Project 4: Exploiting Buffer Overflows

Due Wednesday, December 13, at 9:00 AM (Start of the Final Exam)

The goal of this project is to obtain root privilege on a Linux system by exploiting vulnerabilities in installed programs.

Getting Started

The official VM image for the assignment is located at:

`http://isoptera.lcsc.edu/~seth/cs475/examples/cs475_vm.zip`

It can be run on the class computers, or any other computer with Virtualbox, available for free here:

http://www.virtualbox.org/

The virtual machine has a user "ubuntu", with password "reverse". This user has sudo privileges, so you can install software. The virtual machine does not have a graphical user environment. You can install one if you like, but it will make the VM image larger than it already is. `nano` is an easy-to-use text editor with syntax highlighting that is already installed. If you want network access from the VM, provided VirtualBox is configured correctly, you can enter `sudo dhclient eth1`. The VM runs sshd by default, so you can access it with ssh if it is connected to the network.

Problems

There are 4 vulnerable programs installed on the virtual machine in `/usr/bin`. Each of them takes a command-line argument. By giving a particular string as this argument, you can exploit the vulnerability in the program and run /bin/sh as root. You can run any program as:

```
victim1
```

Source code for the exploits and victims is pre-loaded on the VM. The exploits can be built using make. Each exploit takes a command-line argument, which is the location of the victim. For example:

```
./exploit1 /usr/bin/victim1
```

The program gdb provides an easy way to obtain memory addresses. Stack randomization has been disabled on the virtual machine.

You'll need the contents of the file shellcode.h, in the class examples area.

Turning in the assignment

The assignment should consist of two major components:

- A report explaining how each of your attacks works.
- Exploit programs for each of the 4 victims.