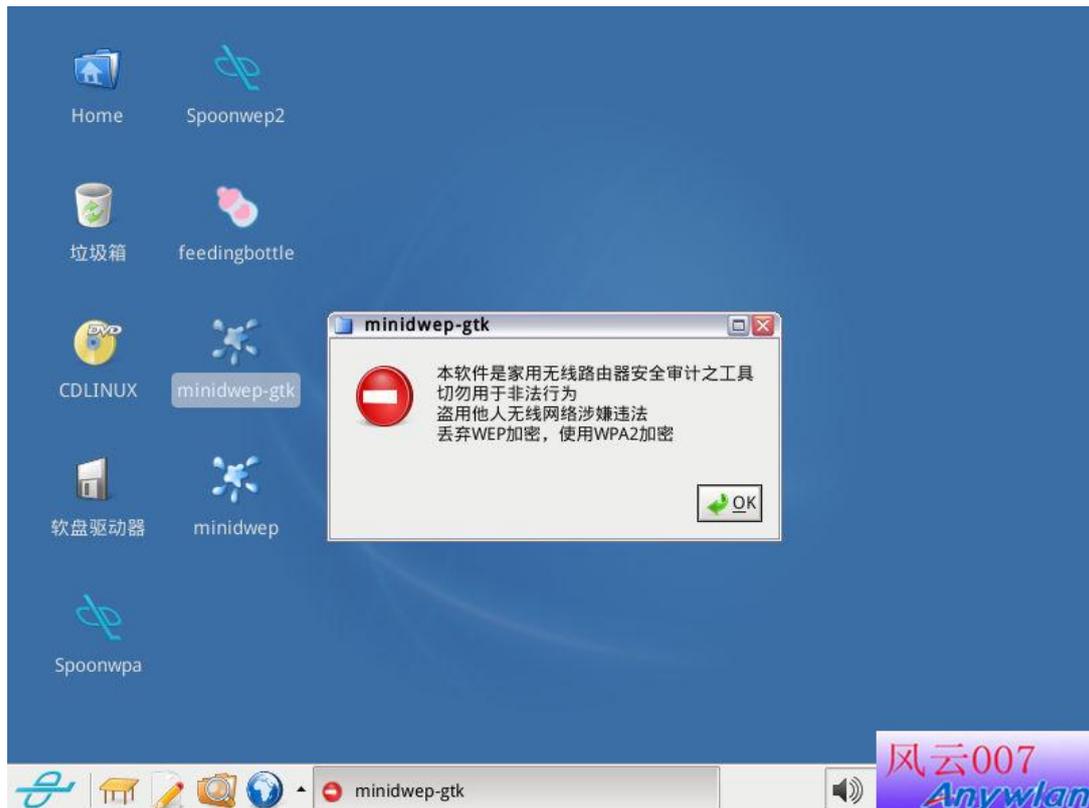


minidwep-gtk 的 WEP 加密安全性研究

启动 CDlinux 后在桌面的 minidwep-gtk 图标上点击鼠标的右键选择执行



