首先大家要明白一种数学运算，它叫做**哈希算法（hash），**这是一种不可逆运算，你不能通过运算结果来求解出原来的未知数是多少，有时我们还需要不同的未知数通过该算法计算后得到的结果不能相同，即你不太可能找到两个不同的值通过哈希得到同一个结果。哈希是一类算法的统称，通常哈希算法都是公开的，比如 MD5，SHA-1 等等。

我们平时说的 WPA 密码其实叫 **PSK（pre-shared key），**长度一般是 8-63 字节，它加上 ssid 通过一定的算法可以得到 PMK（pairwise master key）。**PMK=SHA-1(ssid,psk)** ，PMK 的长度是定长的，都是 64 字节。**由于计算 PMK 的过程开销比较大，是我们破解花费时间长的关键，所以采用以空间换时间的原则把 PMK 事先生成好，这个事先生成好的表就是常说的 HASH 表（生成 PMK 的算法是一种哈希），这个工作就是用 airlib-ng 这个工具来完成的，我们的快速破解就是这么来的。**

认证的时候会生成一个 **PTK（pairwise temporary**），这是一组密钥，具体细节不详细说了，它的生成方法也是采用的哈希，参数是连接的客户端 MAC 地址、AP 的 BSSID、A-NONCE、S-NONCE、PMK，其中 A-NONCE 和 S-NONCE 是两个随机数，确保每次连接都会生成不同的 PTK。PTK 的计算消耗很小。PTK 加上报文数据采用一定的算法（AES 或 TKIP），得到密文，同时会得到一个签名，叫做 **MIC（message integrality check），tkip 之所以被破解和这个 mic 有很大关系。**

四次握手包中含有以上的哪些东西呢？客户端的 MAC 地址，AP 的 BSSID，A-NONCE，S-NONE，MIC，最关键的 PMK 和 PTK 是不包含在握手包里的！

8 A2 m6 T& }) U2 J 认证的原理是在获得以上的所有参数后，客户端算出一个 MIC，把原文连同 MIC 一起发给 AP，AP 采用相同的参数与算法计算出 MIC，并与客户端发过来的比较，如果一致，则认证通过，否则失败。

目前的破解方法是我们获得握手包后，用我们字典中的 PSK+ssid 先生成 PMK（如果有 HASH 表则略过），然后结合握手包中的（客户端 MAC，AP 的 BSSID，A-NONCE，S-NONCE）计算 PTK，再加上原始的报文数据算出 MIC 并与 AP 发送的 MIC 比较，如果一致，那么该 PSK 就是密钥。

目前最耗时的就是算 PMK，可谓破解的瓶颈。即使搞定了运算量的问题，海量的密钥存储也是个问题（PMK 都是 64 字节长度）！

最近出来的 tkiptun-ng 只是可以解开使用 tkip 加密了的数据包，并不是说能够快速算出 PMK 或 PSK。如果感兴趣，可以到书店看看讲哈希的书，说不定你把这些 HASH 算法都破解出来了。

wpa_supplicant 套件中有个小工具,叫做 wpa_passphrase,它和 airolib-ng 的作用差不多，都是用来生成 PMK，在 backtrack 中应该自带这个工具。比如有个 ssid 为 TP-LINK，PSK 是 12345678，那么生成 PMK 的方法就是 wpa_passphrase TP-LINK 12345678，结果应该是这样：

network={ ssid="TP-LINK"

#psk="12345678"

psk=1eecc652f354863e9f985a96d48545c4994e0d21b04955432b60c2600c0743da

psk=1eecc652f354863e9f985a96d48545c4994e0d21b04955432b60c2600c0743da 其实就是 PMK 了，一般在电脑上运行查看无线密码的软件就是得到这个，把 1eecc652f354863e9f985a96d48545c4994e0d21b04955432b60c2600c0743da 直接输入到无线客户端中就可以连上该 ssid，相当于输入了 12345678，生成 PMK 的过程是不可逆的，**即无法通过 1eecc652f354863e9f985a96d48545c4994e0d21b04955432b60c2600c0743da 来逆推得到 12345678**。可以看到同样是 psk 是 12345678，如果 ssid 名字改变，那么 pmk 就会发生改变，这就是为什么用 airolib-ng 建表是只能按 ssid 生成。

