November 2003

ITL Bulletin

ADVISING USERS ON INFORMATION TECHNOLOGY

NETWORK SECURITY TESTING

Shirley M. Radack, Editor, Computer Security Division, Information Technology Laboratory, National Institute of Standards and Technology

Securing and operating today's complex systems is challenging and demanding. Mission and operational requirements to deliver services and applications swiftly and securely have never been greater. Organizations, having invested precious resources and scarce skills in various necessary security efforts such as risk analysis, certification, accreditation, security architectures, policy development, and other security efforts, can be tempted to neglect or insufficiently develop a comprehensive and systematic operational security testing program.

This guide stresses the need for an effective security testing program within federal agencies. Testing serves several purposes. One, no matter how well a given system may have been developed, the nature of today's complex systems with large volumes of code, complex internal interactions, interoperability with external components, unknown interdependencies coupled with vendor cost and schedule pressures, means that exploitable flaws will always be present and will surface over time. Accordingly, security testing must fill the gap between the state of system development as it is and actual operation of these systems. Two, security testing is important for understanding, calibrating, and documenting the operational security posture of an organization. Aside from development of these systems, the operational and security demands must be met in a fast-changing threat and vulnerability environment. Attempting to learn and repair the state of your security during a major attack, for example, may be too late as the damage in cost and reputation could be extremely high. Three, security testing is an essential component of improving the security posture of your organization overall. Organizations that have a systematic, comprehensive, ongoing, and priority-driven security testing regimen are in a much better position to make prudent investments to enhance the security posture of their systems.

NIST Guideline on Network Security Testing

NIST recently issued Special Publication (SP) 800-42, *Guideline on Network Security Testing*, to assist organizations in testing their Internet-connected and operational systems. The guide provides an approach to adopting effective procedures that can help organizations uncover unknown vulnerabilities, institute security controls, and prevent incidents and attacks. Written by John Wack, Miles Tracy, and Murugiah Souppaya, NIST SP 800-42 introduces three aspects of network security testing:

- How network security testing fits into the system development life cycle and the organizational roles and responsibilities related to security testing,
- Available testing techniques, their strengths and weaknesses, and the recommended frequencies for testing, and
- Strategies for deploying network security testing, including how to prioritize testing activities when resources are limited and how to avoid duplication of effort in adopting techniques that are appropriate to the organization's mission and security objectives.

In addition to the basic information about establishing programs to implement network security testing, the guideline provides references, explanations of the terminology used, descriptions of available testing tools, and recommendations on how to use selected tools.

Continued on page 2

ITL Bulletins are published by the Information Technology Laboratory (ITL) of the National Institute of Standards and Technology (NIST). Each bulletin presents an in-depth discussion of a single topic of significant interest to the information systems community. **Bulletins are issued on an as-needed basis** and are available from ITL Publications, National Institute of Standards and Technology, 100 Bureau Drive, Stop 8901, Gaithersburg, MD 20899-8901, telephone (301) 975-2832. To be placed on a mailing list to receive future bulletins, send your name, organization, and business address to this office. You will be placed on this mailing list only.

Bulletins issued since July 2002

- *Overview: The Government Smart Card Interoperability Specification,* July 2002
- *Cryptographic Standards and Guidelines: A Status Report*, September 2002
- *Security Patches and the CVE Vulnerability Naming Scheme: Tools to Address Computer System Vulnerabilities*, October 2002
- *Security for Telecommuting and Broadband Communications*, November 2002
- *Security of Public Web Servers*, December 2002
- *Security of Electronic Mail*, January 2003
- *Secure Interconnections for Information Technology Systems*, February 2003
- *Security for Wireless Networks and Devices*, March 2003
- *ASSET: Security Assessment Tool for Federal Agencies*, June 2003
- *Testing Intrusion Detection Systems*, July 2003
- *IT Security Metrics*, August 2003
- *Information Technology Security Awareness, Training, Education, and Certification*, October 2003

This ITL bulletin summarizes the publication, which is available at http://csrc.nist.gov/publications/nistpubs/index.html.

