PWN 第一次作业

November 28, 2019

1 ex1, 1pt

hint: 这是一道简单的栈溢出题目, 你需要通过溢出覆盖相应局部变量为需要的值. 可以通过 IDA 进行反编译分析.

2 ex2, 1pt

hint: 这是一道利用栈内残留信息的题目, 你可以通过 IDA 进行反编译分析, 利用 gdb 调试来找到适当的偏移位置.

3 ex3, 3pt

hint: 这是一道栈溢出覆盖返回值的题目, 结合了 printf 获取内存信息的简单用法. 你可以通过 IDA 进行反编译分析, 利用 gdb 分析内存的组织结构比如 canary, 返回地址.

注意程序自己设置了一个栈溢出保护器, 编译选项 `-fstack-protector` 又设置了一个, 请上网搜索该选项的作用. 另外请确保你实验的 Linux 系统开启了 ASLR (`echo 2 | sudo tee /proc/sys/kernel/randomize_va_space`), 否则你的方法可能会不正确.

4 提交要求

请注意保存实验的脚本, 分别命名为 ex1.py, ex2.py 和 ex3.py 以便重现.

实验报告命名为 学号-姓名-`PWN1.pdf`. 报告中可以讲解一下解题思路, 如有必要可以配上截图, 如果没有做出来也可以写一写你遇到的困难和对题目的思考.

将实验报告和实验脚本打包为 学号-姓名-`PWN1.zip`.

截止日期: 2019/12/10 22:00, 请提交到课程网站.