本教程全部文字全部来自己原创

转载请注明：欧阳冰峰出品

本教程用于探索无线路由安全漏洞，禁止用于非法用途，违者法律必究（与我无关）

下面进入正题

首先下载“cdlinux -0.9.6.1 ISO 无线破解系统”

http://u.115.com/file/f7650106dd cdlinux_-0.9.6.1_ISO 无线破解系统.iso

然后准备好虚拟机，我用的 vm6

如果不喜欢虚拟机运行的话，可以直接刻录光盘来加载启动

但是为了方便跑包（暴力破解密码），还是在 win 下用虚拟机比较方便

硬件方面，我用卡皇，芯片 8187 的

大家可以根据自己实际情况安排

第一部：设置虚拟机（光盘启动的可以直接路过本部）

首先安装完 vm（绿色版直接运行）我就是绿色版

出现如下画面

1、首先建立一个虚拟机

照片名称：然后直接猛击下一步

2、继续下一步

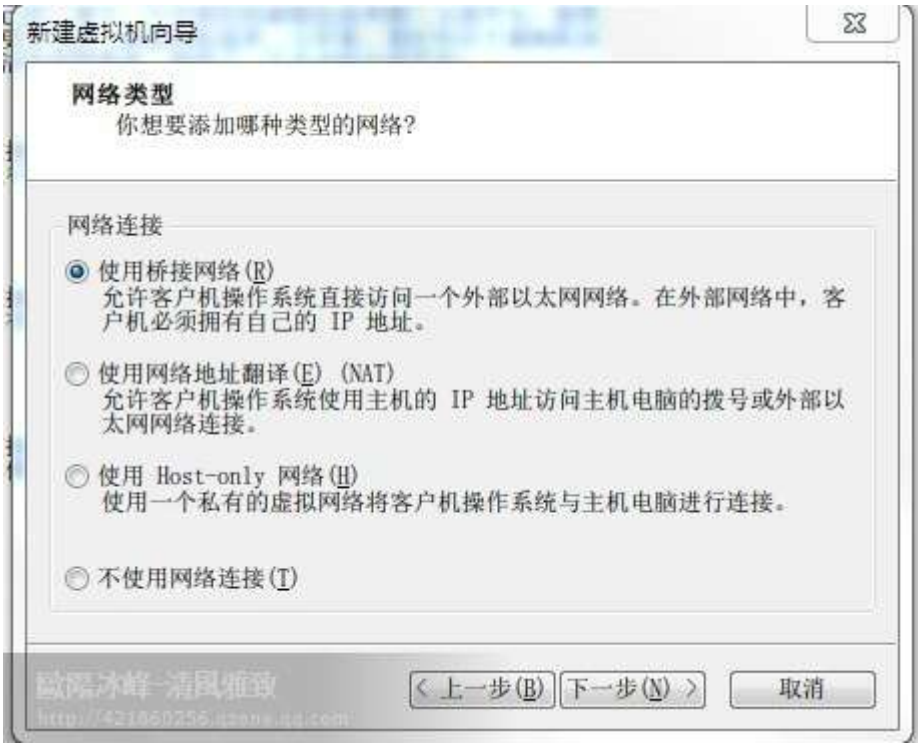
照片名称：然后还是下一步

3、这个吗就是默认了，直接下一步

照片名称：这里客户机操作系统选择 linux，

4、这就是选择操作系统和内核，很重要，按照我的选择就 ok

