详析如何破解路由 Wi-Fi 密码

写在前面

对于黑客，很多人又爱又恨，看见他们熟练的敲击键盘，屏幕中不停滚动鸟文最后 loading 的时候，我们常常羡慕不已，it's so cool！大家一定有过这样的疑问，黑客技术一定很难吧？其实，就像去年小编整理的“黑客三大必杀技”里的总结的那样：骨灰黑客不再需要技术，而是更灵活的头脑。

告诉你，简单的 hack 并不难，学会了今天这一招，让你也过一把黑客瘾！

该教程源自网络，经小编整理。虽然没有视频教程，但说实话这个过程一点不复杂，目的就是通过扫描获取路由器 pin 码（就是第一次连接新路由时要我们输入的那个 8 位编码，一般路由器底部会标出），有了 pin 码，你懂得。方法简单，大家不妨一试，会的同学和高手自动忽略吧，不喜轻喷。

如今，Wi-Fi 信号满天飞，但是看似加过密的路由就真的安全么？或者你摒弃了 wep 加密，以为使用了 wpa2 就可以高枕无忧么？你知道我想说什么，既然是破解教程，就证明你的想当然已经错了。不过，还是那句话，分享这些，并非是希望大家去蹭网，搞破坏，而是希望教会大家如何从中学会保护你的无线网络。

破解的基本理论

由于 wpa2 的出现，以前抓包跑字典这种传统而粗暴的方式已经无法满足日益增长的蹭网需求（呃~），为此，pin 码入侵的时代华丽到来。

pin 码，简单的说就是识别码，路由上的为 8 位纯数字，只要你知道对方的 pin 码，就可以轻松接入无线网络。理论上，pin 码可以设置为随机任何一个 8 位数的数字，但是这 8 个数字可以用穷举法进行破解，并且无线路由默认的 pin 码是存在规律的，如果不进行修改，这就给蹭网提供了便利。

规律是这样的：pin 码分为前 4 位一组，后 3 位一组，之所以可以这么分是因为在 pin 的时候，会产生返回码，从返回码里对前 4 位进行识别。也就是说，前 4 位的验证跟后 3 位没关联，可以一开始单独对前 4 位进行拆解。前 4 位总共 10000 个组合，而后 3 位一共 1000 个组合，最后一位是根据前 3 位计算得出的，如果懒得计算，也可以从 0-9 每个试一次，也不费什么时间，也就是说，这世界上所有无线路由的 pin 码，只有 11010 种可能。用穷举法，假设一秒试一个，全部测试完毕也就 3 个小时而已，可以说花费时间还是比较短的。

而部分厂商为了使出厂的无线路由拥有唯一 pin 码，就会根据无线路由的 mac 进行计算，得出 pin 码，因为 mac 是唯一的，既然是计算得出的，自然就能求出加密方程式，比如有些不靠谱的厂商，使用 mac 后 6 位十六位进制转成十进制，得出前 7 位，也就直接得到 8 位 pin 码。依稀记得就是前几年的事，这些厂商的设备不断被入侵和曝光，有心的人发现：mac 前 6 位相同的，pin 码前 4 位就有可能是一样，但是不同批次的产品也可能不同，不过确实存在规律性。这样就把入侵花费的时间大大降低，1000 个可能性，不到 20 分钟就能全部测试，并且当时有人专门成立了一个网站，全国范围内收集 mac 和成功破解的 pin 码，研究各大无线路由厂商的 pin 码计算公式。

支持 pin 码的路由基本上都会带一个叫做 WPS（Wi-Fi Protected Setup，是一种 Wi-Fi 联盟提出的无线安全防护标准）的功能，简单来说就是为了实现快速连接，现在我们能利用 pin 漏洞，完全要归功于这个功能，防护标准最后却为人利用，我们也只能呵呵了。另外，还要用到一个 QSS 接入程序，网上可以搜到，windows 7 系统已自带。