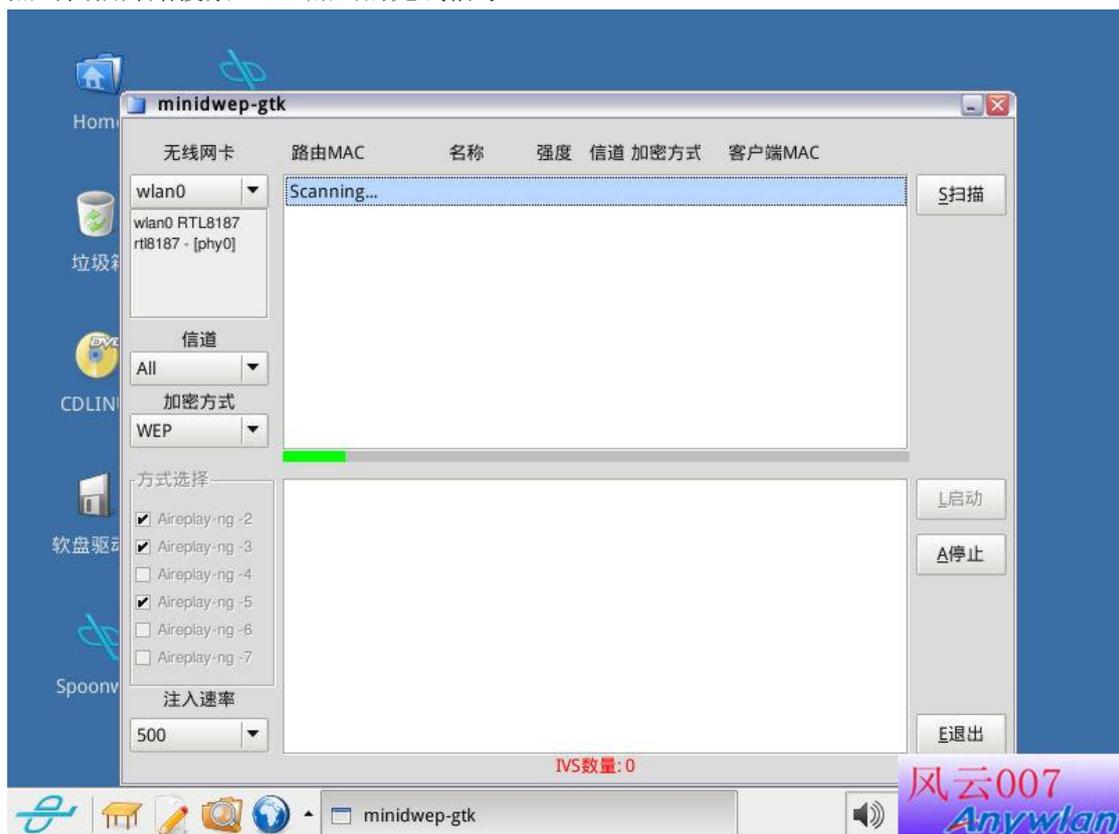
执行后跳出一个警告的对话框，点 OK 就可以了！



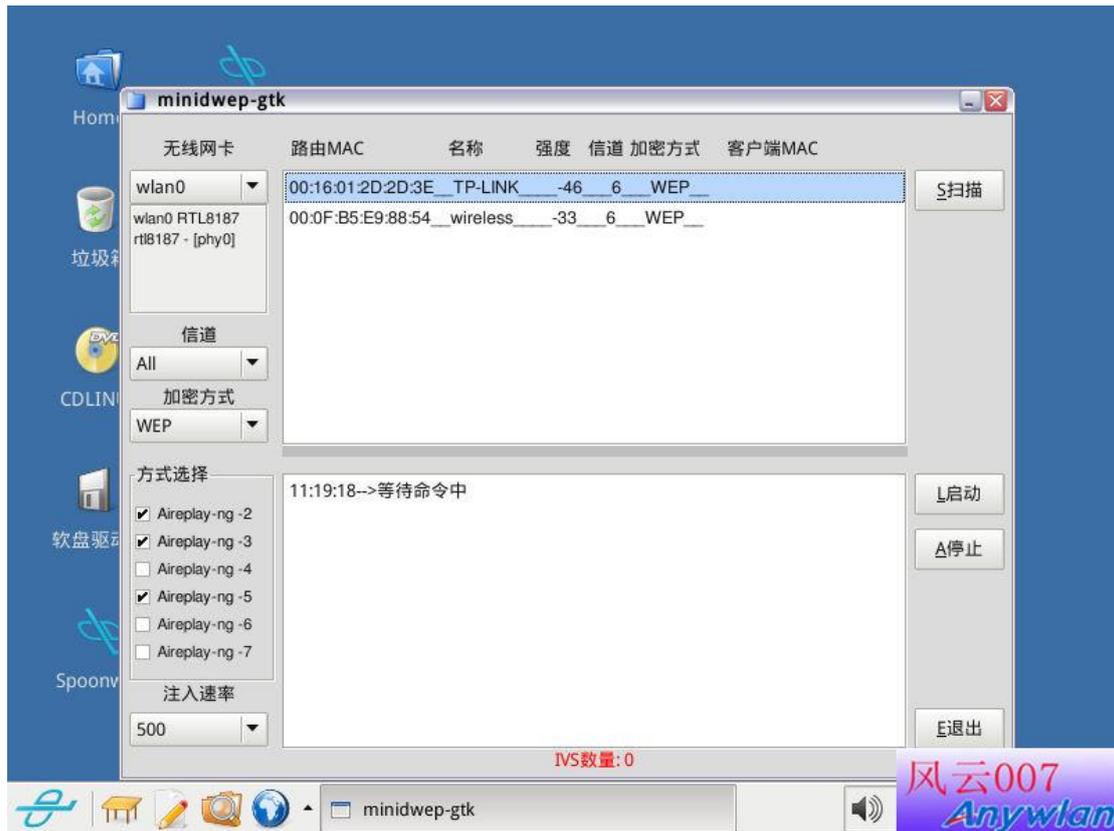
启动完成



