<http://www.cnblogs.com/xingyun/archive/2011/12/10/2283149.html>

<https://hardenedlinux.github.io/system-security/2016/07/01/PIC_PIE_and_ASLR_analysis.html>

PIE相关

多数文件可以通过静态分析和动态调试找到内存里的关键地址。但是部分ELF文件通过编译能随机化变量的存储地址，从而达到隐藏和保护的目的。ELF的文件中有可链接化的相关内容，因此可以使用GOT/PLT技术进行操作。

进行了GOT/PLT技术处理的文件，会在第一次调用部分函数的时候优先在内存中开辟一块地址，将所调用函数的寄存器及内存中相关信息存入那块地址中，以便于下次调用时直接取出地址进行调用。

GOT/PLT是PIE的基础，在编译时进行一些相关设定就能将文件以这种方式编译出。而相关内存中地址时则可以通过一些libc中的相关函数获得