RELRO

> RELocation Read-Only, 重定位只读

- **部分 RELRO**: 在程序装入后，将其中一段 (如`.dynamic`) 标记为只读，防止程序的一些重定位信息被修改
- **完全 RELRO**: 在部分 RELRO 的基础上，在 程序装入时，直接解析完所有符号并填入对应的值，此时所有的 GOT 表项都已初始化，且不装入`link_map`与`_dl_runtime_resolve`的地址 (二者都是程 序动态装载的重要结构和函数)。

Canary

> 金丝雀

插入一个值在 stack overflow 发生的高危区域的尾部。当函数返回之时检测 Canary 的值是否经过了改变，以此来判断 stack/buffer overflow 是否发生。

NX

> non-execute

`NX(Non-eXecute)`位是一种针对 shellcode 执行攻击的保护措施，意在更有效地识别数据区和代码区。通过在内存页的标识中增加" 执行" 位，可以表示该内存页是否执行，若程序代码的 EIP 执行至不可运行的内存页，则 CPU 将直接拒绝执行" 指令" 造成程序崩溃。

PIE(?)

> Position-Independent Executable, 位置无关可执行文件

技术与 ASLR 技术类似，ASLR 将程序运行时的堆栈以及共享库的加载地址随机化，而 PIE 技术则在编译时将程序编译为**位置无关**，即程序运行时各个段加载的虚拟地址也是在装载时才确定。