



I'm Secure... Are You?

Network Vulnerability Assessment

As both the frequency and ingenuity of electronic attacks increase, so does the need to regularly test the effectiveness of your information security controls. Theft of confidential data, such as client financial information and corporate secrets are no longer the sole objective of hackers as web site defacement now provides malicious individuals with a mechanism to degrade the public image of your institution. Network vulnerability assessment remains a powerful tool to identify the vulnerabilities that may exist within your security architecture and gives you the opportunity to fix them before they are exploited.

Identifying Vulnerabilities

Vulnerability testing is like looking for unlocked doors and windows in a building, which represents an essential first step in any security testing strategy.

Our consultants use a proven combination of industry tools and in-house techniques to thoroughly probe and identify vulnerabilities in your Internet-facing IT systems.

And, unlike automated services that typically provide a computer-generated list of every vulnerability that exists on a web or email server, we'll prioritize those that are relevant to your infrastructure and include pragmatic advice on how to overcome them.

Opening the Doors & Windows

Our next level of service goes further by exploiting the weaknesses we've identified and simulating an actual attack. Using the same techniques as actual hackers, our specialists will conduct activities such as information gathering, network fingerprinting and attempting to bypass access controls.

And, with one of the most experienced and respected penetration testing teams, we're able to comprehensively check all operating platforms as well as investigate areas such as cross-site scripting, code hacking problems, SQL database injection, XML and web services.

The Threat from Within

Acknowledging that a significant proportion of malicious attacks originate from within an organization, our most comprehensive level of service employs advanced testing techniques internally as well as remotely.

In fact, some reports indicate that over 70% of hacking takes place internally. Most "think" that their networks are secure. Some "hope" they are based on what their vendors sold or promised them. Very few "know" they are and can prove it. Can you be 100% sure that your network resources are secure?

Our consultants will review your security architecture to identify potential flaws that would afford a knowledgeable intruder access. We will also review software builds on servers, examine web application scripts or check compliance to internal security policies.

DataComm's security consultants will work with your IT staff to simulate Denial of Service attacks, test your responses - by both systems and people - to intrusion efforts, attempt access to wireless networks or use social engineering techniques to identify non-technical points of entry into your organization and its assets.

Regardless of the size of an engagement, though, we'll always develop a comprehensive report detailing the issues we have identified, an explanation of their implications and recommendations for either reducing or eliminating the risks they pose.

All A's

DataComm certified security consultants deploy the "All A's" testing methodology when performing a network penetration test:

Analyze, Assess, and Appraise

During the first phase of a penetration test,

In Depth
No Hassle
From \$995



DataComm's security technicians **analyze** and look for vulnerable devices on your network and determine the types of tests to be performed on the devices.

The second phase of the penetration test consists of an **assessment** of the devices identified in the first phase by thoroughly testing their vulnerabilities.

The final and most important phase in the penetration test consists of the technician **appraising** the security of your network by generating a detailed report of all vulnerabilities that were discovered and solutions to correct them. To make sure that the report is understood in its entirety and all solutions are properly implemented, a follow-up call will be scheduled between the technician that performed the test and selected members of your management and IT staff.

For more information contact Sales.

sales@dcninc.com

800.544.4627

Service Specifications

Note: DataComm's customers are examined by federal and state bodies every year.

Stricter government mandates such as Sarbanes-Oxley and the Gramm-Leach-Bliley Act, along with a dynamic and complex operating environment are forcing organizations to improve the security of business-critical systems and data. Compliance with regulations, the acceleration of potential threats, and a growing remote and mobile workforce are challenging organizations to examine their ability to discover vulnerabilities and take measures to counter them. DataComm's Vulnerability Assessment Services, securSCANSM, combines proven experience and sophisticated technology to ensure vulnerabilities are identified, analyzed and managed effectively, to minimize risk and maximize business results.

DataComm offers ongoing penetration testing where we'll conduct regular, repeat testing of your infrastructure using a pre-agreed program of test levels. The table to the right illustrates our recommended schedule for institutions using the Internet for, say, marketing or promotional purposes as well as those making more extensive use of the web for activities such as the selling or purchasing of products.

Our testing teams are also equipped with specialized tools to provide wireless testing services. This can help you detect rogue Access Points or "sniffer" equipment that may be attempting to gain unauthorized access to your IT systems.

Summary of Test Levels and Recommended Schedule for Annual Testing Service

Level of Testing Performed	Internet Presence Environment	Internet eCommerce Environment
Remote Vulnerability Testing	Every 3 Months	Every Month
External Penetration Testing	Every 6 Months	Every 3 Months
Full Assessment Including External and Internal Penetration Testing	Every 12 Months	Every 6 Months

Feature	Benefit
Why DataComm?	
Security Expertise	Our elite team of security experts is comprised of senior security professionals who have honed their skills through corporate security leadership, security consulting, investigative branches of the government, research and development.
Staff Costs Savings	DataComm offers the experience and skills of its Professional Security Services team to the customer for less than the cost of hiring a single in-house security expert.
Trusted Partnership	We partner with your key staff and management to design a customized plan that meets your organization's security goals.
Specialized Skills and Tools	Our consultants combine proprietary and industry leading security assessment tools with in-depth analysis of vulnerability data to evaluate and build an effective security program that enhances your business operations.
Business Driven Approach	Detailed analysis of business needs, drivers and the existing environment identifies the business critical areas to ensure maximum protection for business-critical operations, provide the most cost-effective use of technology and resources and allow clients to focus on core business functions.
Part of an Integrated Portfolio	Vulnerability Assessment Services are part of a fully integrated end-to-end security solution that provide end-to-end continuity of service and accountability, proactive identification of vulnerabilities in your environment and integration with security and response and remediation services enabling increased control of risk.
Deliverable	
A Management Summary	Listing areas of weakness within the installed applications and their respective business impacts.
Assessment Overview	Details the scope and objectives of the project undertaken, and the methodology utilized by the DataComm Consultants.
Technical Findings	Details any security vulnerabilities discovered during the testing process, and provides detailed explanations of all their security implications. Comprehensive remediation information will be supplied including alternatives should the preferable solution be impractical.
Conclusions	Details managerial and technical recommendations to the client, with a view to mitigating short-term risks, as well as long term strategic solutions.
Exploit Code	Where applicable DataComm will provide the unique service of providing clients with demonstration exploit code.
Additional Recommendations	Where the client is unable to patch any affected products, or the cost of doing so is prohibitive, DataComm Consultants will provide a range of recommendations to mitigate any vulnerabilities discovered during the testing process.

FAST FACTS

- Comprehensive testing of networks, servers, applications and databases
- Detailed reports including solution recommendations
- Annual service option with pre-defined testing schedule
- One of the most experienced and respected penetration testing teams
- Enables clients to focus on core business functions
- Analysis of latest threats counteract the ever-evolving hacker community
- Meets Federal Regulatory Requirements (GLB, SOX, HIPAA)



DataComm Networks, Inc.

6801 North 54th Street

Tampa, Florida 33610

813.873.0674

800.544.4627

www.dcninc.com

sales@dcninc.com