INTERNET SECURITY SYSTEMS™

X-Force™ Professional Security Services

6303 Barfield Road
Atlanta, GA 30328

Tel: 404.236.3971
Email: consulting@iss.net
www.iss.net

X-Force™ Penetration Test

Description

Internet Security Systems X-Force™ Penetration Test is a controlled network attack simulation that provides a snapshot of an organization's security posture as seen from a designated location, typically external. The result is the identification and documentation of specific exploitable vulnerabilities and risks within the organization's network. Analysis of these exposures provides an understanding of the organization's network security posture and validation of the need for an effective information security program.

An elite team of ISS security experts draws upon our world-renowned intellectual capital, best of breed tools and extensive field experience to perform Penetration Tests. The results identify exposures that could be used by a malicious individual to infiltrate an organization's network.

Benefits

- Provides an overview of existing and relevant exposures with detailed analysis of how these vulnerabilities could lead to ingress and exploitation of an organization's systems.
- Tests and validates the effectiveness of security safeguards and controls currently in place.
- Demonstrates the existing risks to an organization's networks and systems.
- Justifies and enables a security program by raising awareness about corporate liability at all levels of the organization.
- Details unauthorized data and server access using step-by-step descriptions.
- Provides detailed remediation steps that can be taken to prevent future exploitation.

Features

- Provides an analysis of an organization's network security as seen from a designated location, typically an external/Internet location.
- Performed by ISS security experts armed with the latest security tools, techniques and ISS X-Force™ intellectual capital to simulate covert and hostile activities typical of malicious attackers in an attempt to compromise perimeter devices and security controls.
- Uses access and information obtained during the perimeter analysis to attempt compromise of DMZ and internal systems.
- Provides documentation, explanation and analysis of the simulated attacks, including screen shots, details of the route(s) taken and the likelihood of an attacker to use that same approach.
- Prioritizes the discovered risks and defines immediate actionable items to correct them.

Penetration Test Offerings

ISS offers the following options for Penetration Testing Services:

- **Perimeter Penetration Test-** From a remote location, ISS uses typical hacker tools and techniques in an attempt to defeat the firewall and other perimeter security devices.
- **Perimeter Test plus Remote Exploitation-** ISS security professionals conduct a Perimeter Penetration Test, then use the information obtained in an attempt to compromise DMZ and other internal systems. This test provides an organization with the ability to see how the DMZ can be leveraged to access data and systems on their internal network.
- **On-site Internal Penetration Test-** ISS conducts this test from within an organization's internal network and simulates the activities of a hostile insider. The results can be used to gauge the exposure present on an internal network.

Standard Methodology

ISS utilizes the same tools and techniques a malicious attacker would use, along with proprietary ISS technology and intellectual capital, to determine whether and how an attacker could penetrate a network and systems. ISS' Penetration Testing includes:

- **Project Initiation-** defines rules of engagement and a project plan to ensure that scope, expectations, timelines and deliverables are appropriately managed.
- **Reconnaissance and Baselining-** baseline testing of the target network and systems to determine what hosts and services are active.
- **Perimeter Testing-** exploitation attempts to identify key vulnerabilities on perimeter systems.
- **Remote Exploitation-** uses the access and information acquired during the perimeter testing to attempt to compromise DMZ and internal systems.
- **Data and Intelligence Gathering-** collects and prioritizes data from the target systems and networks as obtained via exploitation.
- **Analyze Findings and Prepare Deliverable-** analyzes the results and prepares a concise, detailed technical and management report.

Deliverable

ISS presents a final deliverable detailing the each phase of the methodology, each test conducted and its corresponding results. The deliverable includes an overall evaluation and assessment of the organization's security posture and recommends strategies to minimize the identified risks.

Comprehensive Security Solution Recommendations

For a complete assessment and analysis of an organization's security posture, Internet Security Systems recommends combining a Penetration Test with an X-Force™ Information Security Assessment. This service offers a comprehensive evaluation of a company's information security posture. When combined, the Information Security Assessment and Penetration Test provide a thorough examination of an organization's security posture from both a holistic and practical approach.

Get Started Today

Get started today and take advantage of ISS' X-Force™ Penetration Testing Service. Call 404-236-3971, e-mail consulting@iss.net, or visit our Web site at www.iss.net.

About 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.