Testing Software System Security

Effectiveness of security testing can be improved by focusing on the points where security has the highest probability of being compromised. A testing tool that has proved effective in identifying these points is the penetration-point matrix.

This test process provides two resources: a security baseline and an identification of the points in an information system that have a high risk of being penetrated. Neither resource is statistically perfect, but both have proven to be highly reliable when used by individuals knowledgeable in the area that may be penetrated.

The penetration-point tool involves building a matrix. In one dimension are the activities that may need security controls; in the other dimension are potential points of penetration.

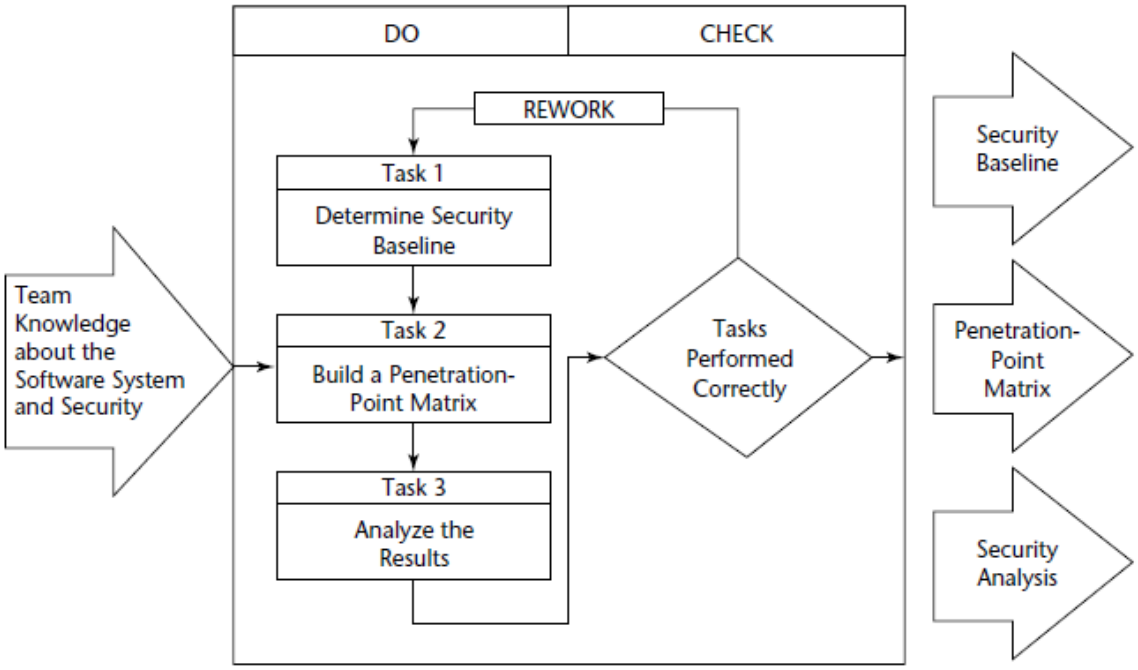

Figure 20-1 Workbench for testing software system security.

Where Vulnerabilities Occur

A vulnerability is a weakness in an information system. It is the point at which software systems are easiest to penetrate. Understanding the vulnerabilities helps in designing security for information systems.

Vulnerable Areas

The following list ranks the nine functional locations according to vulnerability:

- Data- and report-preparation facilities.
- Computer operations.
- Non-IT areas.
- Online terminal systems.
- Programming offices.
- Handling areas for online data preparation and output reports.
- Digital media storage facilities.
- Online operations.
- Central processors.

Task 1: Establish a Security Baseline

A baseline is a snapshot of the organization's security program at a certain time. The baseline is designed to answer two questions:

- What are we doing about computer security?
- How effective is our computer security program?
-

Baseline information should be collected by an independent assessment team; as much as possible, bias for or against a security program should be removed from the process. The process itself should measure both factual information about the program and the attitudes of the people involved in the program.

Two categories of the baseline information need to be collected. The first is related to the security process and includes the policies, methods, procedures, tools, and techniques used to protect computer resources. The second category of information relates to security acts and includes information about attempted and actual penetrations into computer resources. Wherever possible, actual losses should be quantified.

Task 2: Build a Penetration-Point Matrix

This task identifies the activities that need control, as well as the data flow points where penetration is most likely to occur. These concepts are used to build a penetration-point matrix that helps identify security vulnerabilities for management action. The creation of the penetration-point matrix answers the question of where security is needed and whether security controls exist at the most likely points of penetration.

Selecting Security Activities

The determination of the magnitude of the security program is based on the following two factors:

- Type and magnitude of risks
- Type and extent of security controls

The greater the risks, the greater the need for control. The two variables of the scope of the security program are directly related. One can measure the magnitude of the risks to determine the strength of the management security controls needed. The amount of management controls to be installed is also a measure of the scope of the security program.

The activities that require management security controls can be divided into the categories discussed in the following three subsections.

Interface Activities

These are the activities and individuals that use computer resources. The specific activities relate to functions either needed by the computer environment or furnished by the computer environment:

- Program users
- Technical interfaces
- Application systems
- Privileged users
- Vendor interfaces

Development Activities

These are the activities that relate to the acquisition, creation, and maintenance of the software needed to accomplish the processing requirements established by users of computer facilities to meet business needs:

- Policies, procedures, and standards
- Training.
- Database administration
- Communications
- Documentation
- Program change control
- Records-retention program.

Operations Activities

These are the procedures and methods used to process data on the computer using the software developed for that purpose as initiated by the activities that interface with the computer center. Activities also include supporting tasks necessary to ensure the integrity of the mainline operations:

- Computer processing
- Media libraries
- Error handling
- Production library control
- Computer operations
- Disaster planning
- Privileged utilities and commands

Task 3: Analyze the Results of Security Testing

Software testers can analyze the results from testing computer security. This analysis provides a baseline and the points at which security most likely could be penetrated. If the testers have identified the controls at the penetration points, they will have most of the information needed to analyze the adequacy of security.

Analysis of the following proves helpful in determining whether security is adequate for an information system:

- Whether adequate controls exist at the points of highest probability of penetration
- Whether controls exist at the points of most probable penetration
- Adequacy of the controls to protect against penetration at the points of most probable penetration
- Strengths and weaknesses identified in the baseline assessment
- Risks for which there are no controls
- Penetration points for which there are no controls