

windows环境下破解无线网络计算机等级考试 PDF转换可能丢失图片或格式，建议阅读原文

https://www.100test.com/kao_ti2020/644/2021_2022_windows_E7_8E_AF_c98_644693.htm 相信了解无线网络的读者都知道安全性是无线网络的先天不足，正是因为他的传播通过空气，所以信号很容易出现外泄问题，相比有线网络来说信号监听变得非常简单。部分用户通过WEP加密的方式来保护网络通讯数据包避免被监听者破译，不过WEP加密在现今这个安全技术飞速发展的时代已经不再保险，网上也有很多介绍实现无线WEP入侵的方法。今天笔者就再介绍一个更为精简的方法，让我们可以在五分钟之内实现无线WEP网络的入侵，将WEP加密密钥轻松还原出明文。一，五分钟实现无线WEP入侵的特点：众所周知WEP加密入侵需要用户通过监听等方法接收到足够数量的WEP验证数据包，然后通过分析软件使用暴力破解的方法穷举法还原出WEP加密密钥的明文信息。五分钟实现无线WEP入侵也必须通过这种方法来完成，不过不同的是传统的WEP加密破解方法都需要攻击者通过诸如BT3，BT4这样的专业入侵光盘来完成，通过无线扫描和破解光盘启动进入到类Linux操作系统的GUI界面，然后通过内置的破解工具进行扫描和还原密钥工作，一方面操作上受到局限，进入GUI界面无法灵活选择应用程序.另一方面需要下载容量巨大基本上要有几个G的破解光盘镜像，同时还需要刻录成光盘启动。最关键的一点就是这种破解并不支持断点续破，也就是说如果中途关闭电源或者停止破解的话，之前所做的工作将前功尽弃。今天笔者介绍的这个五分钟实现无线WEP入侵的方法则有效的解决了上面传统方法的不足，首

先我们并不需要下载容量巨大的数据光盘，其次所有工作都直接在Windows系统下完成，全部图形化界面，而且我们可以将破解工作划分成收集数据以及破解数据两个阶段，从而大大提高了破解效率，实现了断点续破的功能。通过本文介绍的方法我们可以在很短时间之内实现WEP验证数据包的收集，之后再继续进行WEP暴力破解还原即可。总体来说破解WEP加密的无线网络速度更快。

二，变更无线网卡驱动实现数据监听：和以往针对无线WEP加密破解一样的是，我们首先需要将自己的无线网卡驱动进行更新，因为默认情况下无线网卡虽然能够进行无线通讯，但是无法胜任监听工作。具体步骤如下。

第一步：笔者使用的笔记本是IBM T400，默认情况下他的无线网卡是atheros ar5006系列，我们要将其更改为适合监控的类别。首先在我的电脑任务管理器里找到网络适配器下的无线网卡，在其上点鼠标右键选择“更新驱动程序”。

第二步：接下来会打开硬件安装向导，我们选择“从列表或指定位置安装(高级)”，然后点“下一步”按钮继续。

第三步：接下来是选择驱动程序，我们使用附件中的“驱动程序”目录中的文件进行安装即可，通过“浏览”按钮找到对应的网卡驱动程序，然后继续点“下一步”按钮。

第四步：系统会自动扫描指定目录，然后通过里面的驱动文件更新网卡驱动程序。

第五步：更新完毕后我们的无线网卡就被更改为commview atheros ar5006x wireless network adapter，点“完成”按钮结束。

第六步：再次查询该网卡会看到名称已经被顺利更新到commview atheros ar5006x wireless network adapter了。至此我们就完成了驱动程序的更新，现在我们笔记本的无线网卡已经具备监听无线通讯数据包的功能了。下面我们就可

以通过专业的监控软件完成无线数据包的监听了。三，安装COMMVIEW FOR WIFI并收集相关无线通讯数据包：要想顺利监控无线通讯数据包除了使用专门的破解光盘BT3或BT4外，我们可以通过纯WINDOWS系统下的软件来完成，这也是本文介绍的快速破解WEP加密的主要工具之一。他就是大名鼎鼎的commview for wifi。 commview for wifi小档案 软件版本：6.1 build 607 软件大小：9881KB 软件类别：共享版 软件语言：英文版 适用平台：windows 9X/ME/NT/2000/XP/2003 下载地址：<http://www.onlinedown.net/soft/4632.htm> 第一步：从网上下载commview for wifi 6.1 build 607，值得注意一点的是一定要选for wifi版，否则将无法顺利监控无线通讯数据包。下载后解压缩运行主安装程序，然后一路点next按钮即可，直到完成全部安装。第二步：接下来我们启动commview for wifi软件，在主界面上点“箭头”（开始监控）按钮，然后会打开扫描界面，接下来我们点右边的start scanning按钮将针对当前环境下的无线网络进行扫描，扫描将从频道1开始继续到频道13，所以扫描到的无线网络SSID及设备类别等信息都会直接显示在scanner扫描界面中。点对应的名称后我们还可以看到具体信息，包括信号强度，设备MAC地址，IP地址等信息。小提示：由于实际使用过程中并不是每个频道无线网络都很多的，所以我们可以直接在options标签下设置具体扫描频道，例如只扫描频道3，6，7等。这样可以最大限度的提高扫描速度。设置完毕后确定即可。 100Test 下载频道开通，各类考试题目直接下载。详细请访问 www.100test.com