

External Penetration Test

Compliance Overview

IT Security Compliance regulations and guidelines (GLBA, FFIEC, FDIC, OCC, OTS) require an organization to conduct independent testing of the Information Security Program to identify vulnerabilities that could result in unauthorized disclosure, misuse, alteration, or destruction of confidential information, including Non-Public Personal Information (NPPI). Best Practices state that each organization should perform an External Penetration Test in addition to regular security assessments in order to ensure the security of their external network.

Solution Overview

Penetration testing is one of the oldest, most trusted methods used for assessing security risks because the process is designed to simulate a real-world attack using the tools and techniques employed by actual hackers. Therefore, the primary reason organizations will conduct a penetration test is to find and fix vulnerabilities before a criminal does. An External Penetration Test mimics the actions of an actual attacker without the usual dangers. This test examines external IT systems for any weakness that could be used by an external attacker to disrupt the confidentiality, availability, or integrity of the network, thereby allowing the organization to address each weakness.

TraceSecurity's External Penetration Test follows documented BestPractices security testing methodology including:

- External Port Scan
- External Network Vulnerability Scan
- Asset Classification Assistance
- External Network Vulnerability Review
 - False Positive reduction of scan data through manual 3rd Party review
- Exploit Testing and Penetration Attacking
 - Authentication Attacks
 - Vulnerability Exploitation
 - Privilege Escalation
 - Exploitation of Configuration Flaws
- Immediate Notification of Critical Risks
- Final deliverables deployed through TSCM

The external penetration test results are provided in an extensive report containing:

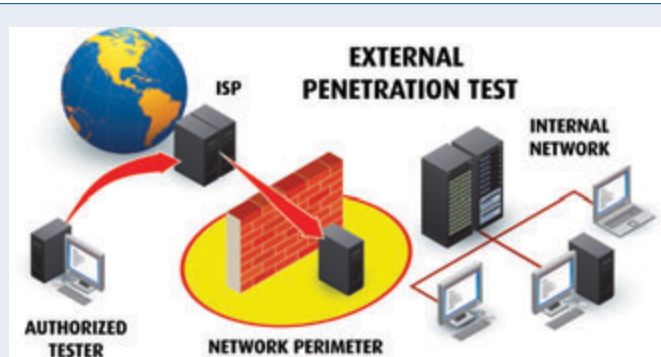
- Project Overview
- Penetration Test Methodology
- Executive Summary
- Business & Technical Risks and Recommendations
- Exploitation Results Listed by Risk and Areas of Concern
- Details and Exposure of Vulnerabilities
- Appendix

TraceSecurity's External Penetration Test includes on-demand access to the **TraceAssess** and **TraceReport** products of TraceCompliance Manager. TraceAssess provides on-demand vulnerability scanning of your network. TraceReport allows reports to be generated as needed for both executive level and technical staff.

The External Penetration Testing Process

Penetration testing (also referred to as “Pen Testing”) is the practice of testing a computer system, network or web application to determine if it is vulnerable to unauthorized access or other malicious activity. From the entire network down to single web application layers, penetration tests are designed to analyze and substantiate many facets of a computer system. The testing process employs methods used by real-world attackers which help determine the actual security weaknesses that may be exploited by an attacker in order to compromise the system and access protected information. The overall objective of penetration testing is to provide the organization a clear view of how vulnerable their systems are to a potential attack.

An external penetration is an iterative process that leverages minimal access to gain greater access. The test mimics the actions of an actual attacker exploiting weaknesses in the network security, but without the usual dangers that come with an actual attack. This test examines external IT systems (firewalls, web servers, online banking servers, e-mail servers, and any other externally available services) for any weakness that could be used by an external attacker to disrupt the confidentiality, integrity or the availability of the network. The process allows the organization to prioritize a plan of action and address each weakness individually.



To simulate an actual external attack, testers are given only minimal information about the targeted system. Prior to the attack, testers collect any usable information through publically accessible sources such as web pages or social networks. Then they use common tools like port scanners and vulnerability scanners to identify target hosts that can be reached from outside the network. At this point, the testers attempt to leverage this minimal access to create a widespread breach.

Business Benefits of Penetration Testing

- Avoid network downtime due to breach
- Provides a way to evaluate the effectiveness of security controls and countermeasures
- Helps identify the effectiveness of security awareness training
- Discover methods hackers could use to compromise customer/member data
- Helps organizations understand their security posture
- Provides information to support regulatory compliance
- Provides a strong basis for helping to determine appropriate security budgets

IT Benefits of Penetration Testing

- Allows staff to identify real and potential vulnerabilities without being overburden by numerous false positives
- Assists IT in prioritizing remediation for discovered vulnerabilities
- Helps verify the findings of the IT staff and track known vulnerabilities
- Enhances the effectiveness of an overall security lifecycle
- Demonstrate the feasibility of an attack and the impact of an attack without incurring the risk
- An effective way to test new technology and reconfigured systems before implementing them in a live environment

About TraceSecurity

TraceSecurity provides compliance and risk management solutions to organizations of all sizes that help them achieve, maintain and demonstrate security compliance while significantly improving their security posture. Over 1,000 organizations currently leverage our on-demand, web-based applications backed by expert professional services and analysis to address all critical components of their security compliance program, including people, process and technology.

TraceSecurity's, flagship **TraceSecurity Compliance Manager** is the first comprehensive software-as-a service platform to integrate and automate vulnerability assessment, vulnerability alerting, regulatory compliance audits, policy management and dissemination, file/URL integrity monitoring and employee education and testing.