COEN225 Lab 1: Lab Environment Setup and C Refresher

Overview

This lab is for students to become familiar with the lab environment. Students will set up a virtual Linux operating system environment and write a basic C program.

Lab Submission

Perform the tasks below and submit your responses to questions noted in the task submission sections. Also include any source code you used to generate exploits or other tests.

The lab work and submission must be completed individually but working with other students is allowed. The Camino message board is the preferred method for asking questions so that the instructor and students can respond and allow all students to learn from it.

Lab Tasks

Task 1: Setting up the lab

Although the concepts covered in this course apply across a wide variety of computing systems and architectures, implementation differences greatly affect how attacks and defenses function. We will use a controlled virtualized lab environment in order to minimize those differences.

First, download and install virtualization software. The labs have been tested on VMWare (vmware.com) and VirtualBox (virtualbox.org). The following instructions assumes that VirtualBox is being used. Create a new virtual machine and use the default settings for a 32-bit Debian Linux guest system.

Important: If you are using VirtualBox, you MUST enable PAE/NX in the virtual machine settings before installing the operating system. To do this, go to Settings -> System -> Processor -> Extended Features and check Enable PAE/NX.

Next, download the Debian installer disc ISO file from the official website. (The installer ISO that was linked here is no longer available. See the assignment page for a new link.)

Load the disc and start the virtual machine. In VirtualBox, the optical drive is under Storage IDE Controller. If successful, the Debian installer boot menu should load. Select "Graphical Install".

Generally click on "Continue" to select the default install settings, but ensure that the following options are set:

- Set up users and passwords
  - Set a root password. This document assumes you set a root password of `toor`

- o Create a normal user. This document assumes you created a user with the name user and password resu
- Partition disks
  - o On the final screen which asks "Write the changes to disks?", select "Yes"
- Configure the package manager
  - o On the screen which asks "Use a network mirror?", select "No".
- Software selection
  - o Additionally checking "Xfce" is recommended, especially for users unfamiliar with Linux GUI environments. This will install a lightweight GUI that is more intuitive than the default setup.
- Install the GRUB boot loader on a hard disk
  - o Install the GRUB boot loader to the master boot record? "Yes"
  - o Device for boot loader installation: Select the primary drive, usually /dev/sda

The system will reboot after installation. If successful, you will be at the login screen. It is highly recommended that you take a snapshot at this point (Menu -> Machine -> Take Snapshot). A snapshot saves the state of the guest machine and allows you to revert to that state at any time. Take a snapshot and name it "Fresh Install".

Login to the system using the user you created (User: user / Password: resu).

Now we will install some additional packages required for C programming

First, re-insert the ISO disc that was ejected after the install completed (Menu -> Devices -> [select file]). Next, open a terminal and elevate to root.

```
$ su -
Password: [toor]
#
```

The # indicates that you are now the root user. You must have root privileges to install packages. Install the GCC compiler and the GDB debugger.

```
# apt-get install build-essential gdb
```

Optionally, you may want to install additional packages. Although nano and vi are installed by default, if you want a Windows Notepad-like GUI text editor, leafpad is the XFCE equivalent. For a web browser, chromium can be installed. Finally, you can install kernel header files if you want to use VMWare Tools or VirtualBox Guest Additions to enable extra functionality. You will need to install the correct version for your kernel version.

```
# apt-get install leafpad chromium linux-headers-3.16.0-4-686-pae
```

Log out from root.

```
# exit
logout
$
```

Finally, eject the disc from the drive (or the machine will try to boot from it on reboot) using the Devices menu. Click on the current ISO with the check mark to eject it. You are now ready for the labs. Optionally save another snapshot here.

Task 1 Submission
Run the following command:

```
$ uname -a
```

The kernel version should be 3.16.0-4-686-pae. If the "pae" is missing, then the PAE/NX extensions were not enabled during installation. No submission is required for this task.

Task 2: Hello World
Write a basic "hello world" C program called hello.c that:

- Compiles with GCC
- Accepts any number of command line arguments
- When the program runs, it must output a string to STDOUT using printf()
- Have at least 3 functions: `main()`, `helloworld()`, and `helloname()`
  - The `helloworld()` function accepts no arguments must output "Hello World"
  - The `helloname()` function accepts a string and outputs "Hello " followed by the string passed to the function
- The behavior of the program is different depending on the number of command line arguments
  - If no command line arguments are passed, call `helloworld()`
  - If one command line argument is passed, call `helloname()` and pass the command line argument as a string to the function
  - If two or more command line arguments are passed, output "Goodbye World"

Task 2 Submission
Compile your hello.c in the lab VM and run it three times with zero, one, and two command line arguments. Include your hello.c and output as a text file in your submission. Your output should look similar to this:

```
$ gcc -o hello hello.c
$ ./hello
Hello World
$ ./hello Alice
Hello Alice
$ ./hello Alice Bob
Goodbye World
$
```

Task 3: Hex refresher

Future lectures and labs will make extensive use of the hexadecimal numeral system. Some familiarity with hexadecimal is recommended. Answer these questions to refresh your knowledge:

What is the decimal value of `0xA`?

What is the hex representation of decimal `33`?

What is the value of `0xC + 0x4` in hex? In decimal?

Answers: `10`, `0x21`, `0x10`, `16`

No submission is required for this task.