Sandia Project Part 3 (Alternate)

Introduction

This alternate project allows you to analyze source code for potential vulnerabilities. You are to select a program that runs with privileges beyond that of a normal unprivileged user (such as a system account, *root*, or *Administrator*), and examine it. (On UNIX and Linux systems, this basically means a network server or a *setuid* or *setgid* program.)You are to determine whether a normal unprivileged user could obtain those extra privileges by using the program in a manner in which the designer and implementer of the program did not intend.

What is Due

You must:

1. Submit the source code of the program, along with annotations showing each section that you examined.
2. Submit a description of what you looked for and why. Be specific. Describe what the threat is and how you looked for vulnerabilities related to the threat. What would indicate that the program was vulnerable to that threat?
3. If you found any vulnerabilities, document them. Describe under what circumstances they could be exploited and how the exploit would work. Writing an exploit to demonstrate this attack is worth extra credit!

   How to submit: Use the *handin* program to submit your work as a set of files into the directory *sandia3*.

Due Date

This is due on Friday, March 15, at 11:59PM.