# 实验四、缓冲区溢出漏洞利用实验

## 一、实验学时

课内4学时+课外10学时

## 二、实验内容

给定一包含栈溢出漏洞的Windows程序（下称测试程序），要求利用其漏洞，启动Windows系统自带的某个程序（如，记事本，计算器，等等）。

测试程序说明：该程序是用VS2017编写，分别在64-bit的Windows10家庭中文版和32-bit Windows7旗舰版中测试通过。如果运行时提示缺某个动态链接库，请安装

VC\_2015-2019\_redist.x86.exe后再试。

## 三、实验工具

1. IDA Pro
2. OllyDbg/Immunity Debugger/WinDbg
3. 文本编辑器，十六进制编辑器
4. VC\_2015-2019\_redist.x86.exe

## 四、实验提交内容

（一）实验报告

报告中至少包括以下内容：

1、溢出点定位方法

2、漏洞利用方法（给出攻击发生时栈的布局）

3、DEP保护绕过方法及实现

参考资料：

（1）教材P117-119

（2）第9次课PPT

（3）通过VirtualProtect绕过DEP.PDF

4、shellcode的设计与实现

5、用于实现漏洞利用的“恶意”文件的结构与内容

6、说明可以复现漏洞利用结果的测试环境

7、实验总结

（二）附属文件

1、shellcode源代码

2、用于实现漏洞利用的“恶意”文件

## 五、提交要求

将实验提交内容打包成一个压缩文件，2021年11月30日24:00前，发送到陈泽茂老师的电子邮箱chenzemao@whu.edu.cn，邮件主题为“软件安全实验四”。