

Penetration Testing An Overview

Steve Cholerton
July 2006

Introduction

Penetration Testing is an attempt to break the security of a computer system or network, under instruction from the owners or maintainers of that facility. It is an attempt to simulate an attempted break in by a computer savvy criminal. A Penetration Test gives a snapshot of the security at a moment in time, and is not a full security audit.

If a criminal attempts to breach your computer network they will generally follow a sequence of five steps:

- Reconnaissance
- Scanning
- Gain Access
- Maintain Access
- Cover Tracks

It therefore makes sense that a Penetration Test follows a similar, although obviously not identical, sequence of events.

Planning and Preparation

This stage involves a meeting between the Penetration Tester and the Client. Key areas to be covered are: Scope, Objective, Timing and Duration. In addition documents must be signed to cover the Penetration Tester and the Client, generally in the form of a Non Disclosure Agreement (NDA).

Information Gathering and Analysis

This next stage involves the Penetration Tester finding as much information as possible about the company he will be asked to target. His first stop will probably be the companies own website, from there he may consult services such as www.netcraft.com. The information he is looking for is Domain Names, Server Names, ISP Information, Host Addresses and anything else that will help him build a picture of the target. The second part of this process involves Port Scanning and OS Fingerprinting.

Vulnerability Detection

If Stage 2 has been successful then the Penetration Tester now has all the information he needs to make the decision as to what hosts to target, and with what vulnerabilities. Some techniques he may use at this stage include Password Cracking, SQL Injection, Rootkit, Social Engineering and Physical Security.

Analysis and Reporting

This is where the Penetration Tester reports back to his Client. The information he is going to present to the client, includes the following:

- An Overview of the work done
- Detailed Analysis of all Vulnerabilities
- Summary of Successful Penetration Attempts
- Suggestions for the next step

Finish Up

This is where the Penetration Tester makes sure that anything he has done in the course of his work will have no effect when he has finished. For example he will remove any backdoors and additional user accounts that he has created, leaving the system how he found it.

The above is a quick overview only of the procedures that may be followed by a Penetration Tester while undertaking their assignment.

Sources

Conducting a Penetration Test on an Organisation: Chan Tuck Wai 2002
Penetration Testing and Network Defence: Andrew Whitaker and Daniel Newman 2005