缓冲区溢出漏洞实验

1．NOP 全称 NO Operation，意思就是无操作既空指令，在 x86 的 CPU 中机器码为 0x90（对应 10 进制为 144）

2．gdb 反汇编可用 disassemble / disass 命令。用法如下：

disassemble

disassemble [Function]

指定要反汇编的函数。如果指定，反汇编命令将产生整个函数的反汇编输出。

(gdb) disassemble main

disassemble [Address]

3．使用“i r”命令显示寄存器中的当前值，其中“i r”即“information register”

esp：栈顶指针，指向栈的顶部。

4．gdb 相关命令：

(gdb) b 2	将断点设置在 12 行
(gdb) run	运行程序
(gdb) n	单步执行
(gdb) n 2	执行两次

其中，run 可以简写为“r”，next 可以简写为“n”