GDB--基本命令

GDB

- gdb level1: gdb调试level1程序的命令
- run: 执行
- disas f*A：反汇编 函数f*A
- break *0xdeedbeef: 在0xdeedbeef位置设置断点
- info breakpoint: 查看已经设置的中断点
- info register: 查看所有的register状态
- x/wx address: 查看address中内容
    - w 可以换成 b/h/w/g 分别代表 1/2/4/8 byte
    - x/100wx: 一次列出100个字
    - 第二个x 可换成u/d/s/x/w（用哪一个取决于该内存地址存放哪种类型的值）
        - u: unsigned int
        - d: 10进制
        - x: 16进制
        - s: 字符串
        - i: 指令
- ni – 执行完下一条指令
- si - 执行完下一步指令
    - ni遇到调用函数，可以把函数执行完；而si会陷入到函数
- backtrace - 显示上层所有stackframe的信息
- continue - 继续执行程序，直到程序结束、程序崩溃或者断点
- set *address = value
    - address的值一次设置4个byte
    - 可换成char,short ,int ,long 表示 1，2，4，8个bytes
    - set [int]0x80408000 = 666
- attach pid：attach 一个正在运行的process

在有debug symbol的时候：

- list：可以列出源代码
- b： 按行号加断点
- Info local： 列出区域变量
- print val： 打印区域变量值

GDB-peda

- checksec – 查看二进制文件中的保护机制
- elfsymbol - 得到每个plt的地址（ROP的时候用得到）
- vmmap - 查看进程内存的分配以及各地址的权限
- readelf - 查看每个section的位置
- find /bin/sh - 查找字符串“/bin/sh”的位置