5、给他一个名字



6、我还是下一步

照片名称：我给他 1g 空间

7、因为 cd 容量很小，130mb 多的文件，你给他 200mb 就够了！我给他 1g

到现在基本上一个虚拟机雏形基本上诞生

接下来最后一步

也是最重要一步

给他一个 iso 包

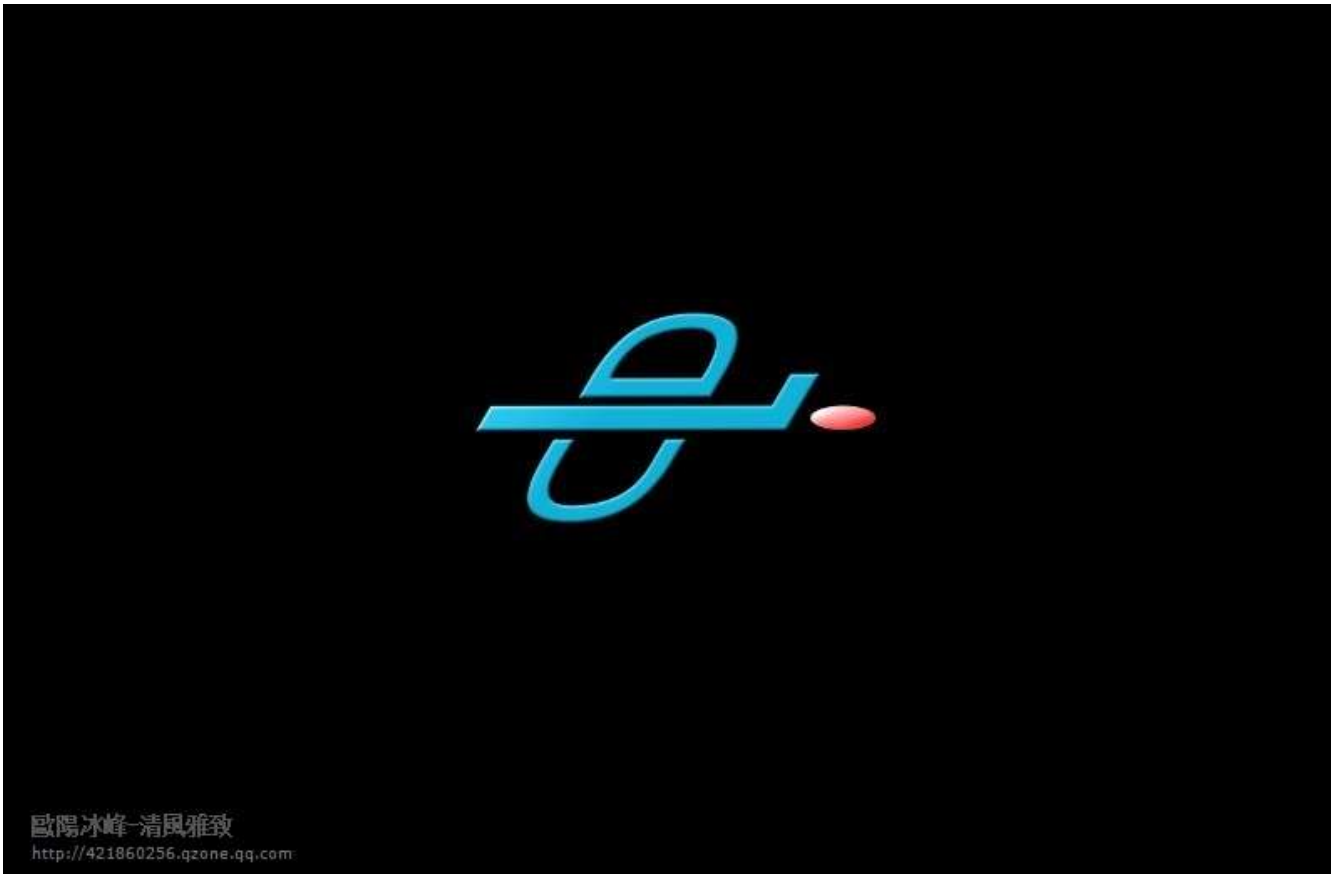
8、给他一个路径，让他知道你的 iso 在哪儿！就这么简单

接下来你就可以启动虚拟机了！

接下来

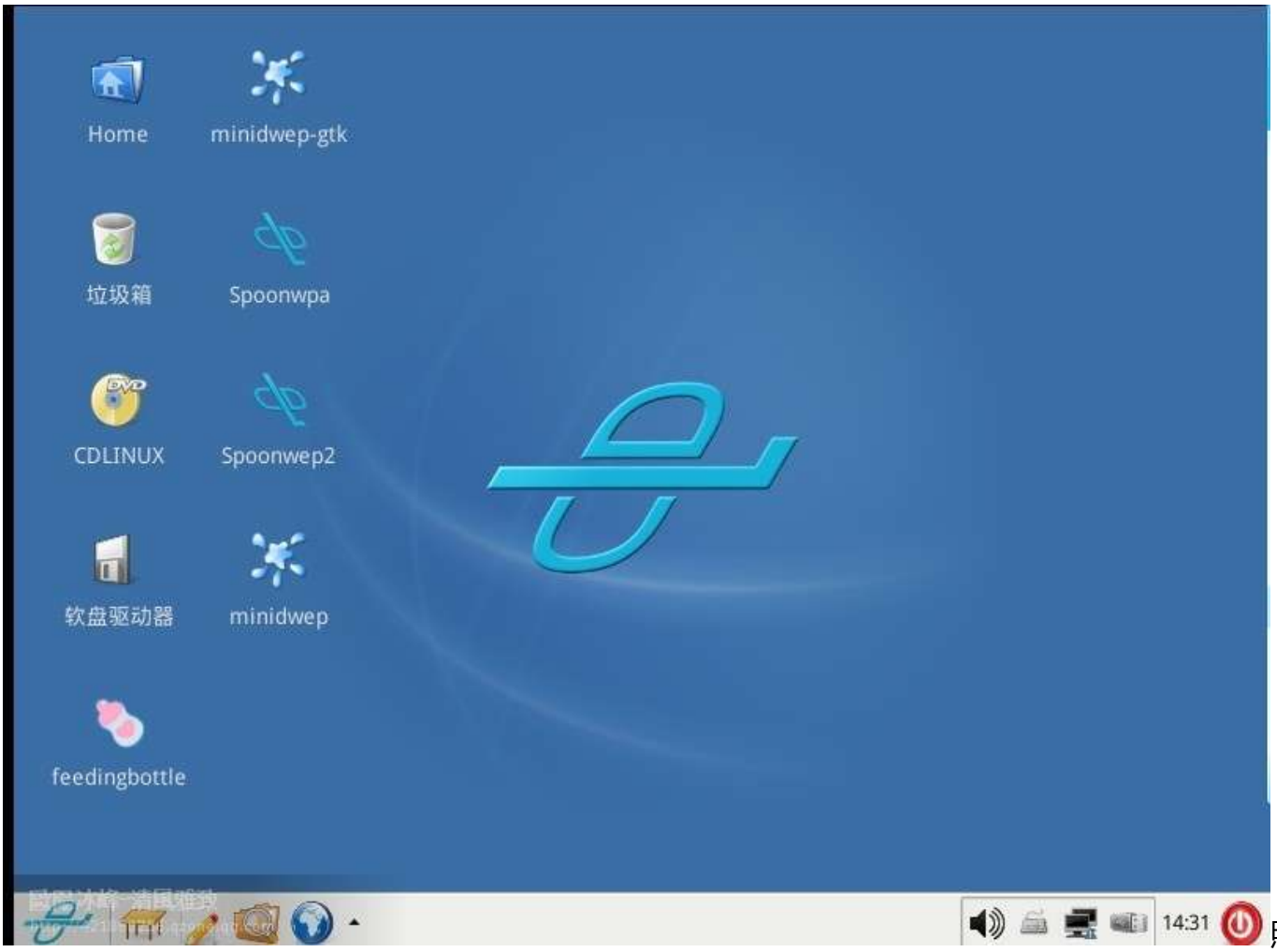
照片名称：这里选择中文，你应该知道吧？

系统启动，选择语言界面，这里你选择中文，如果你是外国人，选择外语，我相信看到这儿都是中国人吧？



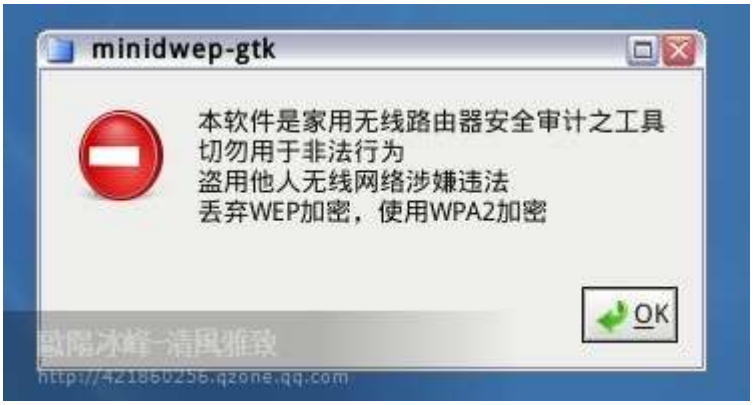
照片名称：系统启动 ing　　启动过后才是令人激动地时刻嘿嘿

第二部：破解 wep/wpa2



照片名称：系统启动成功，桌面

1、系统启动啦，这就是桌面！咋样？熟悉吧？很像 win 的！很容易上手



