Pen-Test Explained by DaAnZeR

A penetration test, or ethical hacking, determines how difficult it is to break into a computer network. The form of such a test varies by situation. The tests can range from a brief overview of the security of an existing infrastructure to an extensive simulated break_in, with the goal of obtaining specific information.
A penetration test can reveal:

- Which information can be obtained from outside the network
- Whether and how the system reacts to attack
- Whether it's possible to break into the system, using available or existing knowledge
- Which information becomes accessible, if the system is broken into

The objective of penetration testing is of course to investigate the system from the attacjer's perspective. The primary aim is to identify exposures and risk before seeking a solution.

Types of testing

There are three types of approaches for penetration testing:
A zero knowledge test, a full knowledge test, and a partial knowledge test.
In a zero knowledge test, the test team has no real information about the target envoirnment and must begin with information gathering. This type of test is designed to provide the most realistic penetration test possible.

In a partial knowledge test, the target organization provides the test team with the type of information a motivated attacker is likely to find, and hence, saves time and expense. A partial knowledge test may also be chosen if there's a specific kind of attack or a specific tagetedhost the test team should focus on. To conduct a partial knowledge test, the test team is provided with stuff like policy and network topology documents, asset inventory, and other valuable information.

In the last type of penetration testing, a full knowledge test, the test team has much information about the target information about the target envoirnment as possilble. This approach is designed to simulate an attacker who has intimate knowledge of the target organization's systems, such as an actual employee.

Techniques of attack

A comprehencive description of attack techniques is essential to minimizeor avoid inadvertent damage or loss of information on the target systems.

Penetration methodologies may vary among service providers, but the primary phases are the same:

- Discovery phase, in which, in which information is gathered on the target organization through websites and mail servers, public records and databases (Address and Name Registrars, DNS, Whois, EDGAR, etc.)
- Enumeration phase, in which the penetration team actively tries to obtain user names, network share information and application version information of running services
- Vulnerability mappin phase, in which the test team maps the profile of the envoirnment to publicly know the vulnerabilities.
- Exploitation phase, in which the test team will try to gain priviliged access to a target system by eploting the identified vulnerabilities

Attackers are constantly refining their skills and tactics. You should do the same so you can spot the holes before they do. Security means finding a balance between the value of information and the amout of resources that have tobe expended to gain access to it. Penetration teste can reveal whether systems work on need to adapt.

For Brief description and manual, please visit http://ideahamster.org/
The Open Source Security Testing Methodology Manual.

I welcome your queries and suggestions. Please drop your mail at daanzer@yahoo.com