Sandia Project Part 2

Introduction

The Sandia project has 4 goals for each part. The goals, in brief, are:

1. Locate, identify, and characterize all of the computers in the network (by reporting their IP addresses, type, and any other characteristics)..
2. Deny services in a controlled and repeatable manner to the user box or DNS server.
3. Gain access to the user box so that you can cause desired changes on it.
4. Same as 3 except for the secure DNS and the protected server(s).

The project description handout gave more details.

What is Due

You must:

1. Submit a list of the IP addresses and operating system types of the Sandia machines you have found (other than the login server). Justify your claim about the operating system; why do you think that system *a.b.c.d* is running MonsterOS 3.7?

   How to submit: Put this information into a file (text, Postscript, or PDF), named appropriately, and use the *handin* program to submit it under *sandia2*.
2. Submit at least 4 entries from your notebook. An entry is described below. Please identify each part distinctly.

   How to submit: Put your entries into files (text, Postscript, or PDF), named *test1* through *test4*, and use the *handin* program to submit it under *sandia2*.

Due Date

This is due on Friday, February 15, at 9AM.

Notebook Entry Format

Each entry consists of 3parts. They are:

1. *Hypothesis*. What vulnerability are you testing for, and why do you believe it exists in the target? Your hypothesis may be based upon specific characteristics of the target (such as running a particular server), upon knowledge of the operating system (such as it being MonsterOS 3.8, and MonsterOS 3.8 is known to have this vulnerability in its TCP/IP stack), or upon knowledge of the system (such as looking at the source to SDNS, and seeing a vulnerability in it). Please state clearly what you suspect the vulnerability is, and why. Provide any general information about the target that helped you decide that this particular vulnerability might exist.
2. *Testing*. State how you will test for the vulnerability, and carry out the test. You can use soneone else's code for the test, but you must make sure it runs, and explain why the program/routine you are using does in fact test the vulnerability. (You have to be specific about your test. You *cannot* say that "I found Tony's attack tool for this vulnerability at attacks-r-us.com." You need to show how the tool works, and why it will establish whether the vulnerability exists.)
3. *Generalization*. If your test fails, why did it fail? Are similar tests likely to fail also? Should you look for other types of vulnerabilities? If your test succeeds, what other vulnerabilities similar to this one might exist? Why do you think so?

It is perfectly fair for you to turn in 4 related vulnerabilities. For example, one vulnerability may lead you to a generalization that suggests other vulnerabilities. If this happens, *please* document your thinking in part 3, and name the files containing the suggested entries.

Note

Please *do not* reuse the data from part 1. The network and systems have probably changed, so simply begin anew. You may of course use the knowledge, tools, and techniques you have gained from the first part …