GUIDE TO INFORMATION SECURITY TESTING AND ASSESSMENT

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

A comprehensive approach to information security testing and assessment is essential to the secure operation of an organization's information technology (IT) systems. By applying technical testing and examination techniques, organizations can identify and assess the vulnerabilities of their systems and networks, and then take steps to improve their overall security.

The Information Technology Laboratory of the National Institute of Standards and Technology (NIST) recently published a new guide to help organizations conduct their information security assessments. Issued in September 2008, the guide presents the key elements of security testing and assessments, explains the specific techniques that can be applied, and recommends effective methods for implementing testing and assessment practices.

NIST Special Publication (SP) 800-115, *Technical Guide to Information Security Testing and Assessment: Recommendations of the National Institute of Standards and Technology*

NIST SP 800-115, *Technical Guide to Information Security Testing and Assessment*, was written by Karen Scarfone and Murugiah Souppaya of NIST, and by Amanda Cody and Angela Orebaugh of Booz Allen Hamilton. The new guide replaces NIST SP 800-42, *Guideline on Network Security Testing*.

NIST SP 800-115 presents the basic technical aspects of conducting information security assessments. It discusses technical testing and examination methods that an organization might use as part of an assessment, and helps organizations to apply the techniques effectively to their systems and networks. The guide stresses the importance of organizational support to the technical assessment process through sound planning, careful analysis of findings, and regular reporting of results and recommendations to management officials.

Topics covered in the guide include detailed descriptions of technical examination techniques such as review of documentation, review of logs, network sniffing, and file integrity checking; techniques such as network discovery and vulnerability scanning for identifying targets and analyzing them for potential vulnerabilities; and techniques used to validate the existence of vulnerabilities, such as password cracking and penetration testing.

The appendices provide a comprehensive collection of supporting information and resources to help organizations implement their security testing and assessments. These include:

* information about publicly available “live” operating system distributions, which allow an assessor to boot a computer using a CD containing tools for security testing;
* a template for creating Rules of Engagement (ROE), the detailed guidelines and constraints established before the start of a security test concerning the execution of information security testing;
* information about application security testing and examination techniques;
* recommendations for performing remote access testing;
* a list of resources to assist organizations in managing the security assessment process;
* a glossary of terms used throughout the guide; and
* a list of acronyms and abbreviations.

NIST SP 800-115 is available from the NIST website: http://csrc.nist.gov/publications/PubsSPs.html.

Information Security Assessments: Methodologies and Techniques

The assessment process enables organizations to determine how effectively the implementers and the components of information systems are meeting their specific security goals and objectives. The elements that can be assessed, called the assessment objects, include the host computer, the entire system, the network, a particular procedure, or a person. Assessment methods that can be employed include:

Testing: exercising one or more assessment objects under specified conditions to compare actual and expected behaviors;

Examination: checking, inspecting, reviewing, observing, studying, or analyzing one or more assessment objects to facilitate understanding, achieve clarification, or obtain evidence; and

Interviewing: conducting discussions with individuals or groups within an organization to facilitate understanding, achieve clarification, or identify the location of evidence.

Several accepted methodologies for conducting different types of information security assessments are listed in Appendix E of the guide. Organizations may want to consider using more than one methodology in conducting their assessments.

NIST has developed a process for federal organizations that, under the Federal Information Security Management Act (FISMA) of 2002, are required to select and implement cost-effective security controls, based on considerations of risk, and to conduct security testing and assessments of the controls that have been implemented. See the **More Information** section at the end of this bulletin for references concerning the federal government’s assessment policies. Another widely used assessment methodology

referenced in Appendix E is the Open Source Security Testing Methodology Manual (OSSTMM), developed by the Institute for Security and Open Methodologies.

Planning, Conducting, and Evaluating Security Assessments

NIST SP 800-115 discusses using a phased information security assessment methodology to make the most efficient use of organizational staff and resources in carrying out information security assessments.

In the **planning phase**, organizations gather the information that is needed to conduct the assessment and establish the assessment approach. A project management plan should be developed to address goals and objectives, scope, requirements, team roles and responsibilities, limitations, success factors, assumptions, resources, timeline, and deliverables.

In this phase, organizations develop a security assessment policy to provide direction for their assessment activities. Planning should also include deciding which systems should be assessed and the frequency of the assessments; these decisions should be based on risk considerations, expected benefits, scheduling and regulatory requirements, and the availability of resources. Testing and examination techniques should be selected based on the requirements, and a plan that documents all activities and resources should be developed.

