CLASS 4

Format String Lab 2

吴瑞欣-E41614059

1、 解释 gcc 参数-fno-stack-protector 的含义，gcc 的参数里面与 stack overflow 相关的还有哪些？

-fstack-protector：
启用堆栈保护，只为局部变量中含有 char 数组的函数插入保护代码。
-fstack-protector-all：
启用堆栈保护，为所有函数插入保护代码。
-fno-stack-protector：
禁用堆栈保护。

2、 （一定要看）非常仔细地阅读 Smashing The Stack For Fun And Profit.

http://www.cs.wright.edu/people/faculty/tkprasad/courses/cs781/alephOne.html

文章详细解释了什么是堆栈，堆栈的原理、缓冲区溢出，以及 exploit 利用。

堆栈是计算机科学中经常使用的抽象数据类型。一堆对象具有放置在堆栈上的最后一个对象将被移除的第一个对象的属性。此属性通常称为后进先出队列或 LIFO。堆栈上定义了几个操作。其中两个最重要的是 PUSH 和 POP。PUSH 在堆栈顶部添加一个元素。相比之下，POP 通过删除堆栈顶部的最后一个元素将堆栈大小减少一个。

堆栈是包含数据的连续内存块。称为堆栈指针（SP）的寄存器指向堆栈的顶部。堆栈的底部位于固定地址。其大小在运行时由内核动态调整。

缓冲区溢出是将更多数据填充到缓冲区而不是它可以处理的结果。

3、 阅读下面两篇文章的同时，熟悉一下 gdb 基本操作，看汇编设断点查看内存之类的基本操作了解一点。

http://seanmurphree.com/blog/?p=157

https://tomasuh.github.io/2015/01/19/IO-Wargame.html

Level 3 部分

在 gdb 中运行 list 命令（缩写 l）可以列出代码
在 gdb 中，运行程序使用 run 命令。
在 gdb 中用 break 命令来设置断点
在调试过程中，next 命令用于单步执行

4、 解释 linux 用 root 执行下面这条命令：

sysctl -w kernel.exec-shield=1 的含义和用途。

kernel.exec-shield 用来控制能否执行存储在栈中的代码，其值为 1 时表示禁止；为 0 时表示允许；默认为 1，表示禁止执行栈中的代码