

哈尔滨工业大学

网络安全课程实验报告

实验一

## 学院：计算机学院

## 班级：1403202

## 学号：1140320206

## 姓名：霍峻杰

## 实验1：栈和堆的溢出

1. **分析缓冲区溢出的原理。**
2. **缓冲区溢出原理：**

通过往程序的[缓冲区](https://baike.baidu.com/item/%E7%BC%93%E5%86%B2%E5%8C%BA)写超出其长度的内容，造成缓冲区的溢出，从而破坏程序的[堆栈](https://baike.baidu.com/item/%E5%A0%86%E6%A0%88)，造成程序崩溃或使程序转而执行其它指令，以达到攻击的目的。造成[缓冲区](https://baike.baidu.com/item/%E7%BC%93%E5%86%B2%E5%8C%BA)溢出的原因是程序中没有仔细检查用户输入的参数

缓冲区溢出攻击的目的在于扰乱具有某些特权运行的程序的功能，这样可以使得攻击者取得程序的控制权，如果该程序具有足够的权限，那么整个主机就被控制了。一般而言，攻击者攻击root程序，然后执行类似“exec(sh)”的执行代码来获得[root权限](https://baike.baidu.com/item/root%E6%9D%83%E9%99%90)的shell。

1. **基于栈的缓冲区溢出的原理：**

栈是从高地址向低地址写入的，一般用作函数调用是存放返回地址，一些参数等，而数据的写入是从低地址写向高地址的，这样就可以将栈顶的返回函数和参数覆盖，从而使程序在执行调用函数完毕时调用ret函数时，可以被攻击者利用为返回到任意地址。进而通过nop等操作使ret“降落”在自己的恶意代码上，今儿执行并危害计算机。

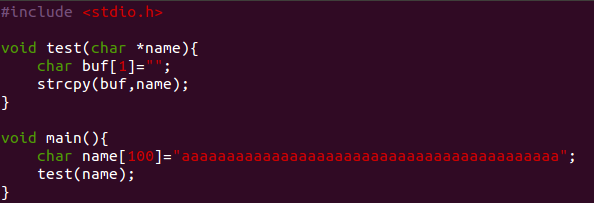
1. **基于堆的缓冲区溢出的原理：**

在给变量分配堆内存空间时，申请到堆的地址在释放之前保持不变，可以利用申请两个堆空间，利用物理地址小的堆地址进行缓冲区溢出，并覆盖后面的大地址的堆空间，达到攻击目的。

1. **实验结果**

**1.栈溢出实验（strcpy）**

源代码：

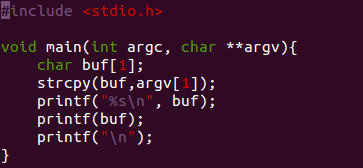


结果：

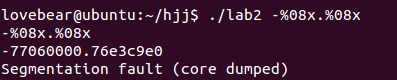


2.printf溢出实验

源代码：



结果：



三、实验总结

这次实验非常的简单，但是可以利用挖掘的地方很多，由于要考研，就没有深入的挖掘，比如可以精心设置程序的返回地址，使其执行我们需要执行的恶意代码，在其中设置缓冲降落区等操作。