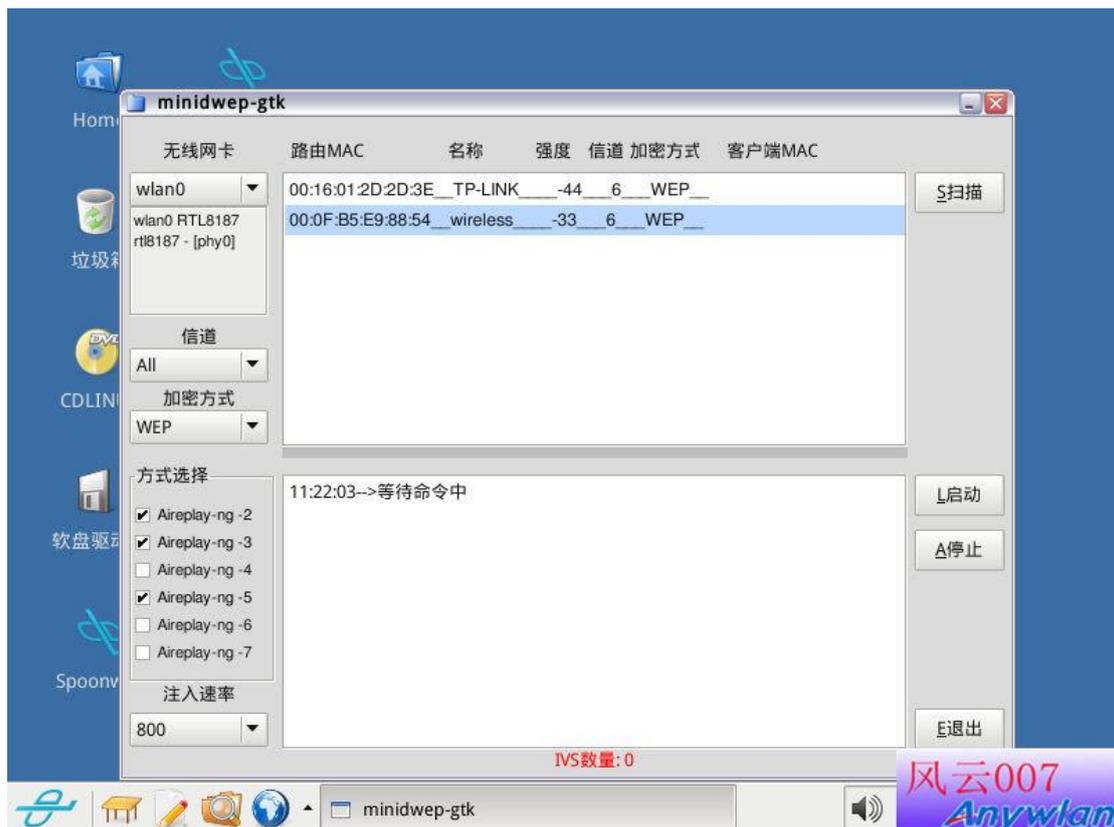
点击扫描开始搜索 WEP 加密的无线信号



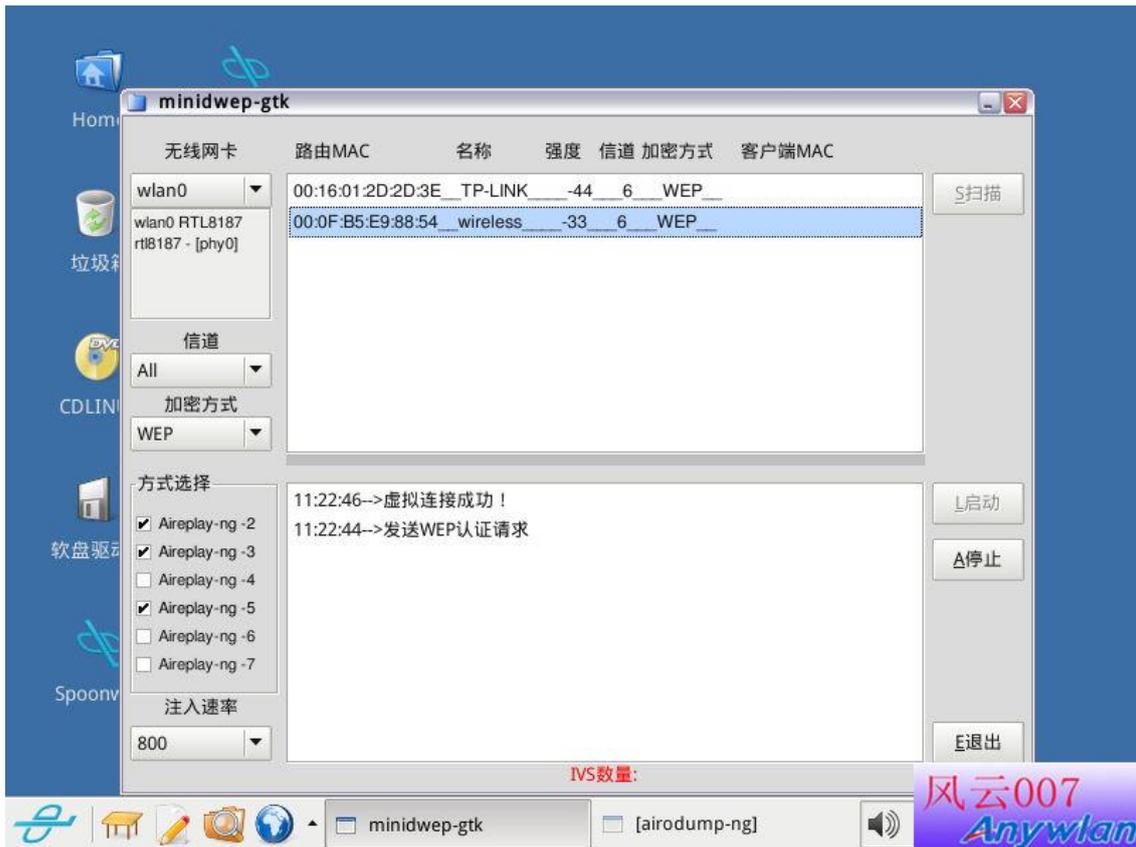
片刻后扫描到 2 个 wifi 信号



