ROP 攻击实验

网络与系统安全综合实验

实验截止: XXXX.xx.xx 星期 X 23:59

概要

本手册主要介绍 ROP 攻击实验的相关内容，并推荐常用工具及使用方法。

1 实验相关

1.1 实验内容

本次实验为网络与系统安全综合实验第一次实验（以下称为 Lab1），主要内容是 ROP 攻击方法的利用。Lab1 一共包括四个题目：

- lab1-1: got hijack
- lab1-2: rop
- lab1-3: rop
- lab1-4: rop

1.2 提交内容

Lab1 需要提交实验报告 (PDF/Word) 和每道题目的解题脚本，实验报告需要完整反映题目解答过程和最后的答案，实验报告和解题脚本一同压缩为.zip 格式上交。

```
命名格式:
压缩包: lab1-学号-姓名.zip                    e.g. lab1-17000000001-张三.zip
报告:   lab1-学号-姓名.[doc/pdf]              e.g. lab1-17000000001-张三.pdf
脚本:   lab1-[1-4].[c/py/...]       e.g. lab1-2-17000000001-张三.py
```

2 工具相关

推荐一些常用的调试/ROP 常用工具。

gdb 插件 peda 或者 pwndbg

```
# PEDA
git clone https://github.com/longld/peda.git ~/peda
echo "source ~/peda/peda.py" >> ~/.gdbinit
# PWNDBG
git clone https://github.com/pwndbg/pwndbg
cd pwndbg
./setup.sh
```

pwntools

```
pip install pwntools
```

ROPgadget and ropper

```
pip install ropgadget
pip install ropper
```