Penetration testing, in plain terms.

Penetration testing is a controlled attack on a system performed by a security professional, to find what an unauthorised attacker could actually do. The output is a report that names every weakness reproducible by the tester, what each weakness could lead to, and what to change. The topics below cover the fundamentals: what a pentest is, how it differs from other security activities, the standard methodology stages, and what a useful report contains.

HOW IT WORKS

01 Topics

- What is Penetration Testing?: plain-language definition, what it covers, why organisations run them.
- Penetration Test vs Vulnerability Assessment-: same words, different work. How they differ and when to use each.
- Penetration Test vs Bug Bounty: paid researcher with fixed scope vs an open crowd. Coverage, cost, and contract differences.
- Penetration Test vs Red Team: checklist coverage vs goal-led adversary simulation. When each fits.
- Black Box vs Gray Box vs White Box: three ways to scope what the tester knows. Tradeoffs explained.
- CREST vs CERT-In: two of the most-asked-for credentials. What each one means and when auditors require it.
- Pentest Methodology Stages: reconnaissance, scanning, exploitation, post-exploitation, reporting. The five-stage model used by every serious team.
- Pentest Report Formats: executive summary, technical findings, reproducible evidence, remediation. What a useful report contains.
- What is Autonomous Penetration Testing?-: software that runs the steps of a pentest on its own, and where it still needs people.

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

Scope a penetration test.
securelayer7.net/learn/pentest

Open online