破解需要准备的东西

1、硬件环境：一个外置高增益信号的大功率无线网卡 一台电脑

2、软件环境：网卡驱动 wm 虚拟机 bt3 xiaopan 等 linux 系统镜像

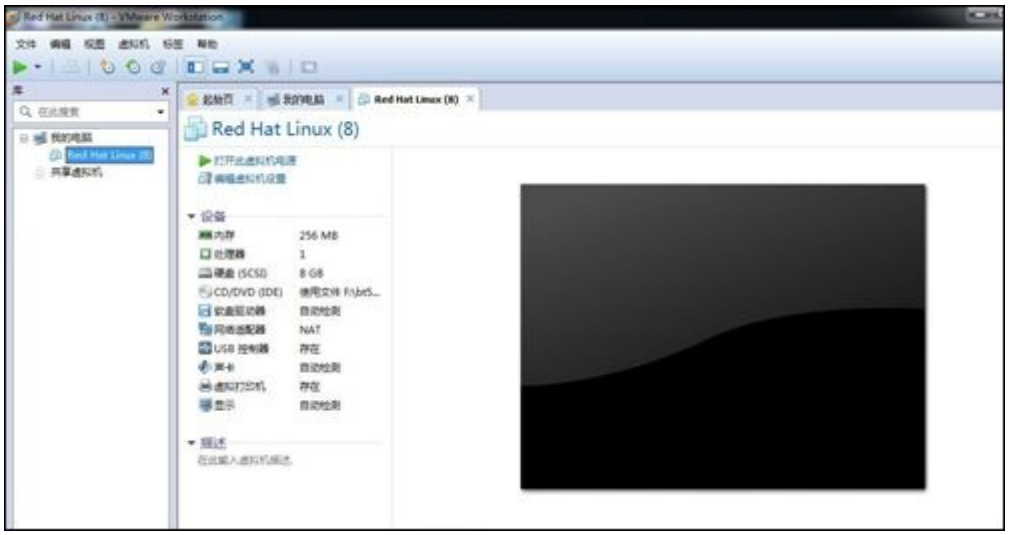
破解教程，如何应对 pin 码入侵回顶部

破解教程

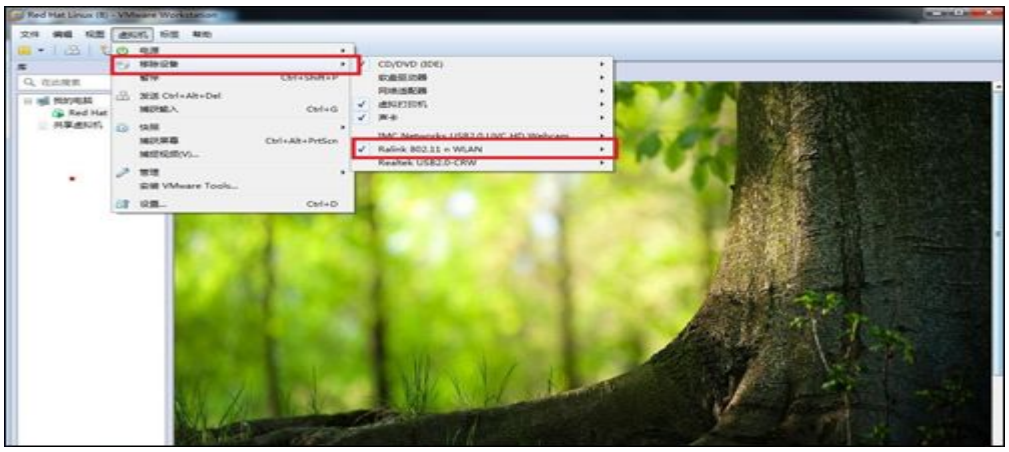
以下这个就是我搜集的各种系统镜像：

首先，把网卡驱动安装好，我这个是已经安装好的，里面有两块卡，无线网络 1 为笔记本内置网卡，后边的是 3070 芯片的网卡。