In the **execution phase**, organizations identify vulnerabilities and validate them when appropriate. This phase addresses activities associated with the assessment methods and techniques that were decided upon in the planning phase and identified in the assessment plan or ROE. The activities may differ depending on type of assessment, but upon completion of this phase, assessors will have identified system, network, and organizational process vulnerabilities.

Proper coordination within the organization is a paramount consideration in this phase to facilitate the assessment process and to reduce the risks. If a security incident is detected during the assessment process, assessors should follow the organization’s reporting procedures about such activities. Analysis of vulnerabilities should take place during the assessment process, as well as after the assessment is completed. This allows individual vulnerabilities to be addressed immediately and enables the organization to analyze the root causes of vulnerabilities. Officials can then deal with program weaknesses, such as insufficient management of software patches, architectural and policy weaknesses, and inadequate training procedures.

During this phase, organizations should make sure that all of the data associated with the assessments has been protected. Information about system vulnerabilities is sensitive and should be collected, stored, and, if necessary, transmitted securely. After the completion of the assessment, data that is no longer needed by the organization should be destroyed in accordance with good security practices.

In the **post-execution phase**, organizations apply the information provided by the assessment to improve their overall information security. Actions should be recommended to mitigate the vulnerabilities, and a report incorporating the recommendations should be prepared. Most important, the recommended actions should be carried out.

Testing and Examination Techniques

Many technical security testing and examination techniques can be used to assess the security posture of systems and networks. No single technique can provide a complete picture of the security of a system or network; techniques can be combined to assure robust security assessments.

Review techniques are used to evaluate systems, applications, networks, policies, and procedures to discover vulnerabilities, and are generally conducted manually. They include documentation, log, ruleset (a collection of rules that govern network traffic or system activity), and system configuration review; network sniffing; and file integrity checking.

Target identification and analysis techniques can identify systems, ports, services, and potential vulnerabilities. These techniques may be performed manually but they are generally performed using automated tools. They include network discovery, network port and service identification, vulnerability scanning, wireless scanning, and application security examination.

Target vulnerability validation techniques corroborate the existence of vulnerabilities and may be performed manually or by using automatic tools, depending on the specific technique used and the skill of the test team. They include password cracking, penetration testing, social engineering, and application security testing.

Comparing Tests and Examinations

Examinations primarily involve the review of documents such as policies, procedures, security plans, security requirements, standard operating procedures, architecture diagrams, engineering documentation, asset inventories, system configurations, rulesets, and system logs. Examinations are conducted to determine whether a system is properly documented, and to gain insight on aspects of security that are only available through documentation. This documentation identifies the intended design, installation, configuration, operation, and maintenance of the systems and network.

Testing involves hands-on work with systems and networks to identify security vulnerabilities, and can be executed across an entire enterprise or on selected systems. The use of scanning and penetration techniques can provide valuable information on potential vulnerabilities, and predict the likelihood that an adversary or intruder will be able to exploit them. Testing also allows organizations to measure levels of compliance in areas such as patch management, password policy, and configuration management.

Testing can provide a more accurate picture of an organization's security posture than what is gained through examinations; however, it is more intrusive and can impact systems or networks in the target environment. Tests known to create denial of service conditions and other disruptions can be excluded to help reduce these negative impacts. Testing does not provide a comprehensive evaluation of the security posture of an organization, and may be costly in terms of staff time and resources. Also, testing is less likely than examinations to identify weaknesses related to security policy and configuration. In many cases, combining testing and examination techniques can provide a more accurate view of security.

Approaches to Testing

External security testing is conducted from outside the organization's security perimeter, allowing the environment's security posture to be examined with the goal of revealing vulnerabilities that could be exploited by an external attacker.

External testing often begins with reconnaissance techniques that search public registration data, Domain Name System (DNS) server information, newsgroup postings, and other publicly available information to collect information that may help the assessor to identify vulnerabilities. The assessor uses network discovery and scanning techniques to determine external hosts and listening services. Initial attacks are generally focused on commonly used and allowed application protocols. Servers that are externally accessible are tested for vulnerabilities that might allow access to internal servers and private information. External security testing also concentrates on discovering access method vulnerabilities, such as wireless access points, modems, and portals to internal servers.

Internal security testing is conducted from the internal network, and the assessor assumes the identity of a trusted insider or an attacker who has penetrated the perimeter defenses. This kind of testing can reveal vulnerabilities that could be exploited and demonstrates the potential damage that could result. Internal security testing also focuses on system-level security and configuration.

Assessors who perform internal testing are often granted some level of access to the network, normally as general users, and are provided with information that users with similar privileges would have. This level of temporary access depends on the goals of the test, and can be up to and including the privileges of a system or network administrator. Working from the level of access they have been granted, assessors attempt to gain additional access to the network and systems by increasing their access privileges, such as user-level to administrator-level privileges.