2、然后打开第二排的第一个软件 minidwep-gtk~~出现此对话框，直接点 ok！就过去了

3、看左上角那个下拉菜单，找到自己的网卡！！！然后右上角！！扫描！！！然后就开始激动人心了！~

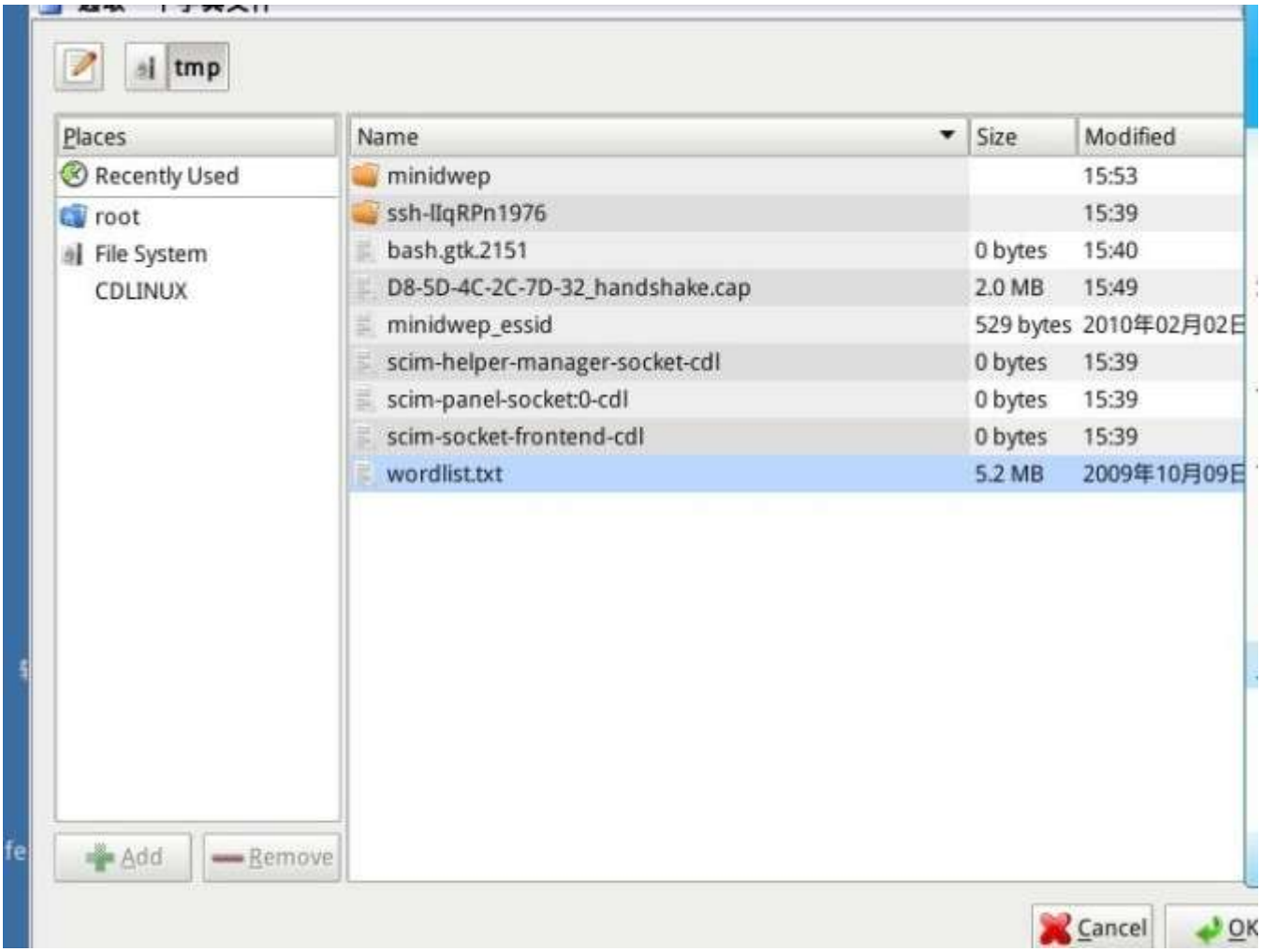
4、够激动吧？看到没有？

sssid---就是扫描到无线接入点的 mac 地址　　pwr：信号强度　　data：这句是所谓的数据包　最后面的 essid 就知道了吧？那就是你扫描到的路由名称！这样就明白了吧？当然了，如果没有数据包的话，你还是省省吧！毕竟是破解！没有数据包代表抓不到握手包，抓不到握手包怎样破解呢？所以还是需要数据量的！然后抓到握手包以后就开始破解啦！

5、怎么样？嘿嘿，看到了吧？软件已经搜索到了 wpa2 加密的方式的路由器！当然了，软件的搜索方式是一起搜索，也就是 wep，wpa2 一起搜索，看看软件左边栏的“加密方式”你选择 wep 就会显示 wep 方式加密的路由，你选择 wpa2 就会显示 wpa2 方式加密的路由，咱们这儿讲的是破解 wpa2 加密方式的路由！所以 wep 一笔带过！如果是破解 wep 的路由，直接右边栏的“启动”按钮，剩下的几乎不用动手自动搜索密码（前提是有数据包哦！）

