SEVNX

PENETRATION TESTING

What is Penetration Testing?

Simply put, it's a collection of tactics that mimic real-world threats the organization is expected to face from modern attackers.

By emulating various attacks against the organization, a penetration test identifies gaps in preventative and detective controls that should be addressed to reduce the likelihood of a successful compromise from hackers. Since there are multiple attack surfaces, a penetration test is comprised of a series of phases:

External Testing
targets the organization from the public Internet. This attack surface is the most frequently and aggressively targeted.

Internal Testing
simulate attackers that have gained internal network access or malicious insiders. This can be the most devastating if successfully compromised.

Social Engineering
is the most common means of compromise for any and every organization. It played a role in 82% of all breaches in 2022 (*Verizon DBIR*).

Physical Security Testing
attempts to gain unauthorized access to secure areas of a facility. This assessment tests the people and/or physical controls in place to protect the organization's personnel and infrastructure.

Is Penetration Testing Right for My Organization?

In short, it depends. For a company with no security program of any kind, it can be an "OK" place to begin, but there may be better places to start when formalizing an information security program.

Mature organizations should be conducting these assessments at least annually. Talk to us for a free and honest consult on whether penetration testing is right for you.

Why Use SEVN-X for Your Next Assessment?

Ditch the generic guidance and unformatted tool output for purposeful, detailed explanations with actionable recommendations, all produced by a team of accomplished ethical hackers.

info@sevnx.com

SEVNX

484.989.0911

ACHIEVE BETTER CYBERSECURITY