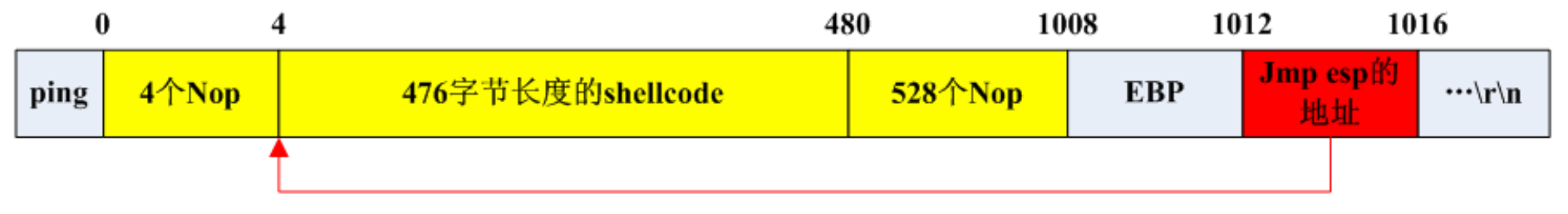
CCproxy缓冲区攻击

缓冲区攻击主要分为两步，首先是dbg确定ret地址存放的位置，确定攻击策略；其次是写攻击代码，注入shellcode，完成攻击。

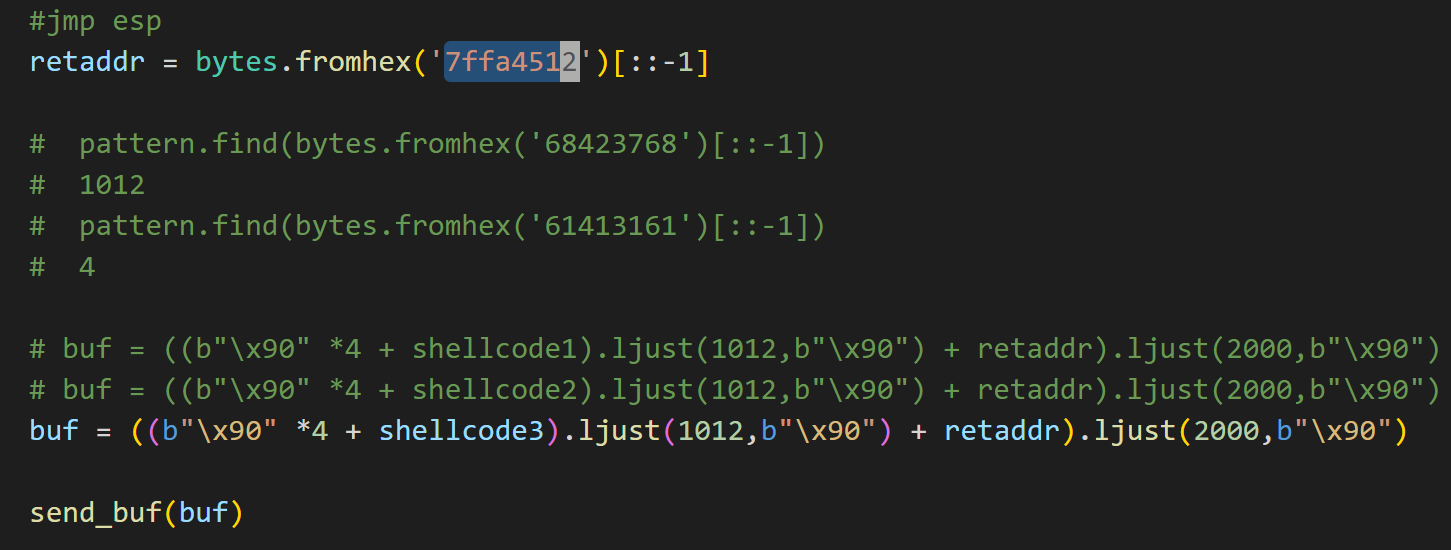
一、用dbg确定攻击策略

1. 打开ccproxy
2. 用dbg连接
3. telnet连接
4. ping 一段不重复的字符串（用于第6步）
5. 在dbg查看eip和esp，根据eip的值可以确定ret的位置，因为函数返回的时候是直接将ret处的值赋给eip，所以当程序崩溃的时候，查看eip的值可以确定ret在缓冲区中的位置，实际操作中得到的值是1012，也就是要把转移控制流的字符串放在1012的位置。选择用jmp esp指令来转移工作流，通用的jmp esp指令的地址为“7ffa4512”。因此把这个字符串放在1012的位置，程序会跳转到esp的值的地方，同样的查询方法可以确定程序崩溃时esp指向的位置在缓冲区中是4，因此可以把shellcode放在缓冲区的第4个位置。
6. 根据第5步可以确定攻击策略：



二、完成攻击

1. 写攻击代码，代码地址在git@github.com:Aganhui/ygh-ccproxy-buffer.git
2. 打开ccproxy
3. telnet连接
4. 发送包含shellcode的buf字符串



1. 完成攻击