Network Penetration Testing: Assess Your Security Before Attackers Do

---

If your business was hacked tomorrow, do you know what would happen? Protecting your valuable assets and customer data is paramount in today's digital landscape. Alongside robust security software, regular network penetration tests play a critical role, and these tests are precisely what cybersecurity insurers will look for when assessing your policy.

What is Network Penetration Testing?

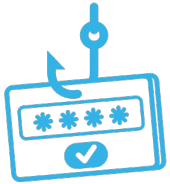
Network penetration testing is a security test where experts try to hack into an organization's computer network to find vulnerabilities and weaknesses. It's like a "mock" hack to see if a hacker could get in and cause damage. The goal is to identify any problems and fix them before a real hacker can take advantage. It's basically a way to check the security of an organization's network.

How Do Data Breaches Occur?

A data breach occurs when a cybercriminal infiltrates a data source and extracts confidential information. This can be done by accessing a computer or network to steal local files or by bypassing network security remotely. The most common cyber attacks used in data breaches are outlined below.

RANSOMWARE

MALWARE



PHISHING

DENIAL OF SERVICE (DOS)

Why you need penetration testing?

Demonstrate real-world risk by simulating a malicious hacker

Understand how attackers target their most confidential/sensitive data

Evaluate current security detection and monitoring controls

Provide remediation strategies to mitigate risk

Penetration Testing is Worth Every Penny

Using the results of a penetration test, your organization can identify ways to **protect its most valuable data** by reducing the number of attack vectors and accessible paths to sensitive resources and systems.

We offer two different network penetration testing services to guide your organization to a better security posture and program.

Internal Network Penetration Testing

Using a device connected to your internal environment, our consultants will discover security vulnerabilities present within the internal network environment. These activities simulate that of a malicious attacker.

External Network Penetration Testing

Assuming the role of a malicious attacker from the public Internet, our consultants will identify security flaws within your external network environment. These flaws can include patching, configuration, and authentication issues.

Why use “Partner Name” for Penetration Testing

Backed by Security Experts

Our solution combines the knowledge, skills, logic, and toolsets of certified penetration testers.

Meet Compliance/Cyber Insurance Requirements

By having the ability to perform a quality network penetration test whenever you want and however often you want, your organization can be assured that it will continuously meet security best practices and compliance regulations.

Why use “Partner Name” for Penetration Testing

We make Penetration Testing More Affordable

Our solution is typically about 50% the cost of other providers. We deploy the latest technology that helps our team perform penetration testing more efficiently and we pass those savings to bring you pentesting at an affordable cost.

We provide the ability to do monthly penetration testing at no additional cost

We make Penetration Testing More Efficient

We provide real-time results and deliver reports within days, instead of weeks or months.