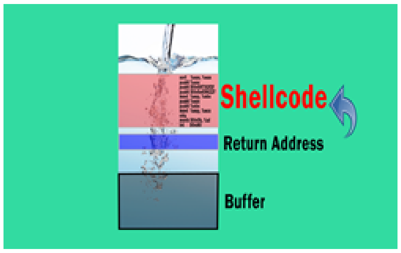
Buffer-Overflow Vulnerability Lab

SEED Lab: A Hands-on Lab for Security Education

Overview



The learning objective of this lab is for students to gain the first-hand experience on buffer-overflow vulnerability by putting what they have learned about the vulnerability from class into actions. Buffer overflow is defined as the condition in which a program attempts to write data beyond the boundaries of pre-allocated fixed length buffers. This vulnerability can be utilized by a malicious user to alter the flow control of the program, even execute arbitrary pieces of code. This vulnerability arises due to the mixing of the storage for data (e.g. buffers) and the storage for controls (e.g. return addresses): an overflow in the data part can affect the control flow of the program, because an overflow can change the return address.

Activities: Students are given a program that has the buffer-overflow problem, and they need to exploit the vulnerability to gain the root privilege. Moreover, students will experiment with several protection schemes that have been implemented in Linux, and evaluate their effectiveness.

Lab Tasks (Description) (Video: Part 1, Part 2, Part 3)

- **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` VM.
- **Older VM versions:** If you are using an older VM version, you should go to the following web sites (they are pretty much the same, but with minor changes caused by the version differences):
  - For SEEDUbuntu11.04
  - 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**

Files that are Needed

- stack.c (the vulnerable program)
- call_shellcode.c
- exploit.c

Suggested Reading

- **SEED Book:** Wenliang Du. *Computer Security: A Hands-on Approach* (Chapter 4).
- Aleph One. Smashing The Stack For Fun And Profit.
- Notes on Non-Executable Stack

SEED Project

- Home Page