6、接下来开始抓取握手包，看图片最后面一行字，抓到一个握手包，正在等待认证，等待认证后就会给你提示！告诉你已经抓到一个握手包，然后就可以破解啦!（当然，抓取握手包是需要耐心的，有时候 rp 暴增，没准上来就能抓到，我这儿抓了十几分钟才抓到）

7、基本上已经成功，剩下的就是破解啦！这里开始进入破解第一部，跑包，开始测试密码！



8、接下来，把你的字典贡献给 minidwep-gtk！嘿嘿，这个都会了吧？我给他一个默认的字典，就是最后一个 wordlist.txt。你可以根据情况来选择字典，其实我上藏了 3g 多的字典呢！嘿嘿，不过这个路由是弱口令的！所以这个字典足够了！

9、这下子就解密啦，成功啦！！！嘿嘿，哈哈！！！看见 wpakey：0123456789　这就是密码！这个密码牛屄吧？够弱智吧？！哈哈哈

10、昨天写的仓促，忘了告诉的大家，虚拟机运行 cd 是不支持内置网卡的，所以需要设置一下的！很简单，我就不上图了！打开 vm 以后，看上面菜单栏里面有个“虚拟机”然后下来看到“可移动设备”，然后看到你的 usb 网卡，然后打上对勾就 ok 了！简单吧！嘿嘿

