesses. No exploitation, no business-logic flaws. (Detailed comparison.)
- Bug bounty. Open call to outside researchers, paid per valid finding. Wide attacker pool, narrow scope rules, no guaranteed coverage. (-Detailed comparison.)
- Red team. Goal-led adversary simulation. Tests the entire security programme (people, process, technology), not just one application. Detection and response are part of the test. (Detailed comparison.)
- Audit. Document review, control verification, evidence collection. Not an attack.

04 How long does a pentest take?

Depends entirely on scope. A focused engagement against a single web application typically runs one to two weeks of active testing plus another week for reporting. A multi-surface engagement (web plus API plus mobile plus cloud) runs three to six weeks. A red team engagement runs four to twelve weeks.

The duration is decided during scoping. A good engagement is bounded by what the customer wants tested, not by how many hours the tester wants to bill.

05 What does a good penetration test report contain?

Every useful report has six things:

- An executive summary for non-technical readers: what was tested, headline findings, business risk in plain language, recommended priorities.
- A scope and methodology section showing exactly what was in scope, what was out of scope, what techniques were used, and what was not tested.
- A findings section with one entry per weakness: title, severity, the affected component, evidence (request, payload, screenshot, video), realistic impact, and remediation.
- A remediation guide developers can act on, not just a CVSS score.
- A retest section describing what was verified after the customer fixed things.
- Appendices with the raw evidence, payloads, and references.

A report that ranks findings only by CVSS without context is not useful. A report that names the change required in the customer's actual code, configuration, or architecture is.

Scope a penetration test in 30 minutes.

securelayer7.net/learn/pentest/what-is-penetration-testing

Open online