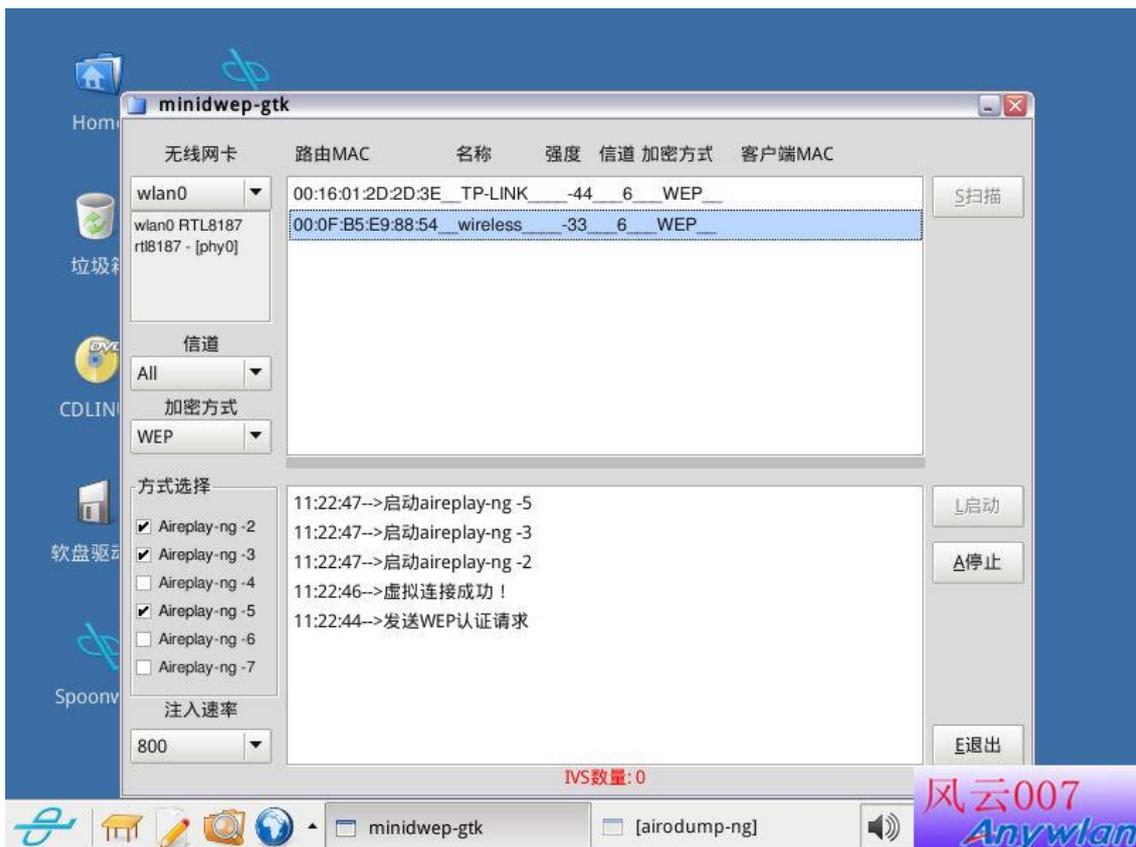
信号强度为负数显示，选择信号强度高的一个准备破解，攻击方式默认-2、-3、-5，注入速度设置到最高 800 ， 最后点击启动开始自动破解.....！



