Set-UID Program Vulnerability Lab

SEED Lab: A Hands-on Lab for Security Education

Overview

Set-UID is an important security mechanism in Unix operating systems. When a Set-UID program is run, it assumes the owner's privileges. For example, if the program's owner is root, then when anyone runs this program, the program gains the root's privileges during its execution. Set-UID allows us to do many interesting things, but unfortunately, it is also the culprit of many bad things. Therefore, the objective of this lab is two-fold: (1) Appreciate its good side: understand why Set-UID is needed and how it is implemented. (2) Be aware of its bad side: understand its potential security problems.

Lab Tasks (Description) (Video)

- **For instructors:** if you prefer to customize the lab description to suit your own courses, here are our Latex source files.
- **VM version:** This lab has been tested on our pre-built SEEDUbuntu12.04 and SEEDUbuntu11.04 VMs.
- **Older VM versions:** If you are using an older VM version, you should go to the following web sites:
  - For SEEDUbuntu9.11

Recommended Time:

- Supervised situation (e.g. a closely-guided lab session): **2 hours**
- Unsupervised situation (e.g. take-home project): **1 week**

Helpful Documents

- Checklist for Security of Setuid Programs
- Chen, Wagner, and Dean. Setuid Demystified
- Bishop. How to write a Set-UID program