[zz]"西厢计划"技术解析 ⧉

从 farseerfc.wordpress.com 转载

文章版权归原作者所有。以下是正文。

原文：http://blog.youxu.info/2010/03/14/west-chamber/

声明：本文是一篇技术文章，不涉及任何政治立场。

前几天，一个名为西厢计划的"过滤系统"，在技术达人的圈子里头颇是火了一阵。不过火爆了几天，却很快又烟消云散。技术圈子里面都在议论这到底是不是一个骗局。作为一个技术人员，从技术的角度仔细分析一下这个所谓的西厢计划到底能做什么，应该是件蛮有意思的事情，于是便有了本文。

我们知道，目前国内最主要的互联网封锁技术，是依靠发送伪造的 TCP Reset 包来中断正常的连接的。当检测到敏感词时，就会发送 Reset, 让连接双方都误认为是对方断开了连接，这样用户就无法正常访问被封锁的地址了。国内封锁的特征是发送 Reset 包 (对于 Linux, 具有 root 权限，通过 iptables, 可以很容易地过滤掉 Reset 包。)而正常连接不会发送 Reset, 因此只要能分辨正常与不正常的封锁，过滤掉 Reset 包，封锁问题就迎刃而解。过滤掉这些发送的 Reset, 中断连接的目的便不能达到，这样便实现了突破封锁的可能性。这并不是什么高深技术——但是需要特别指出的是：TCP 协议是个双向的协议，通讯双方，你过滤掉了发给你的这个包，你的通讯对方那里却仍然会收到一个"伪造"的数据包，这样依然会导致连接中断，换句话说，封锁依然

□□

　　□□ □□□"□□"□□□"□□□□□□□"□□ TCP □□□□□□□□□□□□□□ □□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□ TCP □□□□□□□□□□□□□□□□□□□"□□"□□□□□□□□□□□□□□□□□□□□□"□□□□□"□□

　　□□□□□□□□□ TCP □□ TCP □□□□□□□□□□□□□□□□□□□□□□□□□□□ TCP □□□□ RFC□□□□□□□□□□□□□□□□□□□□□□□□□□□ TCP □□□□□□□□□□□□□□□□□□□□□□ □□□□□□□□□□□□□□□□□□□□□□□ SYN/ACK □□□□□□□□□□□□□□ ACK □□□□□□+1 □□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□ +1 □ FIN □□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□ FIN □□□, □□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□(□□ ma de in china, □□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□ SYN/ACK □□ □□

　　□□ □□□□□□□□□□□□□□□□□□□□□ RFC, □□□□□□□□□□□□□□ RFC □□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□ SYN/ACK □□□□□□□□□□□□□□□□□□□□□+1 □ ACK□□□□□□□□□□+1□□□□□ ACK □□□□□□□□ □□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□ ACK □□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□ RFC □□□□TCP □□□□□□□□□□□□□□□□□□□ Reset. □□□□□□□□□□□□□□ Reset□□□ Reset □□□ Reset □□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□ ACK, □□□ □□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□

　　□□□□□□□□□□□□□□□□"□□"□□ DNS□□□□□ DNS □□

在 Linux 上运行 的嵌入式设备。写一个运行在 Linux 内核的 netfilter, 在 Linux 内核协议栈中实现数据包的过滤和修改是很好的选择。 当然也可以在用户空间通过 libpcap 和 libnet 来实现，不过性能会差一些，而且需要自己处理很多协议栈的细节。总之，网络编程的世界很精彩，欢迎来到 Linux 世界 :)

PS 1: 关于网络抓包工具的使用，可以参考http://img.ly/Dli
　　PS 2: 关于 TCP 协议的细节，可以参考相关书籍或者查阅相关资料
　　PS 3: 关于网络编程的更多内容，欢迎大家一起讨论交流
　　PS 4: 关于本文的任何问题，欢迎大家指正，也可以自行搜索Google。