Penetration Test: The Rules

Introduction

The purpose of the penetration test is to provide you with some experience in the practise of computer security, to teach you how to analyze systems for security problems, and to give you experience in detecting and preventing exploitation of flaws. You will work in groups, with 3 to 4 people in a group; this will enable you to brainstorm, and to bring different perspecitives and experiences to the problem.

Your goal in this exercise is to acquire superuser status.

The Rules

The rules for the penetration test are simple.

1. You must use the Flaw Hypothesis Methodology as discussed in class. Where you get the information needed to hypothesize flaws is up to you.
2. You are not allowed to use social engineering techniques. You cannot try to trick, bribe, extort, or swindle your way in (or any variant thereof).
3. You may not ask for help from other sources. You **are** free to use help you can obtain passively. For example, it's okay to look in the archives of the bugtraq mailing list, but it's not okay to post a message to bugtraqs asking for help.
4. You must keep written logs of your work. In particular, for each hypothesized flaw, you must record a high-level summary, a detailed description of the hypothesized flaw, its priority (or severity), how you could test for it, how an attacker could exploit it, and where you heard about it or what made you think of it. You are free to include other information, but you must keep the above at a minimum.
5. If you test by attacking, youmust keep a log of every command you type, and the inputs and outputs, and their affect. If you can script the session, that is fine (but do print out the script).
6. Have fun!

The System

The system is a Sun SparcStation 1 running Solaris 2.5.1. Its IP address is 128.120.56.74, and its name is ecs253.cs.ucdavis.edu. We will ***not*** pit this name in the DNS or mail servers; you ***must*** get to it using the IP address.