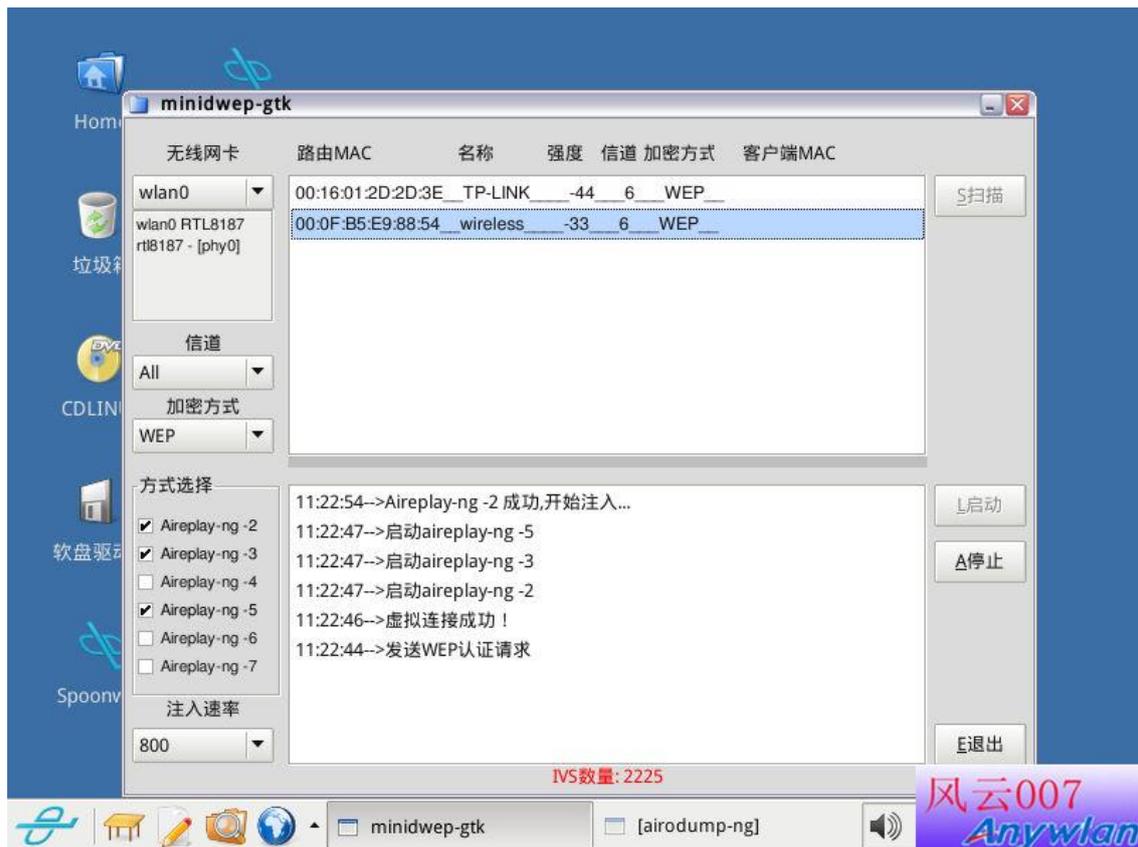
自动开始进行虚拟连接.....后面的事情就不需要我们参与了!



