

CMPSCI 177 – Computer Security
Fall 2011
Homework 7 – Buffer Overflow

Due: 22 NOV 2011 @ 2PM

This assignment helps you develop a detailed understanding of the call stack organization on IA32 Intel Pentium processors. It is divided into two parts as explained below.

Part 1

In this part, your task is to write a program (buggy.c) that has a buffer overflow vulnerability. You must also write another program (exploit.c) that exercises the vulnerability by overwriting the return pointer and jumping to a function called not_used that would normally not be executed during normal runtime. "not_used" must be the same as the following:

```
void not_used()
{
    printf("The buffer was successfully overflowed. Isn't cs177 a lot of fun? \n");
    exit(177);
}
```

Note: For grading purposes, calling exit(177) from outside not_used is cheating!

Part 2

In this part, your task is to write a program (exploit.c) that will exploit the program, vulnerable.c, shown below. This program has been provided in your home directory on the server.

```
void main()
{
    int val;
    val = getbuf();
}

int getbuf()
{
    char buf[12];
    gets(buf);
    return 1;
}
```

Unlike part1, to exploit this program you would have to execute code on the

stack, which is the actual challenge involved in buffer overflow exploits.

Your exploit should open a new shell (/bin/sh).

Test Environment

1. You should carry out the buffer overflow assignment on 128.111.48.180
2. Your login and password have been provided via email. If you did not receive it, please email your TA at iland [a t] cs.ucsb.edu.
3. In your home directory there will be two directories, part1 and part2.
4. In each directory are the files that you will turn in and a makefile, which compiles your programs.

Assignment Turnin and Instructions

In addition to the required files, you need to add a README file to each directory explaining how you exploited the buffer overflow.

Instructions for turning in your homework are as follows:

Simply create an archive of the directories part1 and part2 called solution.tgz in your home directory. We will use this archive for grading, not the directories.

We will be shutting down the server and collecting all solutions at the deadline, so make sure you get it created before then.