Penetration Testing

DATASHEET

tracesecurity
Compliance, simplified.

877-275-3009 tracesecurity.com sales@tracesecurity

Don’t Be a Target

Every company has safeguards against cybersecurity attacks – things like firewalls, intrusion detection and prevention – but do you truly know how effective these protections are? There is value in performing a vulnerability assessment to scan networks for vulnerabilities, but penetration testing goes a step further with manual exploitation of these vulnerabilities to find what a real-world attacker could access.

Attackers are always looking for unsecured networks to exploit, and it's easy to be a target. Penetration testing is the best way to test your network against a real world attack.

What We’ve Noticed

The most common vulnerabilities discovered during penetration testing are related to network configuration. Many default systems that organizations use to communicate over their networks actually allow malicious attackers to capture information as it travels through the network, leaving your organization vulnerable to a breach. Another common vulnerability comes from your device and server configurations. Leaving default configurations on any device may not seem harmful, but it provides an easy access point for attackers to access sensitive areas.

Secure Your Networks

With several types of penetration testing available, you can get a manual test on any area of your network – including internal, external, wireless and more. Once you know how deep our analysts can get into your networks, you’ll know what areas need to be focused on. You can begin remediation on the weakest areas and ensure malicious attackers can’t get in.

Benefits of Penetration Testing:

- ✓ **Manual exploitation of vulnerabilities using real-world hacking techniques**
- ✓ **Understand any network security gaps and how to fix them**
- ✓ **Simulation of what an attacker could access through unsecured networks**
- ✓ **Verification of network security controls**

Types of Penetration Testing

External Penetration Testing (EPT)

Simulate what an attacker could get to through your external network including firewalls, web servers, mail servers, and more. We’ll perform a vulnerability scan and then attempt to manually exploit any found vulnerabilities to see what a malicious attacker could acces.

Internal Penetration Testing (IPT)

If external measures have been breached, this assessment simulates what an attacker could access once inside your internal network. We’ll perform a vulnerability scan of internal networks and manually exploit any found vulnerabilities to determine what could be accessed by a malicious attacker or a rogue employee.

Penetration Testing Including Medical Devices

This special type of Internal Penetration Test focuses on what an attacker could compromise, even through medical devices connected to your networks. We’ll attempt to exploit any found vulnerabilities to ensure your information, including protected health information, is secure.

PCI DSS Penetration Testing

Learn the vulnerabilities associated with electronic card transactions with a PCI scan followed by manual testing to determine if an attacker could compromise your customer data or payment card information.

Web Application Testing

We’ll perform a vulnerability scan against your application and then attempt to manually exploit any found vulnerabilities. Applications typically have the most sensitive and important information to your organization, and our team will find your security gaps before an attacker does.

Wireless Assessment & Penetration Test (WAPT)

Get a detailed review of your wireless configurations to analyze and identify different network attack vectors. We’ll manually test your device configurations, wireless policies, and wireless topology mapping to ensure this isn’t a gateway for attackers.