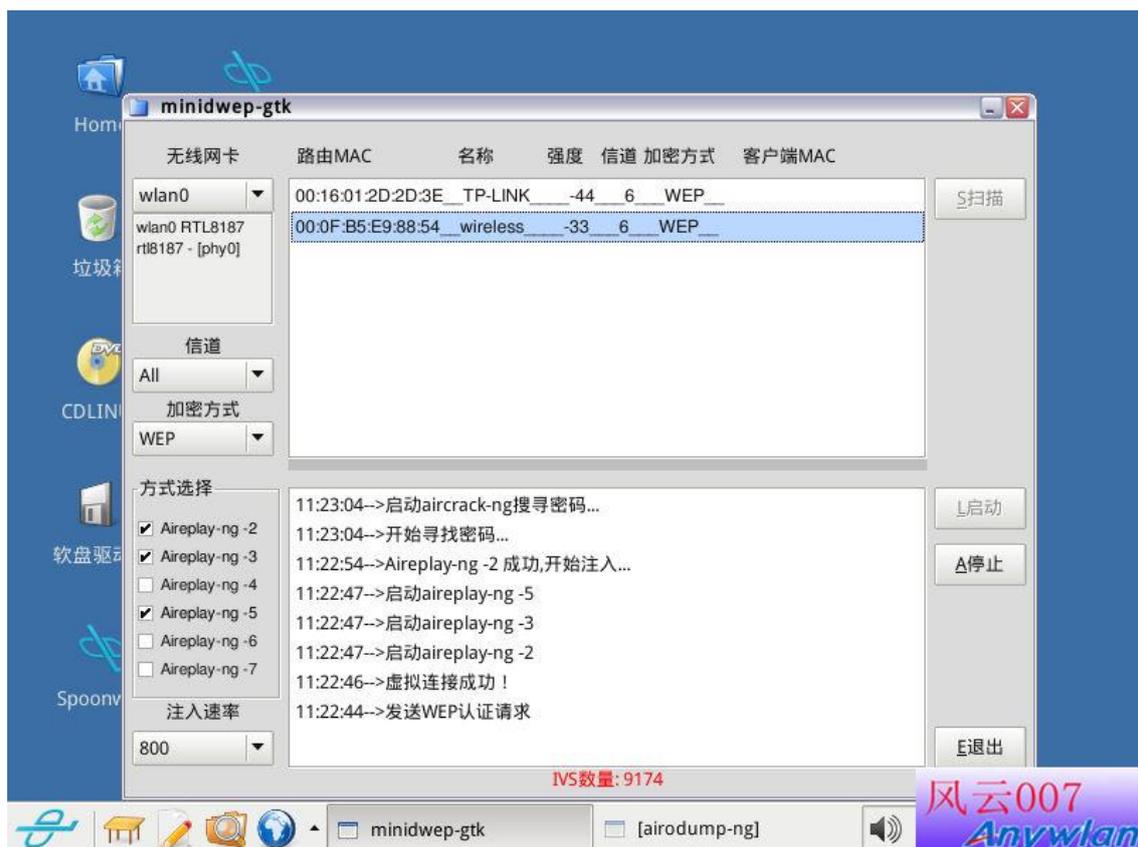
同时发动-2、-3、-5 的攻击.....



