Stack：先进后出

|  |  |
| --- | --- |
| Main\_addr | 返回main重新开始 |
| Puts\_plt | Plt地址  用来运行puts |
| Puts\_got | Got表地址 |
| Pop\_rdi | 寄存器压栈 |
| b(0x57)  …  … | 溢出覆盖返回地址 |
| b | 溢出 |
| \0 | Strlen读到“\0”停止 |

|  |  |
| --- | --- |
| system |  |
| Binsh |  |
| Pop\_rdi |  |
| Ret | 栈对齐 |
| b(0x57)  …  …. |  |
| b |  |
| \0 |  |