

PENETRATION TESTING

Old techniques, new techniques. red techniques. blue Techniques.
Real-world attack simulation against your organization.



A penetration test is a set of tactics that mimic the real-world threats your organization faces. By emulating modern attackers, we surface the gaps in your preventative and detective controls before a real adversary finds them. Because attackers come from every direction, a full test runs across several attack surfaces. **You won't get AI slop from us, just curated, detailed findings with actionable fixes.**

ATTACK SURFACES WE TEST

External Testing



Targets your organization from the public internet, the surface attackers probe most frequently and aggressively.

Internal Testing



Simulates an attacker who already has network access, or a malicious insider. Often the most devastating if it succeeds.

Social Engineering



Bypasses your technical controls by going right to the most common source of errors, the users. Documented as 62% of breach root causes in 2026. (Source: Verizon DBIR)

Physical Security Testing



Gains unauthorized access to secure areas, testing the people and physical controls that protect your facilities.

WHY SEVN-X

At SEVN-X, AI is seen as "Augmented Intelligence", not "All-the-Things Intelligence." We sift through the data, tool output, and findings to provide you a hyper-focused report **handwritten by real hackers, not AI agents.**

● Accomplished ethical hackers

● Actionable recommendations

● Annual cadence recommended