Security Testing and the System Development Life Cycle

Organizations should evaluate their systems security at different stages of system development. Security evaluation activities include, but are not limited to, risk assessment, certification and accreditation (C&A), system audits, and security testing at appropriate periods during a system's life cycle. These activities are directed toward ensuring that the system is being developed and operated in accordance with the organization's security policy.

The Security Test and Evaluation (ST&E) process is an examination or analysis of the protective measures that are placed on an information system once it is fully integrated and operational. The process will help to uncover design, implementation, and operational flaws, determine the adequacy of security mechanisms, and assess whether the system is implemented as documented. ST&E addresses computer security, communications security, emanations security, physical security, personnel security, administrative security, and operations security.

Network security testing is conducted after the system has been developed, installed, and integrated during its Implementation and Operational stages. The results of testing can help to identify vulnerabilities, demonstrate progress in meeting security requirements, and indicate needs for system improvement. Therefore, security testing provides information for other system development life cycle activities such as risk analysis and contingency planning. Security testing results should be made available for staff members involved in other information technology and security-related areas.

ITL Bulletins Via E-Mail
We now offer the option of delivering your ITL Bulletins in ASCII format directly to your e-mail address. To subscribe to this service, send an e-mail message from your business e-mail account to listproc@nist.gov with the message **subscribe itl-bulletin**, and your name, e.g., John Doe. For instructions on using listproc, send a message to listproc@nist.gov with the message **HELP**. To have the bulletin sent to an e-mail address other than the From address, contact the ITL editor at 301-975-2832 or elizabeth.lennon@nist.gov.

Tools for Network Security Testing

Network security testing should be conducted on a regular basis while systems are running in their operational environments to provide information about the integrity of an organization's networks and associated systems. Some testing techniques are predominantly manual, requiring an individual to initiate and conduct the test. Other tests are highly automated and require less human involvement. The staff members who set up and conduct the security testing activities must have solid security and networking knowledge.

Testing techniques are available for network mapping, vulnerability scanning, password cracking, penetration testing, war dialing, war driving, file integrity checking, and virus scanning. Often, several of these testing techniques are used together to gain a more comprehensive assessment of the overall status of network security. For example, penetration testing usually includes network scanning and vulnerability scanning to identify vulnerable hosts and services that may be targeted for later penetration. Some vulnerability scanners incorporate password cracking. None of the tests by themselves will provide a complete picture of the network or its security posture. After tests are completed, all test results should be documented, and system owners should be informed of the results to ensure that vulnerabilities are patched or mitigated.

Several techniques for network testing are introduced in SP 800-42. Table 1 summarizes the types of testing and the strengths and weaknesses of each test technique.

Table 2 summarizes the baseline frequencies for running the tests.

Deployment Strategies

The goal of security testing is to maximize the benefit to the organization as a whole. The guideline recommends that organizations adopt consistent approaches to network security testing, using levels of security testing that are appropriate to organizational missions and security objectives.

The types and frequency of testing during the operational and maintenance phase (both for minimum and comprehensive testing) should be ranked according to a priority order, based on the security category, cost of conducting the tests, and the expected overall benefits to the organization's systems. The decision about what to test for during the implementation phase normally involves a single system. The same decision during the operational and maintenance phase becomes more complicated because of internal and external connections. To maximize the value of testing, the prioritization process should consider the interconnectivity of systems. Senior managers should be involved in the prioritization process to ensure that the organizational perspective is considered.

The basic steps that organizations should take in developing a priority ranking for their network testing activities include:

- Determine the security category for the organization's information systems. Federal Information Processing Standards (FIPS) 199, *Standards for Security Categorization of Federal Information and Information Systems*, covers this important step. It defines three levels of potential impact on organizations (or on individuals) should certain adverse events occur. These are events that could jeopardize the information systems needed by the organization to accomplish its assigned mission, protect its assets, fulfill its legal responsibilities, maintain its day-to-day functions, and protect individuals. Security categories are to be used in conjunction with vulnerability and threat information to assess the risk that an organization incurs when operating an information system. FIPS 199 is available as a pre-publication final document at http://csrc.nist.gov/publications.

