

Vulnerability Assessments / Penetration Testing

“Evaluate your security controls the same way the hackers do.”

“What is the real cost of a security breach to your organization’s reputation”



Don't know if your network is secure? You're not alone.

Securing your environment is a perpetual process that affects every aspect of your organization. Whether it's maintaining the physical security of a data center, keeping your user community informed of threats and their responsibilities, ensuring IT systems are up-to-date, or maintaining regulatory compliance (i.e., NERC CIP), your job as a security manager sees no end. One of the leading causes of a vulnerable IT environment is having systems that are unpatched or misconfigured. In theory, rigorous patch management and system hardening programs should address these concerns. In reality, these programs can miss systems, and users may be introducing new vulnerabilities on a daily basis. As such, it may be difficult to maintain confidence in the state of security in your IT environment due to the inherently fluid nature of information technology.

Security Assessments

With a Vulnerability Assessment, Network & Security Technologies gives you a snapshot of your current state of security either across the organization, or in a specific area of need.

- Are you concerned that due to expansion your Internet-facing environment may be vulnerable to attack? Allow us to conduct an External Vulnerability Assessment where we gather information on your environment, identify services available to the Internet, then check, verify, and validate vulnerabilities associated with those services.
- Are you concerned that the possibility of easy access to critical information within your organization could lead to the theft of proprietary data or the unavailability of critical systems? Allow Network & Security Technologies to conduct an Internal Vulnerability Assessment which can include:
 - Technical Security Assessment – Attempting to collect information by technical means such as scanning systems, attempting to guess easy passwords, or collecting information while listening on the network.
 - Social Engineering – Attempting to collect information through non-technical means such as sifting through trash bins, watching employees while they're on their computers, utilizing manufactured emails and websites, or fraudulent phone calls to the help desk.
 - Physical Security Assessment – Attempting to enter restricted areas by taking advantage of improper procedures by personnel, or improper use of physical security technology.
 - Process and Procedure Review – A review of security processes and procedures used in the day-to-day administration of security within your organization. This can be unobtrusive if there is sufficient documentation or may require interviews with staff if the processes and procedures are informal.
- Are you concerned that an internal or external application may not be protecting customer information? Allow us to conduct an Application Test where we use one set of user credentials to attempt to access information meant for other users.

Our passion for technical excellence and commitment to our clients' business success results in practical solutions to complex problems

Contact Us:

Network & Security Technologies
161 North Middletown Road
Pearl River, NY 10965

Phone:
(845) 620-9500

Fax:
(845) 620-1525

E-mail:
info@netsectech.com

URL:
www.netsectech.com

Penetration Testing

Simply having a vulnerable system or environment does not necessarily mean that you are at high risk. A threat must exist to exploit the vulnerability for an actual loss to be seen. Network & Security Technologies can simulate this threat through a Penetration Test, either externally over the Internet or internally on your corporate network. If your primary business function is Internet-based transactions then Network & Security Technologies can pose as a hacker on the Internet. If your primary business asset is information or situational awareness then a scenario simulating a disgruntled or malicious employee may be more appropriate. The purpose of the Penetration Test is to attempt to compromise critical systems or to collect critical information that is supposed to be off limits to general users, and then use that access or information to compromise other systems.

Assessment Process

Network & Security Technologies has a rigorous assessment process that ensures completeness while limiting the potential impact on production systems.

Gathering information about network addresses, telephone number ranges, network topology, processes and any relevant technology made publicly available.

Perform testing using commercial, public domain, and Network & Security Technologies proprietary techniques and tools.

Analyze and quantify the risk posed by the vulnerabilities identified in terms of both likelihood and impact.

Produce a plan for reducing the risk to an acceptable residual through actionable recommendations.

Network & Security Technologies experts possess the experience and expertise to evaluate a wide range of vendors and products. Clients utilizing novel or proprietary solutions can rely on Network & Security Technologies consultants to have the expertise in secure product development to analyze unique software and identify weaknesses.

Delivering Prioritized Actions and Peace of Mind

The output of the assessment is a report that permits the IT manager and business executive to understand the probable impact of the vulnerabilities in their technology and processes, as well as the likelihood that the vulnerability will be exploited by an attack. Our clients are given prioritized action plans for the remediation of high impact threats and vulnerabilities; resulting in secure networks and peace of mind.

Thorough, Experienced, Effective

By turning to Network & Security Technologies for Vulnerability Assessments and Penetration Testing, you can ensure the smooth and safe operation of your organization's infrastructure. Network & Security Technologies prides itself on delivering its projects on-time and on-budget using skilled resources. All N&ST consultants are full-time employees with many years of computer networking and cyber security experience. Our projects are carefully managed to ensure complete client satisfaction within the quoted timeframe and price. Our consultants will respond immediately to your request while providing world class technology and security consulting expertise. And, we will work hard to make sure your secure infrastructure is not just a theory.