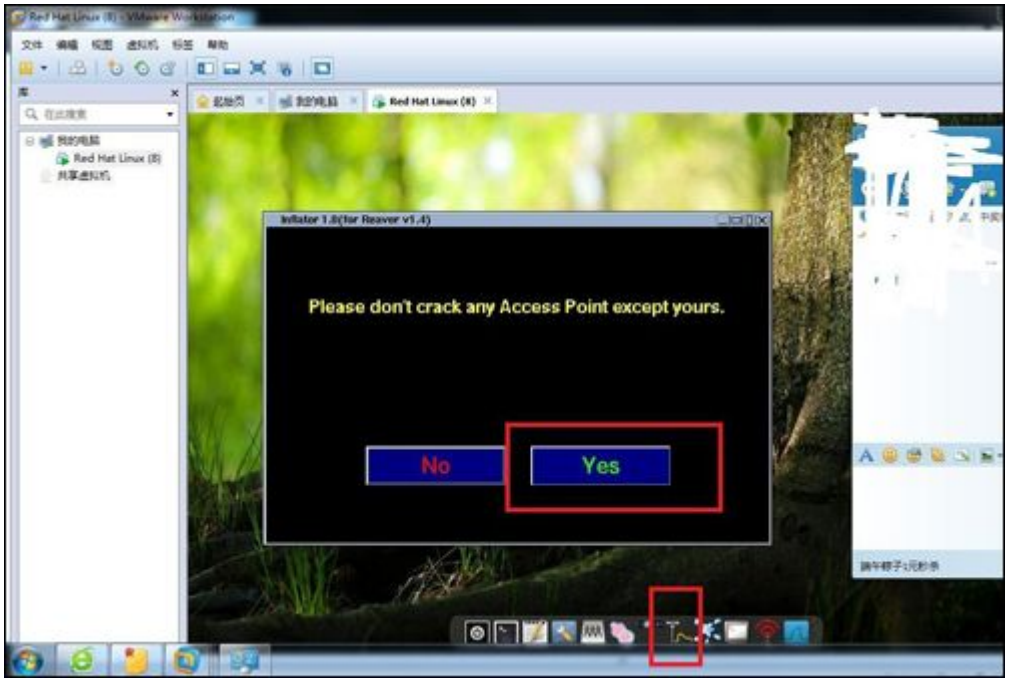
安装虚拟机，配置过程就不细给大家讲了，不会的百度吧。然后加载上系统镜像，在此我用的是 xiaopan 的。



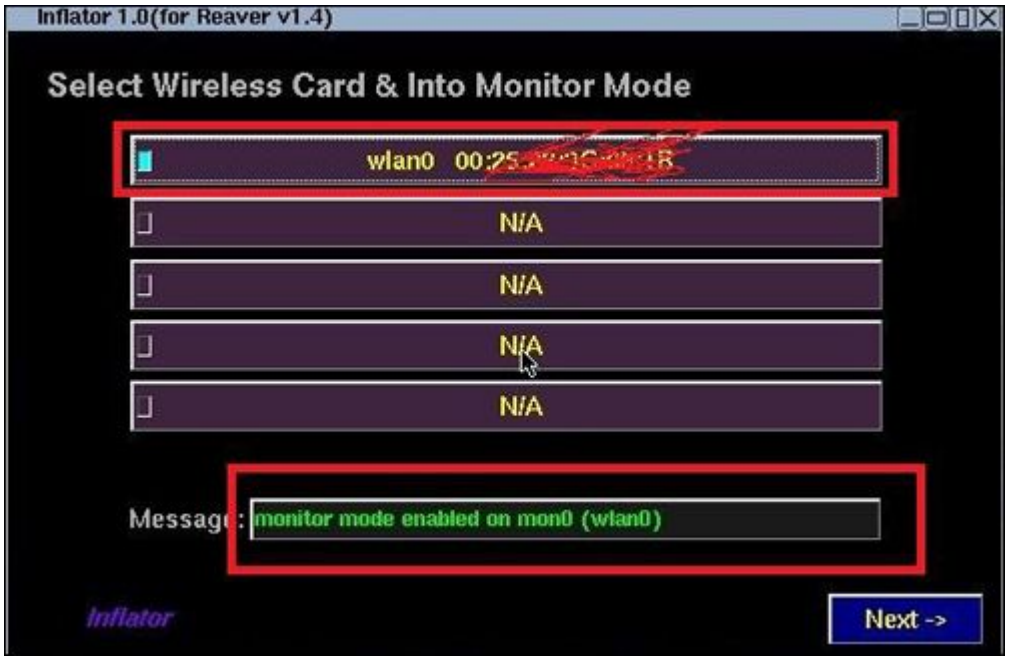
各版本虚拟机不同，但是原理大同小异，把无线网卡添加进去。ps：之前好几次没有添加成功，到最后才发现笔记本左侧 u 口是 3.0 的，提示大家 usb3.0 不支持，需要 2.0 的接口。



