

{ External Vulnerability/Exploitation Assessment }

Hackers are interested in everything. Some break into systems for fun. Some do it for profit. Others will simply use hacked machines for purposes that suit them, such as to launch attacks against other systems that may or may not belong to the same organization.

An External Vulnerability/Exploitation Assessment is a comprehensive examination of an Internet access point to identify security vulnerabilities, evaluate their seriousness, and communicate the risk to the customer in order to help them reduce the threats presented by hackers. igxglobal security analysts mimic the actions of a remote intruder or hacker, and attempt to identify vulnerabilities and gain unauthorized access to system data and resources.

igxglobal's External Vulnerability/Exploitation Assessment focuses on finding security flaws in an organization's network perimeter that may lead to eventual penetration, data destruction, website defacement, or just simple disruption of services. Any one of these events may lead to irrecoverable damage to a company's reputation in the eyes of its customers, potential losses in revenue, and higher costs. Upon completion of the External Vulnerability/Exploitation

Assessment, a report is provided that details the discovered security vulnerabilities, why the vulnerabilities are dangerous, and recommended countermeasures. This penetration test satisfies many regulatory requirements for an independent security assessment regarding Internet access connectivity.

igxglobal has been a focused provider of security services, such as the audit and assessment practices and compliance GAP analysis (HIPAA, GLBA, etc.), since 2000. In 2006, igxglobal, Inc. was approved by Visa and the Payment Card Industry as a certified PCI Data Security assessor. igxglobal's staff consists of experienced Information Security professionals who can simulate the latest attacks and techniques used by hackers, in order to provide a realistic test of your systems.



SECURITY OPERATIONS



THREAT MITIGATION



SECURITY TECHNOLOGIES



PROFESSIONAL SERVICES



EXTERNAL VULNERABILITY/EXPLOITATION ASSESSMENT

igxglobal's External/Vulnerability/Exploitation Assessment employs a variety of data gathering and perimeter scanning techniques in order to develop a sound assessment of a company's security posture. igxglobal conduct the review in these stages:

- **Fingerprinting**
The systematic identification of a client to create a complete profile of the organization. Process determines the ease of identifying the client's Internet access point, includes collection of information from public sources, and allows for the identification of potential social engineering avenues.
- **Identify Accessible Hosts, Services and Applications**
Identification of all accessible hosts available from an Internet access point and their associated services and applications.
- **Vulnerability Scan**
Identification of vulnerabilities using both public and proprietary techniques. Discovered vulnerabilities are correlated to determine if a combination of vulnerabilities will result in a larger exploit.
- **Exploitation**
This step goes beyond a simple identification and validation of vulnerabilities. Attempts to exploit discovered vulnerabilities and gain access to data residing within the client's network are made. This step allows for a true understanding of the exposure faced and the amount of damage that could occur.
- **Application Testing**
The testing of Internet accessible applications to validate the security of the applications. This testing utilizes techniques such as verifying authentication, SQL injection, etc.
- **Perimeter Security Review**
A review of router, firewall, and host configuration files and network diagrams in order to detect possible security holes not necessarily found with vulnerability scanners.

Upon completion of the External Vulnerability/Exploitation Assessment, a report is provided that details the following:

- A summary report of all data collected with sources documented
- Summary of what information needs to be protected and the implications if it is damaged or lost
- Summary of security measures in place and their effectiveness
- Discovered vulnerabilities and their risks
- Exploitation guide detailing what systems were exploited, what data was recovered, and how exploitation was performed
- Countermeasures for mitigating the vulnerabilities and where appropriate cost associated with mitigating said risks