



INTERNET
SECURITY
SYSTEMS™

Penetration Tests: The Baseline For Effective Information Protection

What is a Penetration Test?

A penetration test offers an invaluable and compelling way to establish a baseline assessment of security as seen from outside the boundaries the organization's network. Properly executed penetration tests provide evidence that vulnerabilities do exist and that network penetrations are possible. More importantly, they provide a blueprint for remediation in order to start or enhance a comprehensive information protection strategy.

A penetration test simulates covert and hostile network attack activities in order to identify specific exploitable vulnerabilities and to expose potential entryways to vital or sensitive data that, if discovered and misused by a malicious individual, could pose increased risk and liability to the organization, its executives and shareholders. Qualified security consultants who perform penetration tests attempt to gain access to online assets and company resources through the network, servers and desktops, from either the internal or external perspective, much like an intruder would. These results clearly articulate security issues and recommendations and create a compelling event for the entire management team to support a security program.

Reasons to Get a Penetration Test

- **Provides a Good Starting Point.** Many organizations underestimate how wide open their security exposure is, and overestimate the capacity and resources their internal IT staff can utilize to address it. A penetration test provides a good first step to understanding current security posture specifically because it identifies gaps in security, and outlines where to apply security technologies and services so that the organization can develop an action plan to minimize the threat of attack or misuse.
- **Creates a Compelling Event.** How can network administrators and security managers justify a needed increase in the security budget or make the security message heard at the executive level? Well-documented results from a penetration test that expose the susceptibility of customer data, human resources records or even executive e-mail accounts create compelling events that any executive concerned with company finances, liability or reputation needs to know.
- **Performs Due Diligence and Independent Audits.** Security posture needs to be examined on a regular basis to account for the evolution of new Internet threats. An unbiased security analysis and penetration test can focus internal security resources where they are needed most. In addition, an independent security audit provides evidence of due diligence in a legal context for protecting online assets, limiting C-level liability and/or minimizing potential loss of shareholder value. These independent audits are rapidly becoming a requirement for obtaining cyber-security insurance.
- **Meets Regulatory Requirements.** Regulatory and legislative requirements are making penetration tests required as a necessity of doing business. Regulations such as HIPAA (Health Insurance Portability and Accountability Act), OCC Bulletin 2014, and Graham Leach Bliley all include security compliance codes.
- **Protects Against Inter-Connected Partner Risk.** Online commerce initiatives require organizations to grant partners, suppliers, B2B exchanges, customers and other trusted connections into their networks. The entire structure is only as strong as its weakest link. Any poorly secured system, left unchecked, poses dangerous security risks for everyone else. Many organizations are now requiring that their security vendor provide security audits of partners to ensure that all connected entities have a standard baseline for security.
- **Offers validation.** As organizations adapt to new business models and technologies, a penetration test provides validation between business initiatives and a security framework that allows for successful implementation at minimal risk. In other words, after an organization establishes its security practices and believes that its infrastructure is secure, a penetration test provides critical validation feedback.

Requirements for a Successful Penetration Test

Penetration tests require certain key elements to be in place in order to ensure useful, timely results. First, they must cover the full range of the threat spectrum, from the presence of an antivirus engine to the presence of malicious code to vulnerabilities that might enable denial of service and other sophisticated attacks. Second, they must deliver clear, unambiguous results that address both the technical and business objectives of the client. Third, the consultants who perform the tests must follow robust testing methodologies, use software that carries the most up-to-date vulnerability research available, and they must possess creative instincts to manipulate the tools in both typical and unconventional ways. Finally, the experienced technicians who administer the penetration tests must know how to gain maximum results with minimal disruption to normal business operations.

What to Look for in a Penetration Testing Service Provider

Many companies offer penetration testing services, but the best choice is a provider who offers focus on the entire threat spectrum, including highly researched vulnerability and threat intellectual capital and tools. Look for a robust penetration testing methodology, preferably one that provides a multi-layer approach that identifies and leverages small cracks that springboard into identifying major cracks not found by typical security tools. Make sure the final deliverable report provides business value, as security recommendations should be based on the client's business objectives and the appropriateness of security measures per exposure. Lastly, use a provider that has a proven track record of finding known and new threats and whose recommendations provide a holistic approach to security.

A final note: reconsider before using a penetration testing service provider who merely runs a security audit or scanning tool and delivers a report on that one tool's results. While an individual tool provides some value as a standalone assessment device, it can never replace the human mind to creatively apply new methods and techniques to break and bypass standard security systems, much like an intruder would.

ISS X-Force™ Penetration Testing Service

Internet Security Systems introduced the *Internet Scanner*™ application, the industry's first penetration testing solution, in 1994. Today, ISS' *X-Force*™ **Penetration Testing Service** provides the premier attack simulation and analysis service available. This powerful combination of ISS' X-Force security intelligence, research and development and ISS' highly experienced, business-driven consultants provides customers with the timely, accurate testing and reporting they need to make knowledgeable information protection decisions. For more information about the X-Force Penetration Testing Service, contact ISS at 1-404-236-3971, or e-mail consulting@iss.net.

Conclusion

A penetration test from a trusted provider offers an excellent means by which an organization can baseline its current security posture, identify threats and weaknesses, and start implementing remediation strategies. By identifying risk exposures and highlighting what resources are needed to correct them, penetration tests provide not only the basis for a security action plan, but also the compelling events, due diligence and partner interface protocols necessary to establish information security as a key corporate initiative.

About Internet Security Systems (ISS)

Founded in 1994, Internet Security Systems (ISS) (Nasdaq: ISSX) is a world leader in software and services that protect critical online resources from attack and misuse. ISS is headquartered in Atlanta, GA, with additional operations throughout the United States and in Asia, Australia, Europe, Latin America and the Middle East.

Copyright © 2001, Internet Security Systems, Inc. All rights reserved worldwide.

Internet Security Systems, the Internet Security Systems logo, X-Force and Internet Scanner are trademarks of Internet Security Systems, Inc. Other marks and trade names mentioned are marks and names of their owners as indicated. All marks are the property of their respective owners and used in an editorial context without intent of infringement. Specifications and content are subject to change without notice.