# 栈溢出利用的分析

进行以下文献阅读、实验操作和代码（指令）分析，撰写分析报告。

1. 阅读 buffer_overflow.pdf 的第 4.1～4.7 节，理解栈溢出攻击的原理。

2. 按照 README，运行 exploit 程序，生成 badfile。利用 xxd 分析 badfile，同时分析 exploit.c 源代码，理解并解释为什么程序能够生成 badfile 的内容。

3. 按照 README 运行 stack 程序，实施栈溢出利用，观察 shellcode 的执行效果。

4. 详细分析 stack.asm 中的 main 函数及 bof 函数对应的汇编指令序列，画出从 main 起始到调用 bof 函数执行、再到返回 main 的过程中关键的栈状态。解释这些关键的栈状态，说明栈溢出攻击是如何实现的。（需要画出并解释的栈状态包括但不限于：call fread 后，call bof 前，bof 内 call strcpy 前，bof 内 call strcpy 后，bof 内 ret 前，从 bof 返回 main 后）。

注：要求自己画栈状态，禁止从阅读材料中复制。

4. 提交要求：

截止时间：4 月 17 日 23:59:59。

形式：分析报告（word 或 pdf），内含以上要求的分析内容、关键栈状态图（不限画图软件，但必须自己画，粘贴到报告中）和对攻击过程的解释。

提交到助教邮箱（见第一次课“intro.pdf”），邮件标题：“[学号]姓名-软件与系统安全作业 1”。