“软件安全”实验报告

**.**

**班 级：　　　 网安2104班　　 　.**

**姓名：　　　　　邬雪菲　　　　　.**

**学号：　　　　U202112131　　　　.**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **项目** | **撰写规范** | **实验过程** | **问题分析与小结** | **总分** | **教师签字** |
| 分值 | 20 | 50 | 30 | 100 |  |
| 评分 |  |  |  |  |  |

# 目　录

[目　录 I](#_Toc151928771)

[1 Linux平台漏洞攻防工具使用 1](#_Toc151928772)

[1.1 实验目的 1](#_Toc151928773)

[1.2 实验要求 1](#_Toc151928774)

[1.3 实验环境 1](#_Toc151928775)

[1.4 实验过程记录 1](#_Toc151928776)

[2 栈保护机制绕过与漏洞利用 2](#_Toc151928777)

[2.1 实验目的 2](#_Toc151928778)

[2.2 实验要求 2](#_Toc151928779)

[2.3 实验环境 2](#_Toc151928780)

[2.4 实验过程记录 2](#_Toc151928781)

[2.实验遇到的难点与问题分析 3](#_Toc151928782)

[3.实验小结 4](#_Toc151928783)

[4.课程意见与建议（可选） 5](#_Toc151928784)

1.严格按照模板格式包括行距、字体、段落格式等等，来写 不按照模板来，严重扣分!

2.封面要一致(上面有评分项)

3.封面 目录 内容 总结

4.评分分为：撰写规范性 实验过程 问题分析与小结

5.必须双面打印，单面打印属于规范不及格！

6.请打印前去掉本说明。

# Linux平台漏洞攻防工具使用

## 实验目的

* 掌握Linux进程的原理；
* 了解ELF可执行文件格式与载入原理；
* 掌握知名反汇编工具的工作原理与使用方法；

## 实验要求

* 编写代码独立解析ELF文件，获取ELF文件元信息；
* 需独立使用进程分析工具分析给定ELF的进程地址空间。
* 以小组为单位完成对ELF程序的逆向分析后获取flag

## 实验环境

* 实验平台：pwn.hust.college
* 操作系统：Ubuntu 20.04
* 分析工具：IDA free version

## 实验过程记录

注意：每个实验按照这四个部分写，难点与问题分析以及小结2个实验写在一起。大家注意实验报告页码最长不超过25页。

# 栈保护机制绕过与漏洞利用

## 实验目的

* 掌握反汇编代码分析工具分析原理与使用方法；
* 掌握栈溢出和 Stack Canary 的原理；
* 掌握栈溢出漏洞的利用技巧和 Stack Canary 的绕过手法；
* 理解栈溢出漏洞的防范措施；

## 实验要求

* 调试与掌握函数反汇编执行流程
* 定位程序溢出点
* Stack Canary 爆破绕过，劫持程序控制流；
* 编写 ROP 链，获取具有任意命令执行功能的 Shell

## 实验环境

* 实验平台：pwn.hust.college
* 操作系统：Ubuntu 20.04
* 溢出软件：mitigation-bypass
* 溢出工具：pwndbg，vscode，XFCE桌面，bash命令行

## 实验过程记录

# 2.实验遇到的难点与问题分析

# 3.实验小结

# 4.课程意见与建议（可选）