PCI Penetration Testing

DATA SHEET

Penetration Testing To Protect Customer Data - And Your Business - From A Breach

Conducting a penetration test will allow you to discover the vulnerabilities in your IT infrastructure and correct them before they can be exploited by hackers and other hostile forces. One of the oldest and most trusted methods for assessing security risks is penetration testing. Penetration testing is designed to simulate a real-world attack using tools and techniques employed by actual hackers. It provides realistic examples of how a real hacker could compromise sensitive data. A PCI Penetration Test involves the technical testing of your information resources and externally accessible networks, firewalls, IDS, routers, switches, servers, and services as they pertain to your business' credit card environment.

The Compliance Overview

PCI DSS Requirement 11, commonly referred to as the "pentest requirement," mandates any company that processes, stores and transmits electronic card transactions to conduct one PCI penetration test annually. Additionally, the requirement states that organizations must conduct a penetration test each time a significant change occurs to network infrastructure of applications. What is deemed "significant" is highly dependent on an entity's risk assessment process and on the unique IT environment. Penetration testing of such changes will ensure that controls assumed to be in place continue to work effectively after the upgrade or modification.

Important Dates:

- July 2015: PCI Penetration Testing requirements become official, making pen tests mandatory for compliance.
- March 2015: The PCI Security Standards Council (SSC) released supplemental guidance, Information Supplement: Penetration Testing Guidance, effective July 1, 2015.

The TraceSecurity Penetration Testing Overview

To better equip organizations to prevent cybersecurity attacks and maintain PCI compliance with changing regulations, TraceSecurity delivers a best practice security testing methodology for the entire Cardholder Data Environment (CDE) perimeter, any critical systems that may impact the security of the CDE and all environments that are in-scope for PCI DSS 3.1. This includes the external perimeter (public-facing attack surfaces). A TraceSecurity PCI Penetration Test also includes access to TraceCSO vulnerability management and reporting capabilities.

A TraceSecurity PCI Penetration Testing engagement includes:

- Engagement Interview
- Network Documentation Collection
- Network Scope
- Segmentation Checks
- Application and Network Testing
- Immediate Notification of Critical Risks and/or Encountering Cardholder Data
- Post-Engagement Retesting and Environment Clean-Up

PCI Penetration Testing

DATA SHEET

PCI test results are provided in an extensive report containing:

- **Executive Summary:** describes major findings and remediation information
- **Statement of Scope:** systems tested as part of the engagement
- **Statement of Methodology:** details the method and tools used to complete testing
- **Statement of Limitation:** documents the restrictions imposed on testing
- **Testing Narrative:** details the testing method and documents testing progress
- **Segmentation Test Results:** summarizes test performance to validate segmentation controls
- **Severity Score Assignment:** scores each detected security issue high, medium, low, or informational
- **Retesting Report:** details efficacy of remediation efforts

Options:

Social Engineering: While the PCI DSS Penetration Testing Guidelines do not require social engineering, they do acknowledge social engineering as a way to determine effectiveness of a security awareness program. TraceSecurity offers social engineering as an optional service that can be performed in conjunction with the required penetration testing. If a social engineering engagement is performed as part of a PCI Penetration Test, the findings will be reported in accordance with the PCI DSS Penetration Report.

TraceSecurity Qualifications

Since 2004, TraceSecurity has performed nearly 10,000 penetration tests. TraceSecurity Information Security Analysts conducting assessments have between 5 and 20+ years of experience in the IT and security industry with credentials and professional experience including Certified Ethical Hacker (CEH), Offensive Security Certified Professional (OSCP), CISSP, CISM, CISA, CCNA, CCNP, CCIP, CCDA, CCNA Security, Security +, Linux+, MCSE: Security, MCITP, CWNA, CWSP, VCP, CEH, Network +, and they boast degrees in Computer Engineering, Information Systems, Computer Science, Business Administration, Electronics Engineering, and Information and Computer Science. Each is skilled and trained in the implementation and training of TraceSecurity products and the delivery of its security services.

Your Single Sources for a Full Range of IT Security Services

The complex and constantly evolving nature of security and compliance requires a range of experience and expertise that is nearly impossible for most companies to maintain internally. TraceSecurity's comprehensive suite of information security services is the answer. Our seasoned experts help enhance your security posture, reduce risk, facilitate compliance, and improve operational efficiency. To provide maximum effectiveness, the TraceSecurity information security services listed can be delivered in combination with TraceCSO, our integrated cloud-based IT GRC management platform.

- Vulnerability Assessment
- Risk Assessment
- IT Security Audit
- Penetration Testing
- Social Engineering
- Web Application Testing
- Wireless Assessment
- Security Training
- Advanced Persistent Threat Assessment