Table 1

Type of Test	Strengths	Weaknesses
Network Scanning	• Fast (as compared to vulnerability scanners or penetration testing) • Efficiently scans hosts, depending on number of hosts in network • Many excellent freeware tools available • Highly automated (for scanning component) • Low cost	• Does not directly identify known vulnerabilities (although will identify commonly use Trojan ports [e.g., 31337, 12345, etc.]) • Generally used as a prelude to penetration testing not as final test • Requires significant expertise to interpret results
Vulnerability Scanning	• Can be fairly fast depending on number of hosts scanned • Some freeware tools available • Highly automated (for scanning) • Identifies known vulnerabilities • Often provides advice on mitigating discovered vulnerabilities • High cost (commercial scanners) to low (freeware scanners) • Easy to run on a regular basis	• Has high false positive rate • Generates large amount of traffic aimed at a specific host (which can cause the host to crash or lead to a temporary denial of service) • Not stealthy (e.g., easily detected by IDS, firewall and even end-users [although this may be useful in testing the response of staff and altering mechanisms]) • Can be dangerous in the hands of a novice (particularly DoS attacks) • Often misses latest vulnerabilities • Identifies only surface vulnerabilities
Penetration Testing	• Tests network using the methodologies and tools that attackers employ • Verifies vulnerabilities • Goes beyond surface vulnerabilities and demonstrates how these vulnerabilities can be exploited iteratively to gain greater access • Demonstrates that vulnerabilities are not purely theoretical • Can provide the realism and evidence needed to address security issues • Social engineering allows for testing of procedures and the human element network security	• Requires great expertise • Very labor intensive • Slow, target hosts may take hours/days to “crack” • Due to time required not all hosts on medium or large sized networks will be tested individually • Dangerous when conducted by inexperienced testers • Certain tools and techniques may be banned or controlled by agency regulations (e.g., network sniffers, password crackers, etc.) • Expensive • Can be organizationally disruptive
Password Cracking	• Quickly identifies weak passwords • Provides clear demonstration of password strength or weakness • Easily implemented • Low cost	• Potential for abuse • Certain organizations restrict use
Log Reviews	• Provides excellent information • Only data source that provides historical information	• Cumbersome to manually review • May filter out important information
File Integrity Checkers	• Reliable method of determining whether a host has been compromised • Highly automated • Low cost	• Does not detect any compromise prior to installation • Checksums need to be updated when system is updated • Checksums need to be protected (e.g., read only CD-Rom) because they provide no protection if they can be modified by an attacker
Virus Detectors	• Excellent at preventing and removing viruses • Low/Medium cost	• Require constant updates to be effective • Some false positive issues • Ability to react to new, fast replicating viruses is often limited
War Dialing	• Effective way to identify unauthorized modems	• Legal and regulatory issues especially if using public switched network • Slow
War Driving	• Effective way to identify unauthorized wireless access points	• Possible legal issues if other organization’s signals are intercepted • Requires some expertise in computing, wireless networking and radio engineering

Table 2

Test Type	Category 1 Frequency	Category 2 Frequency	Benefit
Network Scanning	Continuously to Quarterly	Semi-Annually	• Enumerates the network structure and determines the set of active hosts, and associated software • Identifies unauthorized hosts connected to a network • Identifies open ports • Identifies unauthorized services
Vulnerability Scanning	Quarterly or bi-monthly (more often for certain high risk systems), when the vulnerability database is updated	Semi-Annually	• Enumerates the network structure and determines the set of active hosts, and associated software • Identifies a target set of computers to focus vulnerability analysis • Identifies potential vulnerabilities on the target set • Validates that operating systems and major applications are up to date with security patches and software versions
Penetration Testing	Annually	Annually	• Determines how vulnerable an organization's network is to penetration and the level of damage that can be incurred • Tests IT staff's response to perceived security incidents and their knowledge of and implementation of the organization's security policy and system's security requirements
Password Cracking	Continuously to same frequency as expiration policy	Same frequency as expiration policy	• Verifies that the policy is effective in producing passwords that are more or less difficult to break • Verifies that users select passwords that are compliant with the organization's security policy
Log Reviews	Daily for critical systems, e.g., firewalls	Weekly	• Validates that the system is operating according to policies
Integrity Checkers	Monthly and in case of suspected incident	Monthly	• Detects unauthorized file modifications
Virus Detectors	Weekly or as required	Weekly or as required	• Detects and deletes viruses before successful installation on the system
War Dialing	Annually	Annually	• Detects unauthorized modems and prevents unauthorized access to a protected network
War Driving	Continuously to weekly	Semi-annually	• Detects unauthorized wireless access points and prevents unauthorized access to a protected network