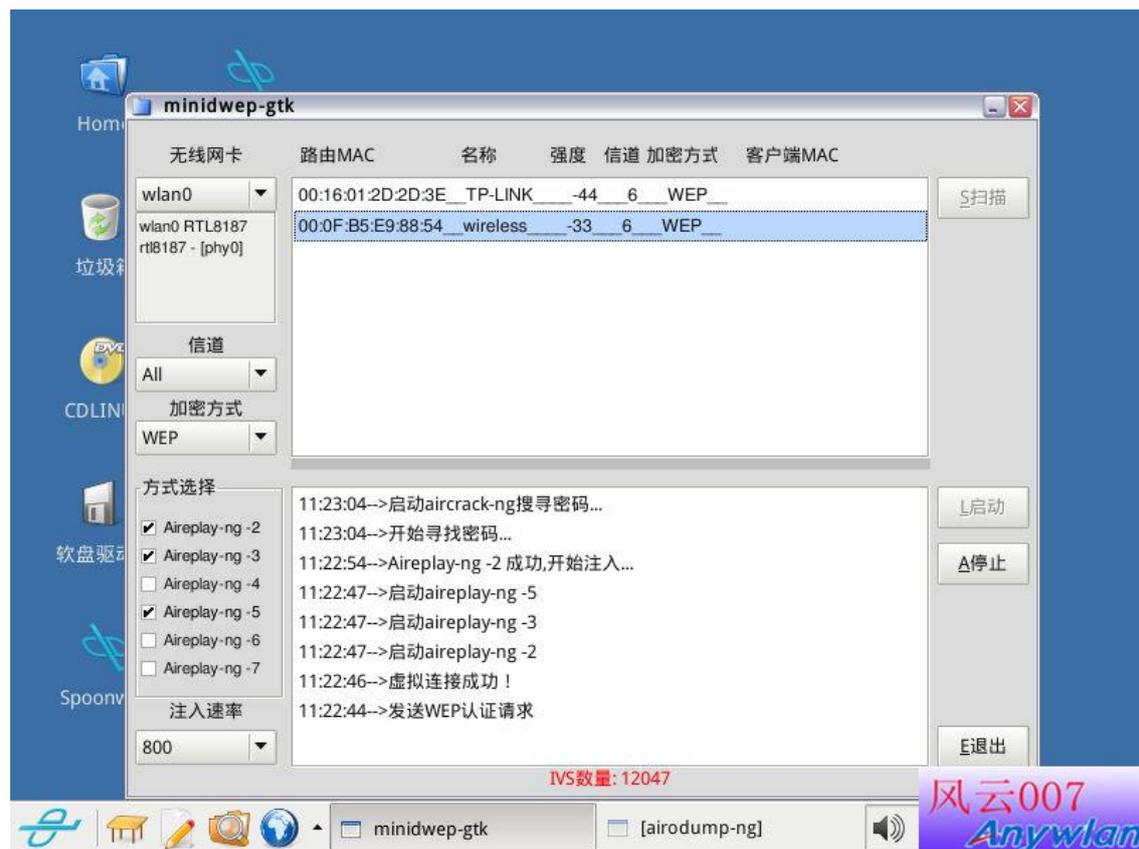
-2 攻击注入成功，IVS 的数值开始快速增长，这个时候破解密码就是时间的问题了。



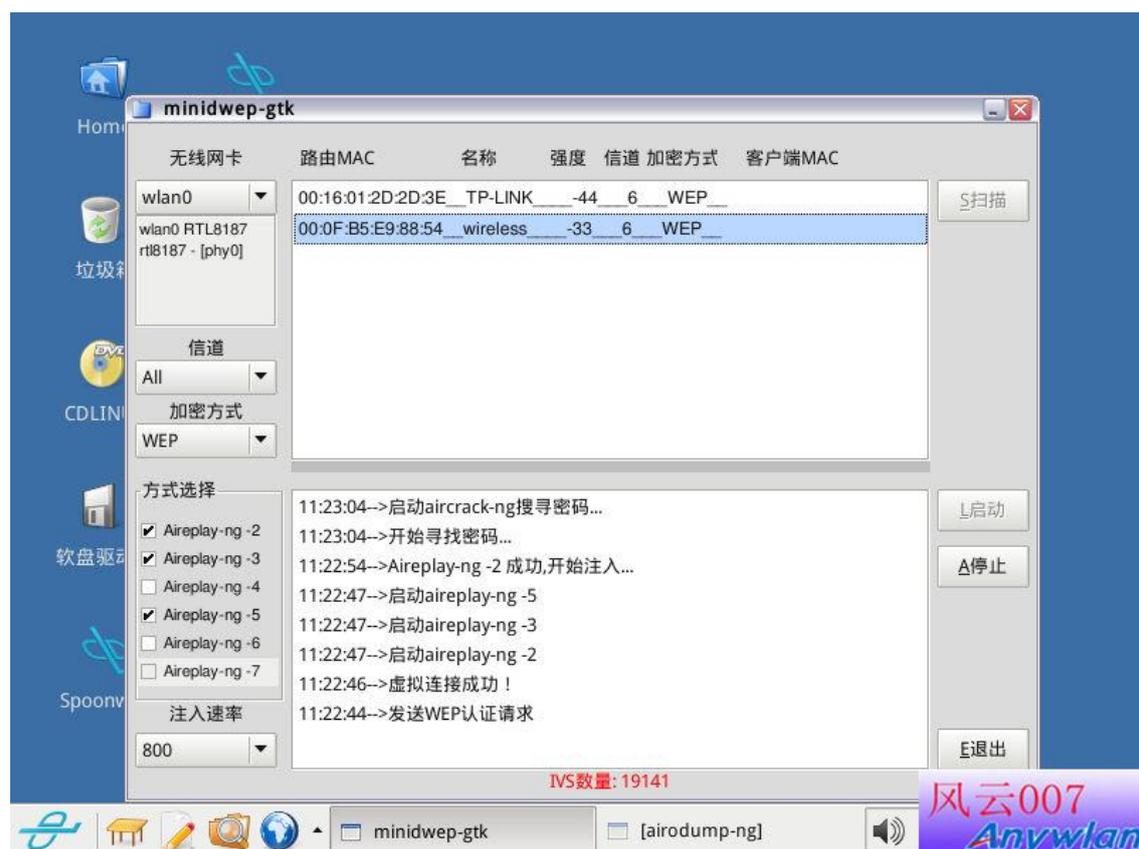
IVS 的数值继续快速增长，并且在超过 6000 后就自动启动 aircrack-ng 搜寻密码。



