电子科技大学信息与软件工程学院

**实 验 报 告**

学 号 2020090916007

姓 名 贾怀宇

（实验） 课程名称 网络安全攻防技术

理论教师 罗绪成

实验教师 罗绪成

**电子科技大学教务处制表**

**电 子 科 技 大 学**

**实 验 报 告**

**学生姓名：贾怀宇 学号：2020090916007 指导教师：罗绪成**

**实验地点：三教502 实验时间：2022.11.29**

1. **实验名称：**

**缓冲区溢出实验**

1. **实验学时：**

**4学时**

**三、实验目的：**

1） 理解进程和调用栈的相关概念；

2） 理解 shellcode 运行的原理；

3） 理解栈溢出的原理；

4） 掌握基本的栈溢出攻击技术。

**四、实验原理：**

缓冲区溢出是目前最常见的一种安全问题，操作系统以及应用程序大都存在缓冲区 溢出漏洞。缓冲区是一段连续内存空间，具有固定的长度。缓冲区溢出是由编程错误引 起的，当程序向缓冲区内写入的数据超过了缓冲区的容量，就发生了缓冲区溢出，缓冲 区之外的内存单元被程序“非法”修改。

一般情况下，缓冲区溢出导致应用程序的错误或者运行中止，但是，攻击者利用程 序中的漏洞，精心设计出一段攻击载荷，覆盖缓冲区之外的内存单元，并劫持程序的控 制流程，运行特意设计的 shellcode，从而获取系统的控制权。

目前，操作系统（Windows、Linux、Unix）、数据库以及应用软件主要采用 C/C++ 语言开发，但 C/C++语言缺乏数组边界条件检查、程序执行不受控制等特点，因此，这 些软件不可避免地存在缓冲区溢出漏洞，成为安全隐患。

**五、实验内容：**

1） 编写程序测试 Shellcode；

2） 通过栈缓冲区溢出进行提权；

3） 提升难度的栈缓冲区溢出提权。

**六、实验器材（设备、元器件）：**

PC机电脑，配有windows或者mac操作系统，Ubuntu或者kali虚拟机

**七、实验步骤：**

（一）编写程序测试 shellcode

（二）通过栈缓冲区溢出进行提权

（三）通过栈缓冲区溢出进行提权—升级版

**八、实验结果与分析（含重要数据结果分析或核心代码流程分析）**

**九、总结及心得体会：**

**十、对本实验过程及方法、手段的改进建议：**

**报告评分：**

**指导教师签字：**