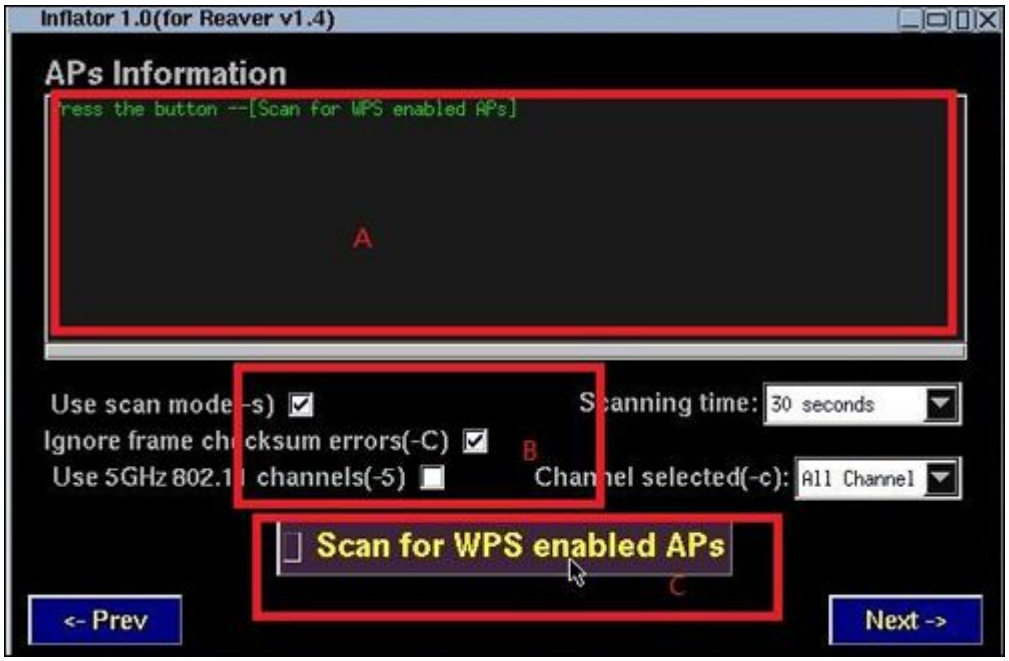
稍等一下就能进入 xiappan 系统了，下方红色方块里有个打气筒的图标，今天我们的攻击就靠它了，咱们要用打气筒把路由 pin 码给逼出来。



勾选这个网卡，进入到监听状态：



B 方框中勾选这两项，点 C 方框搜索附近的新号，会在方框 A 中罗列出来，这时 A 方框中会出现绿字，罗列出路由器 mac 地址、信号、ssid、加密方式等等，而最主要的是看，这台路由器是否开了 WPS。



选好信号最强的那个，椭圆里会显示该路由的 ssid、mac、信道等等信息，勾选方框 s 开 pin 吧，穷举法，开头已经说了，耐心等着吧。若信号好的话，且该路由不防 pin，基本上几个小时就能出结果。pin 中，窗口会显示进度，当 pin 出前 4 位后直接跳到 90.0%开始 pin 后 4 位，这时候其实基本上已经成功了。

告诉大家怎么破解，最后必须还要写下这么一段话，表明初衷：

如何应对 pin 码入侵

首先，关 WPS，其次就是把默认的 pin 给改了。没错，就这么简单，你能做的也只能这样。

剩下的防护措施大家想必都听过了，不过还是罗列一下，给那些开始察觉到路由安全，为此焦虑的朋友们。别问为什么，照着做就是了：

1、加密方式改为 wpa2；

2、尽量不使用 DHCP 服务；

3、隐藏 SSID；（现在很多路由的无线设置里都带这个功能了，如果没有，大家可以把 SSID 命名为空字符，神马是空字符？就是“　”了）

4、把 mac 和 ip 绑定；

5、无线路由能开启无线就能关闭，有的路由还带独立的 Wi-Fi 开关，如果你只用有线，还是把没用的无线关了吧。

虽然加密和破解一直都是共同进步着的，只有加密技术领先才能防止破解，当然，现在的加密技术已经相当强大了，所以蹭网什么的，难度越来越大，其实加密手段无需做到完全不能破解，只要保证能在短时间内不能破解就行了，毕竟真正的黑客没那么多闲工夫放在这玩意上。不过要杜绝蹭网，下调网费才是最终撒手锏吧。