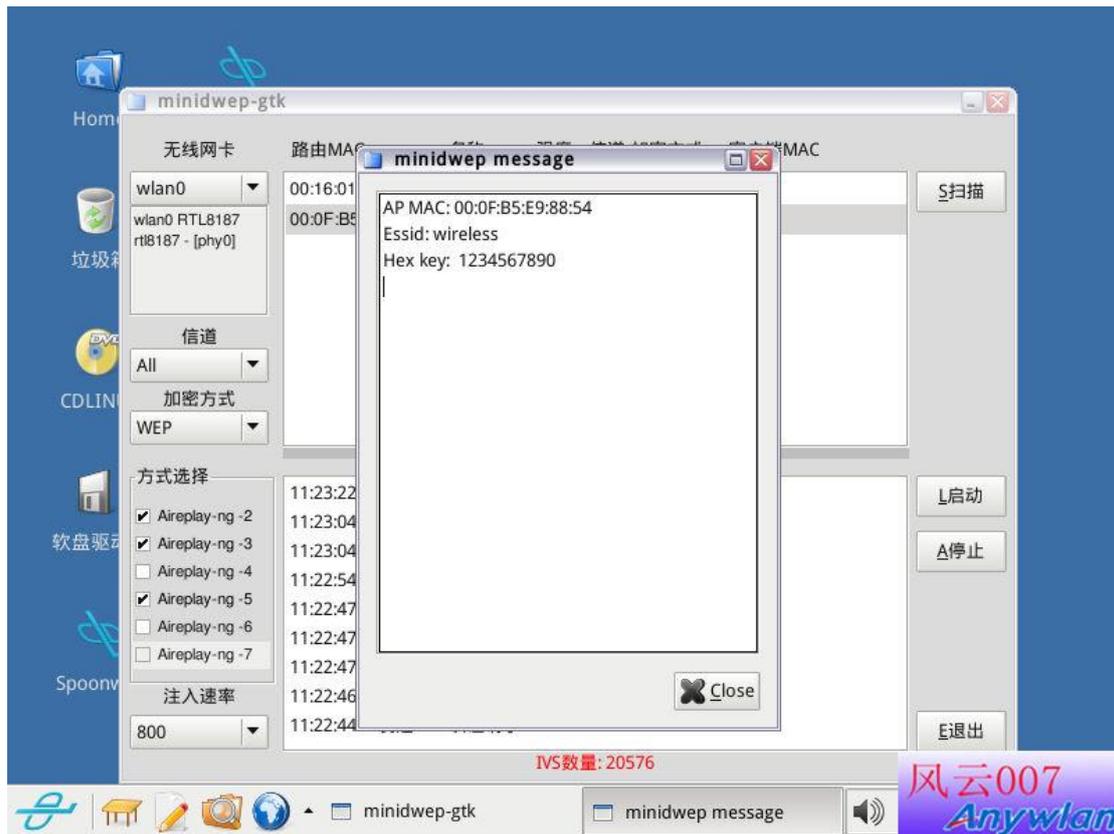
密码还没有计算出来继续搜集 IVS 数值.....



IVS 数值快速增长中.....



搜集一定数量的 IVS 密码就会自动就会跳出来，KEY：后面显示的就是密码。
这个教材里面的密码比较简单并且是 64 位的加密，所以速度很快。



欢迎假如QQ技术交流群 114705111