Category 1 systems are generally those systems whose operation is critical to the organizational mission. Category I systems include:

- ❑ Firewalls, both internal and external,
- ❑ Routers and switches,
- ❑ Related network-perimeter security systems such as intrusion detection systems,
- ❑ Web servers, e-mail servers, and other application servers,
- ❑ Other servers such as for Domain Name Service (DNS) or directory servers or file servers, and
- ❑ Other selected high-priority applications and systems.

Category 2 systems include general staff and related systems, e.g., desktop, standalone and mobile client systems. While the security of these systems is important, Category 1 systems should generally be tested more frequently than Category 2 systems.

- ❑ Determine the cost of performing each test for each system. Costs vary depending upon the size and complexity of the system to be tested, the level of human interaction required for each test, the feasibility of selecting a sample for the tests, and the size of the sample.

- ❑ Identify the benefits of each test type per system to assure that the cost of testing does not exceed its value to the organization. These benefits can include knowledge gained about systems and networks, and reduced chances for intrusion or business disruption.

- ❑ Prioritize systems for testing, based on security category, cost of testing, and benefits. The prioritized list should include the resources required for conducting each type of test for each system under consideration. The starting point for determining minimum required resources should be minimum testing for those systems with the highest level of impact. If resources are not available for minimum testing for the highest impact systems, additional resources should be requested.

Summary of NIST Recommendations

- **Make network security testing a routine and integral part of the system and network operations and administration.** Organizations should conduct routine tests of systems and verify that systems have been configured correctly with the appropriate security mechanisms and policy. Routine testing prevents many types of incidents from occurring in the first place. The additional costs for performing this testing will likely be offset by the reduced costs in incident response.
- **Test the most important systems first.** In general, systems that should be tested first include those systems that are publicly accessible, that is, routers, firewalls, web servers, e-mail servers, and certain other systems that are open to the public, are not protected behind firewalls, or are mission-critical systems. Organizations can then use various metrics to determine the importance or criticality of other systems in the organization and then test those systems as well.
- **Use caution when testing.** Certain types of testing, including network scanning, vulnerability testing, and penetration testing, can mimic the signs of attack. Testing should be done in a coordinated manner, with the knowledge and consent of appropriate officials.

Who we are

The Information Technology Laboratory (ITL) is a major research component of the National Institute of Standards and Technology (NIST) of the Technology Administration, U.S. Department of Commerce. We develop tests and measurement methods, reference data, proof-of-concept implementations, and technical analyses that help to advance the development and use of new information technology. We seek to overcome barriers to the efficient use of information technology, and to make systems more interoperable, easily usable, scalable, and secure than they are today. Our website is http://www.itl.nist.gov/.