Internal testing is less limited than external testing because it takes place behind perimeter defenses, even though there may be internal firewalls, routers, and switches in place that pose limitations. Examination techniques such as network sniffing may be used in addition to testing techniques. When both internal testing and external testing are

performed, the external testing usually takes place first. This approach avoids assessors acquiring insider information that might not be available to an attacker.

Overt security testing, also known as white hat testing, involves performing external and/or internal testing with the knowledge and consent of the organization's IT staff, enabling comprehensive evaluation of the network or system security posture. The IT staff can provide guidance to limit the testing's impact, and useful training opportunities for staff members are created.

Covert security testing, also known as black hat testing, takes an adversarial approach to testing without the knowledge of the organization's IT staff but with the full knowledge and permission of upper management. Some organizations designate a trusted third party to ensure that the target organization does not initiate response measures associated with the attack without first verifying that an attack is indeed underway. This type of test is useful for testing technical security controls, the IT staff's response to perceived security incidents, and staff knowledge and implementation of the organization's security policy. The testing may be conducted with or without warning, and enables the organization to examine the damage or impact an adversary could cause, but it does not identify every vulnerability or test every security control.

Overt testing is less expensive and less risky than covert testing, which is often time-consuming and costly due to its stealth requirements. However, covert testing provides a better indication of the everyday security of the target organization.

NIST Recommendations

NIST recommends that organizations apply the following policies in planning and implementing their security assessment activities:

Establish an information security assessment policy to identify the organization's requirements for carrying out assessments, and to identify the appropriate individuals who will ensure that assessments are conducted in accordance with the requirements. The organizational requirements for assessments should be specified, providing the roles and responsibilities of individuals, the need for adherence to an established assessment methodology, the assessment frequency, and documentation requirements.

Implement a repeatable and documented assessment methodology to provide for consistency and structure to the assessment process, to expedite the transition of new assessment staff members, and to address resource constraints associated with assessments. Using a repeatable and documented methodology enables organizations to maximize the value of assessments while minimizing possible risks introduced by certain technical assessment techniques. These risks can range from not gathering sufficient information on the organization's security posture for fear of impacting system functionality to affecting the system or network availability by executing techniques without the proper safeguards in place. Organizations can minimize the risk caused by certain assessment techniques by using skilled assessors, developing comprehensive

assessment plans, logging assessor activities, performing testing off-hours, and conducting tests on duplicates of production systems, such as development systems. Organizations should determine the level of risk that they are willing to accept for each assessment and tailor their approaches accordingly.

Determine the objectives of each security assessment and tailor the approach that is adopted. Security assessments have specific objectives, acceptable levels of risk, and available resources. No single technique can provide a comprehensive picture of an organization's overall security position; therefore, organizations should use a combination of techniques, a practice that helps organizations to limit their risks and their use of resources.

Analyze findings, and develop risk mitigation techniques to address weaknesses. To ensure that the security assessment process provides maximum value, organizations should conduct root cause analysis upon completion of an assessment to assure that the assessment findings are acted upon and implemented in the application of practical techniques that will improve overall security. The results may indicate that organizations should address not only technical weaknesses, but weaknesses in organizational processes and procedures as well.

More Information on Conducting Information Security Assessments

Security testing and examination is required by FISMA and other regulations. NIST has developed a risk-based program for federal government agencies that starts with the categorization of federal information systems as low-impact, moderate-impact, or high-impact for the security objectives of confidentiality, integrity, and availability, and the selection of an appropriate set of security controls for their information systems.

These requirements are specified in Federal Information Processing Standard (FIPS) 199, *Standards for Security Categorization of Federal Information and Information Systems*, and FIPS 200, *Minimum Security Requirements for Federal Information and Information Systems*. After systems are categorized, agencies select an appropriate set of security controls from NIST SP 800-53, *Recommended Security Controls for Federal Information Systems*, to satisfy their minimum security requirements.

A companion guide, NIST SP 800-53A, *Guide for Assessing the Security Controls in Federal Information Systems*, introduces the fundamental concepts that support the assessment of security controls, including the integration of assessments into the system development life cycle and the need for an organizational strategy for conducting assessments of security controls. NIST SP 800-53A discusses the framework for development of assessment procedures, describes the process of assessing security controls, and offers assessment procedures for each control. NIST SP 800-53A was developed to be used in conjunction with NIST SP 800-37, *Guide for the Security Certification and Accreditation of Federal Information Systems*.

For information about NIST standards and guidelines that are listed above, as well as other security-related publications, see http://csrc.nist.gov/publications/index.html.

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.