

Internal Penetration Test

Solution Overview

The internal network (file servers, workstations, etc.) of the organization is exposed to threats such as external intruders breaching perimeter defenses or malicious insiders attempting to access or damage sensitive information or IT resources. In a 12-month period alone, more than 100 million personal records have been compromised due to security breaches. Almost 1/3 of these breaches were the result of hackers.

IT Security Compliance regulations and guidelines (GLBA, FFIEC, HIPAA, NCUA, FDIC ETC) 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 recommend that each organization perform an Internal Penetration Test in addition to regular Security Assessments in order to ensure the security of their internal network. An Internal Penetration Test differs from a vulnerability assessment in that it actually exploits the vulnerabilities to determine what information is actually exposed.

An Internal Penetration Test mimics the actions of an actual attacker exploiting weaknesses in network security without the usual dangers. This test examines internal IT systems for any weakness that could be used to disrupt the confidentiality, availability, or integrity of the network, thereby allowing the organization to address each weakness. TraceSecurity can perform this testing both onsite or remotely.

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

- **Scoping & Rules of Engagement**
- **Network Mapping**
 - Internal Network Scanning
 - System Fingerprinting
 - Services Probing
- **Analysis & Identification of Attack Vectors**
- **Exploit Testing and Penetration Attacking**
 - Authentication Attacks
 - Vulnerability Exploitation
 - Privilege Escalation
 - Exploitation of Configuration Flaws
- **Immediate Notification of Critical Risks**

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

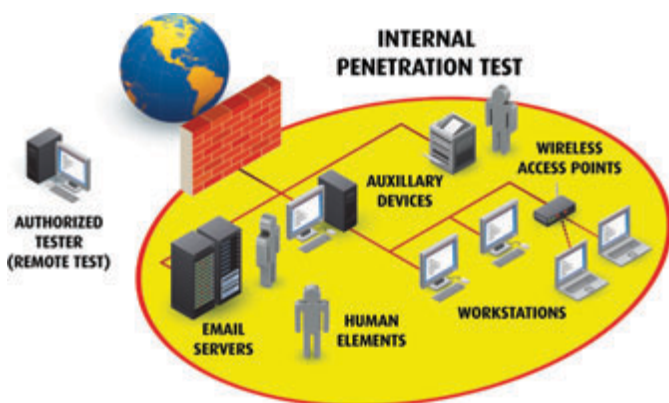
- **Project Overview**
- **Penetration Test Methodology**
- **Executive Summary**
- **Business & Technical Risks and Recommendations**
- **Exploitation Results Listed by Risk and Areas of Concern**
- **Details and Exposure of Vulnerabilities**
- **Appendix**

TraceSecurity's Internal Penetration Test also 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/board level and technical staff.

The Internal 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.

Internal penetration testing is performed to examine the internal IT systems behind the network perimeter (core processors, Active Directory servers, e-mail servers, etc.) for any weaknesses that could be exploited by an attacker. It is typically performed from within an organization’s technology environment, but may also be carried out remotely. This type of test usually mimics an attack originating from inside the company, perhaps from a disgruntled employee, an unauthorized visitor, or an external hacker who managed to get to the internal network via wireless access or by a successful external penetration test.



This test simulates an attack from behind the firewall. Testers are usually given a low level of access to the network and provided with the information that someone with the provided privileges would normally have. The tester then tries to gain a greater level through privilege escalation.

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 overburdened 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.