- **Ensure that security policy accurately reflects the organization's needs.** The policy must be used as a baseline for comparison with testing results. Without an appropriate policy, the usefulness of testing is drastically limited. For example, discovering that a firewall permits the flow of certain types of traffic may be irrelevant if there is no policy that states what type of traffic or what type of network activity is permitted. When there is a policy, testing results can be used to improve the policy.
- **Integrate security testing into the risk management process.** Testing can uncover unknown vulnerabilities and misconfigurations. As a result, testing frequencies may need to be adjusted to meet the prevailing circumstances, such as when new controls are added to vulnerable systems or other configuration changes are made because of a new threat environment. Security testing reveals crucial information about an organization's security posture and its ability to surmount external attacks or to avoid significant financial costs or damage to its reputation as a result of internal malfeasance. In some cases, the results of the testing may indicate that the policy and the security architecture should be updated.
- **Ensure that system and network administrators are trained and capable.** The staff members recruited for network system testing may already be involved in system administration. While system administration is an increasingly complex task, the numbers of trained system administrators generally has not kept pace with the increase in computing systems. Competent system administration may be the most important security measure an organization can employ, and organizations should ensure they have sufficient staff members with the required skill level to perform system administration and security testing correctly.
- **Ensure that systems are kept up-to-date with patches.** As a result of security testing, it may become necessary to patch many systems. Applying patches in a timely manner can sharply reduce the organization's exposure to vulnerabilities.
- **Look at the big picture.** The results of routine testing may indicate that the organization should readdress its systems security architecture. Some organizations may need to step back and undergo a formal process of identifying the security requirements for many of its systems, and then begin to redesign or adapt its security architecture accordingly. This process will result in improved efficiency of operations and fewer costs related to incident response operations.
- **Understand the capabilities and limitations of vulnerability testing.** Vulnerability testing may result in many false positive scores, or it may not detect certain types of problems that are beyond the detection capabilities of the tools. Penetration testing is an effective complement to vulnerability testing, aimed at uncovering hidden vulnerabilities. However, it is resource intensive, requires much expertise, and can be expensive. Organizations should assume that they are vulnerable to attack regardless of how well their testing scores indicate.

Useful References

The following NIST Special Publications (SPs) and Federal Information Processing Standards (FIPS) provide useful information about planning, implementing, and maintaining secure information systems. These publications are available at: http://csrc.nist.gov/publications/

NIST SP 800-12, *An Introduction to Computer Security: The NIST Handbook*, October 1995, provides guidance on general security procedures.

NIST SP 800-14, *Generally Accepted Principles and Practices for Securing Information Technology Systems*, September 1996, describes common practices for the security of information systems.

NIST SP 800-18, *Guide for Developing Security Plans for Information Technology Systems*, December 1998, provides details on developing and updating security plans.

NIST SP 800-26, *Security Self-Assessment Guide for IT Systems*, November 2001, provides details on self-assessment.

NIST SP 800-27, *Engineering Principles for Information Technology Security (A Baseline for Achieving Security),* June 2001, presents system-level security principles to be considered in the design, development, and operation of information systems.

NIST SP 800-30, *Risk Management Guide for Information Technology Systems*, January 2002, discusses the process of identifying risk, assessing risk, and taking steps to reduce risk to an acceptable level.

NIST SP 800-31, *Intrusion Detection Systems (IDS)*, November 2001, discusses hardware and software systems that monitor events occurring in a computer system or network.

NIST SP 800-34, *Contingency Planning Guide for Information Technology (IT) Systems*, June 2002, gives information on developing and implementing IT contingency plans.

NIST SP 800-40, *Procedures for Handling Security Patches*, September 2002, provides guidance on developing and implementing an organizational patch and vulnerability approach.

NIST SP 800-41, *Guideline on Firewalls and Firewall Policy*, January 2002, presents information about the use of firewalls and development of firewall policies.

NIST SP 800-48, *Wireless Network Security: 802.11, Bluetooth, and Handheld Devices*, November 2002, provides guidance on improving the security of wireless systems and mobile devices.

NIST, SP 800-61 (Draft), *Computer Security Incident Handling Guide*, discusses forming incident response teams, establishing incident response policies and procedures, and handling incidents.

NIST SP 800-64, *Security Considerations in the Information System Development Life Cycle*, October 2003, presents a framework for incorporating security into all phases of the system development life cycle.

FIPS 199 (Pre-publication Final), *Standards for Security Categorization of Federal Information and Information Systems*, December 2003. http://csrc.nist.gov/publications/drafts/draft-fips-pub-199.pdf

Disclaimer
Any mention of commercial products or reference to commercial organizations is for information only; it does not imply recommendation or endorsement by NIST nor does it imply that the products mentioned are necessarily the best available for the purpose.

U.S. DEPARTMENT OF COMMERCE
National Institute of Standards and Technology
100 Bureau Drive, Stop 8900
Gaithersburg, MD 20899-8900

Official Business
Penalty for Private Use $300

Address Service Requested

PRSRT STD
POSTAGE & FEES PAID
NIST
PERMIT NUMBER G195