Welcome to the Human Side of Tech

Penetration Testing

Discover internal and external vulnerabilities through a simulated cyber-attack by highly-skilled experts using sophisticated tools and technology. A Pen Test is a simulated cyber attack that offers unparalleled insight into an organization's data security effectiveness. During the test, security vulnerabilities are identified and attempts are made to compromise systems and gain unauthorized access to data. At the conclusion of the test, TCDI provides a written report summarizing the vulnerabilities identified, threat level, and suggested remediation steps.

Our goal is to identify systems that exhibit known vulnerabilities, weak configurations, or out-of-date software, and to measure the impact of those vulnerabilities on the network as a whole. Our engineers routinely write custom attack programs, or modify existing techniques to take advantage of security conditions that are unique to a given customer environment.

By hiring experts to simulate a cyber attack, vulnerabilities can be identified and corrected before they are exploited by a hacker or malicious insider.

External

An external network penetration test identifies and validates vulnerabilities in internet-facing hosts and addresses the ability of a hacker to gain access to an internal network from outside the firewall.

Firewall

A firewall penetration test involves a configuration review of an organization's perimeter devices. This often includes an analysis of a firewall's rules and settings against industry best-practices in order to identify potential security gaps.

Web Application

A web application penetration test identifies and validates vulnerabilities by analyzing system configurations, authentication mechanisms, session management, authorization, and data validation, among other factors.

Internal

An internal penetration test analyzes an attack from inside the firewall by an employee, trusted vendor, or unauthorized user and addresses the ability to achieve privilege escalation, pivot to other systems, and gain access to sensitive organizational resources.

Wireless

A wireless penetration test evaluates an organization's wireless network and infrastructure, including routers and Voice-over-IP (VoIP) systems, to identify and validate vulnerabilities that could lead to access to an organization's internal network or other wirelessly connected systems.

To Request More Information / 1.877.840.4357 / www.tcdi.com