嘿嘿，同志们别拍砖，别骂！破解 wpa 不是开玩笑！关键是你的机器是否够强悍！字典是不是够多！！！

如果你的机器够强悍，跑包跑到几十万的话！字典收藏几百 G，估计你不能破解的密码不多了！有很多“大侠”告诉我说破解不了，说我骗人的！后来问人家，你字典多大？人家说了，我字典超牛逼！！！有 3m 的 txt 文件作字典！！！！同志们啊！！！这样的“大侠啊”您觉得他能破解吗？

看过留名哦！觉得受用就回复一下子！嘿嘿！哈哈！

本次教程所使用软件下载地址

http://u.115.com/file/f7d949c203

VMware6.0.rar(本教程所用软件)

http://u.115.com/file/f758c8914b

VMware7.0 绿色版.rar

http://u.115.com/file/f77cd2c61e

EWSA.rar

http://u.115.com/file/f7650106dd

cdlinux_-0.9.6.1_ISO 无线破解系统.iso

传说中的奶瓶

http://u.115.com/file/f7a4c507ed

Beini-1.2.1 集成 500W 密码增强版.iso

附上我收藏的字典：压缩后 80 多 mb，解压缩后 3g 空间！

http://u.115.com/file/f7d8f179da

wpa2 破解字典（解压后 3g 文件）.rar

http://u.115.com/file/f716661ca0

all_birth(vip).rar

http://u.115.com/file/f73b4d2345

Beini-1.1_中的新字典.rar

http://u.115.com/file/f760ed169e

14365003.rar

http://u.115.com/file/f742663269

142183.rar

http://u.115.com/file/f7bc03925f

133127.rar

http://u.115.com/file/f7533611f

0-9.8 位纯数密码.rar

http://u.115.com/file/f7d077303a

3+sr.rar

http://u.115.com/file/f76a7b09c8

生日 1980-2010 年.rar

http://u.115.com/file/f74d658ab6

弱口令集.rar

http://u.115.com/file/f7cd77abab

超级字典.rar

http://u.115.com/file/f7e9e85619

WPA 英文字典.rar

http://u.115.com/file/f720ee3656

wordlist.rar

http://u.115.com/file/f7a42521bf

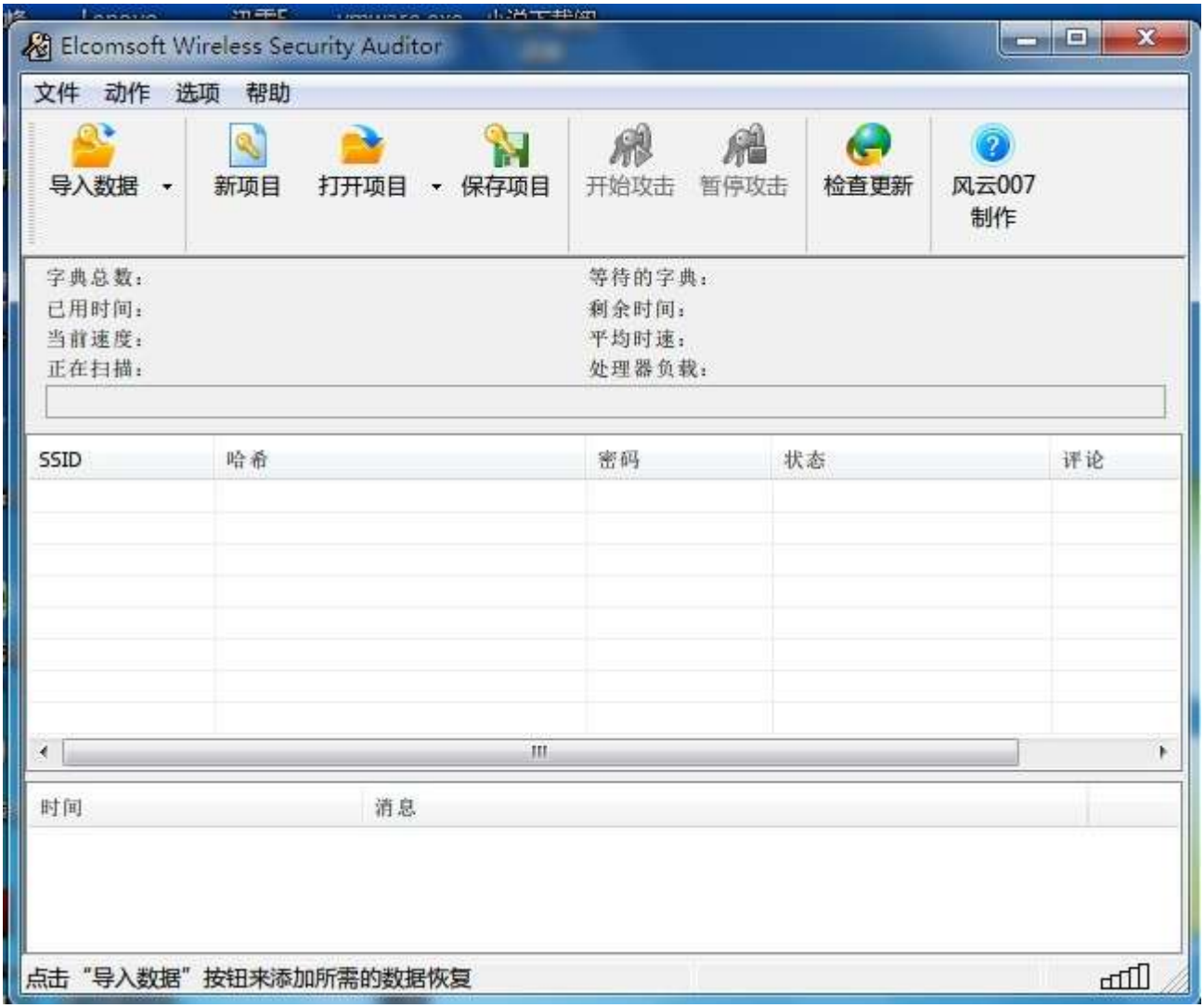
10 位数字.rar

关于破解字典

其实破解是最简单却也是最复杂的，简单的是只需要几个步骤设置好以后就可以暴力破解，复杂的是需要极好的耐心与运气才能破解成功，机器配置越高，字典越多，你跑包的速度就越快，你破解的几率就越高，所以不要问我多久能破解一个 wpa2，我是回答不了的，因为破解有很多因素的吗！下面开始告诉大家如何在 win 下跑包！

