# [Rop攻击](http://www.cnblogs.com/long123king/p/3580269.html)

参考：[http://en.wikipedia.org/wiki/Return-oriented\_programming](http://en.wikipedia.org/wiki/Return-oriented_programming" \o "http://en.wikipedia.org/wiki/Return-oriented_programming" \t "/home/taqini/Documents\\x/_blank)

Rop全称Return-Oriented Programming，就是对栈上的返回地址进行利用的一种攻击方式。

对于栈的利用经历了几个阶段，都是在“道高一尺，魔高一丈”的正邪较量中不断地升级地。

#### 1. Stack Smashing Attack

简单版本，主要是覆盖返回地址，将其指引到自己构造好的shellcode中去。

因为自己的shellcode通常是存储在数据之中，所以可以通过DEP的机制来防御这种攻击。

#### 2. Return Into Library

既然无法使用自己构造好的shellcode，那么就可以复用已经写好的library代码，因为这些代码是被信任地，加载到可以执行的内存区域中去的。通过精心构造的栈传递特定参数来调用library中特定函数的方式，来构建有效的攻击逻辑。

这种机制可以通过限制library中的函数的破坏性的方式，以及64系统带来的新的函数调用方式（函数调用的第一个参数不再是通过栈传递，而是通过寄存器传递）来防御。

#### 3. Borrowed Code Chunk

这一机制通过查找library中特定的指令序列，通过这些指令序列将构造好的参数传递到寄存器和栈中来完成攻击。

#### 4. Return-Oriented Programming

通过查找library中的代码来构造出可以执行任意逻辑的攻击链。

有两种方式来防御：

ASLR, Address Space Layout Randomization, 通过随机化地布局library加载到内存中的地址，来增加构造攻击链的难度。

kBouncer, 通过检查返回指令是否返回到一个立即调用call指令的位置的方式来监控是否有攻击链的行为，缺点是性能太差。