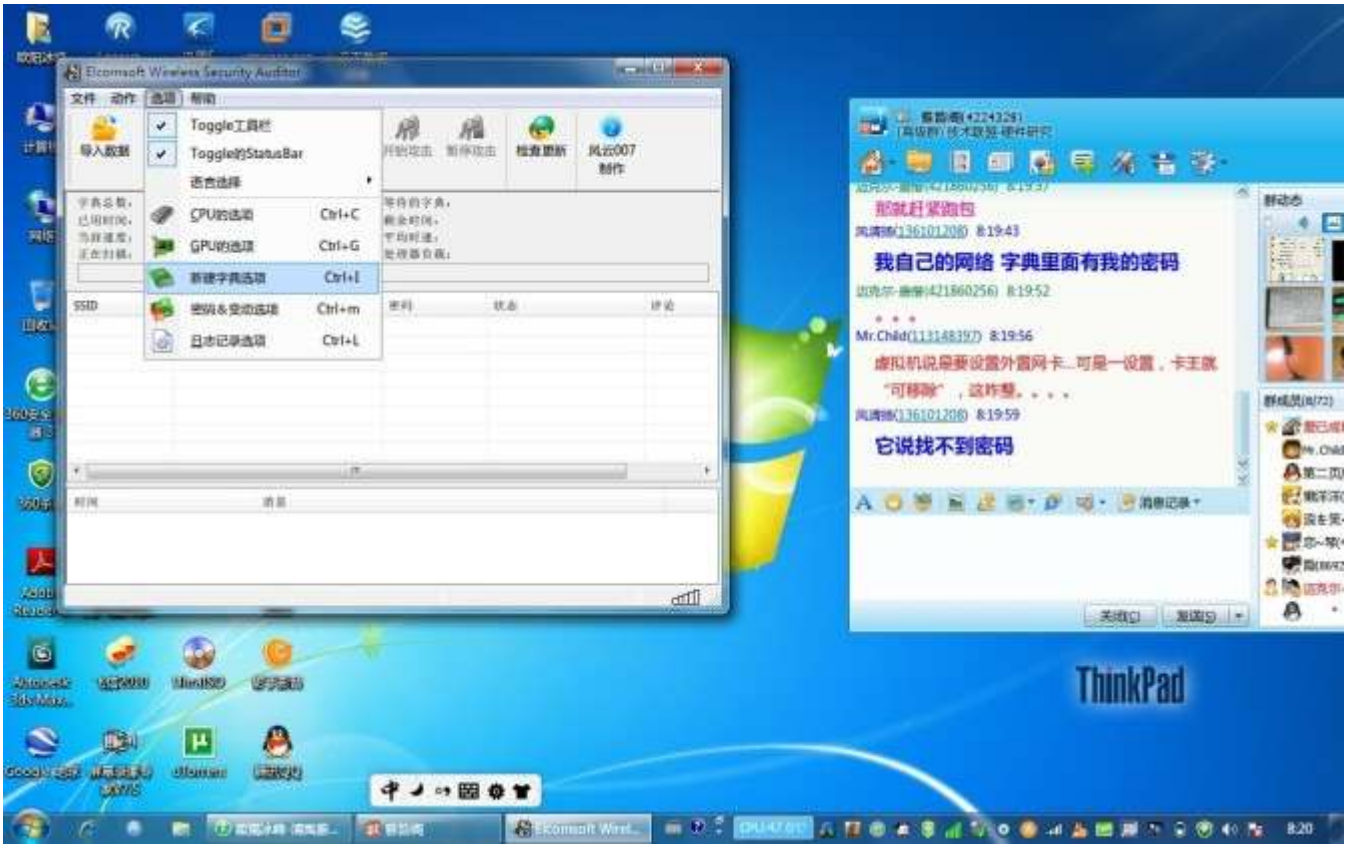
首先需要准备的软件：EWSA（老规矩，懒得下载的后面留言，我发送）字典若干

首先打开 EWSA

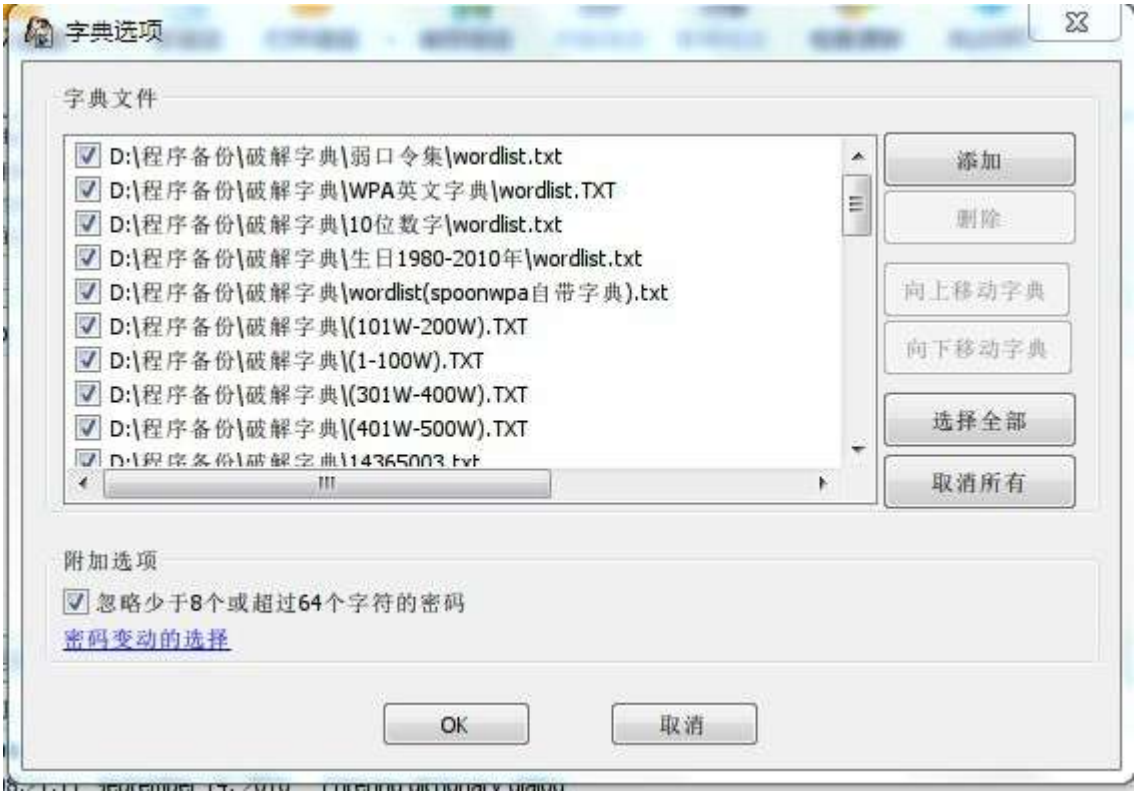

Elcomsoft Wireless Security Auditor
文件 动作 选项 帮助
导入数据
新项目
打开项目
保存项目
开始攻击
暂停攻击
检查更新
风云007
制作
字典总数:
已用时间:
当前速度:
正在扫描:
等待的字典:
剩余时间:
平均时速:
处理器负载:
SSID
哈希
密码
状态
评论
时间
消息
点击“导入数据”按钮来添加所需的数据恢复


那就赶紧跑包
我自己的网络 字典里面有我的密码
虚拟机说是要设置外置网卡...可是一设置，卡主就
“可移除”，这咋整。。。
它说找不到密码
ThinkPad

然后导入你抓到的握手包



然后新建字典选项



然后添加你字典所在路径

然后 ok 就可以开始攻击握手包进行破解了