无线网络攻击安全介绍

作者：午夜的猪[TAT]

通常大家入侵最多的目标就是网站、以及一些小型的服务器之类的，好像却没有多少人对于无线网络的入侵以及安全有所认识吧？这期我们就来介绍介绍关于无线网络的入侵方法以及要注意防范的一些问题。看完这期之后，让大家对于无线网络安全以及攻击有了更加深入的了解。

在介绍如何入侵无线网络之前，首先跟大家回顾一下一些通常我们都会见到、听说过的网络设备，因为这些于无线网络有一定相关的联系，当然无线网络也会使用到，而且使用率很高喔！通常我们所使用的网络设备会有：路由器、调制解调器、交换机等等。而什么是路由器呢？

要解释路由器的概念，首先得知道什么是路由。所谓“路由”，是指把数据从一个地方传送到另一个地方的行为和动作，而路由器，正是执行这种 行为动作的机器，它的英文名称为 Router,是一种连接多个网络或网段的网络设备，它能将不同网络或网段之间的数据信息进行“翻译”，以使它们能够相互 “读懂”对方的数据，从而构成一个更大的网络。

而我们常说的入侵路由器，只不过是入侵家用的 Modem 设备。为什么这么说了？而 MODEM 又是什么了？

调制解调器（Modem） 作为末端系统和通信系统之间信号转换的设备，是广域网中必不可少的设备之一。分为同步和异步两种，分别用来与路由器的同步和异步串口相连接，同步可用于专线、帧中继、X.25 等，异步用于 PSTN 的连接。因为我们所使用的 ADSL MODEM 大部分都是存在着路由功能的，厂商为了用户在使用 MODEM 的时候可以减少大量的操作以及配置，所以都会自配一些适合家庭用户的路由功能，例如:NAT、PPPOE 等等的功能。家庭用户可以不需要懂得路由器的配置方法就可以很轻松的配置好自己的路由器了，而大型的路由器却不是如此，对于普通人来说配置一台路由器并非是一件容易的事情。

作为一个入侵者，如果他所针对的并非是目标的服务器，而是针对其线路上的联通，导致其服务瘫痪或者导致其他的用户不能够正常访问其服务的话，大多数会采用 D.D.O.S 或者更有甚者会直接入侵目标服务器所经过的路由器，控制路由器致使访问者不能够访问其服务，或者利用路由器的功能去攻击目标服务器。无线网络的攻击就是利用嗅探、破解无线网络所使用的加密钥匙、以及局域网相同的攻击形式。接下来我就向大家介绍无线网络的入侵以及安全配置。

一、 入侵无线网络

1、什么是无线网络？

无线网络(WI-FI)是最近热门的话题，一种局域网的网络架构。适用于办公室以及家庭用户。哪什么是 WI-FI 了？

Wi-Fi WirelessFidelity，无线保真 技术与蓝牙技术一样，同属于在办公 室和家庭中使用的短距离无线技术。该技术使用的使 2.4GHz 附近的频段，该频段目前尚属没用许可的无线频段。其目前可使用的标准有两个，分别是 IEEE802.11a 和 IEEE802.11b。该技术由于有着自身的优点，因此受到厂商的青睐。

越来越多的热点都提供免费或者收费的无线网络服务,.而且现在大多数的热点都存在着一个普遍的问题,因为人流量以及人手的问题,导致很多热点所提供的服务器都是很随意的,只要你所携带的手提电脑能够接受连接无线网络就可以无需要任何的验证方式进行使用,往往这样子的管理模式造成了很多安全的问题,理论上无线电波范围内的任何一台电脑都可以监听并登录无线网络。 如果这些热点的安全措施不够严密，则完全有可能被窃听、浏览甚至操

作电子邮件.而且更深一步的来说,如果入侵者控制了 AP 的话,修改 AP 内的 DNS 设置从而使到利用热点所提供的网络进行网络钓鱼式攻击的话,其影响就会更加的广泛.用户群的安全意识薄弱再加上国内对于无线网络安全并不是重视的情况下,参考国外的安全检测来看,估计国内的无线网络可能利用加密的仅仅少于 7%.
而企业方面更加不用说,因为办公机器数量有一定规模,而且人员流动会比较频繁.很难控制介入网络的用户数量以及进行适当的分配.当企业内部人员监守自盗自行介入网络,然后进行嗅探等等的攻击的来盗取企业内部资料,这样子造成企业的损失将难以估计.

2、无线网络所使用的加密方式以及介绍

对于无线 AP 的入侵其实很简单，根据上述所说的，我们可以利用无线网络的配置，从而很容易的介入一个无线网络，然后寻找其网络的无线 AP 根据默认密码或者利用 WEB 页面安全口令工具去破解 AP 的登陆密码以及帐号。

无线 AP（AP，Access Point，无线访问节点、会话点或存取桥接器）是一个包含很广的名称，它不仅包含单纯性无线接入点（无线 AP），也同样是无线路由器（含无线网关、无线网桥）等类设备的统称。

如果无线 AP 有 WEP 加密的话，入侵者会怎么办了？WEP 是一种使用共享密钥和 RC4 加密算法。访问点（AP）和连接到该访问点的所有工作站必须使用同样的共享密钥。因为 WEP 的特殊性以及当初开发商的不重视，所以在使用 WEP 的情况下会存在以下几点安全问题。

•RC4 算法本身就有一个小缺陷，可以利用这个缺陷来破解密钥。

•WEP 标准允许 IV 重复使用（平均大约每 5 小时重复一次）。这一特性会使得攻击 WEP 变得更加容易，因为重复使用 IV 就可以使攻击者用同样的密文重复进行分析。

•WEP 标准不提供自动修改密钥的方法。因此，您只能手动对访问点（AP）及其工作站重新设置密钥；因此，在实际情况中，没人会去修改密钥，这样就会将他们的无线局域网（Wireless LAN，WLAN）暴露给收集流量和破解密钥的被动攻击。

•最早的一些开发商的 WEP 实施只提供 40 位加密——短得可怜的密钥长度。更现代的系统提供 128 位的 WEP；128 位的密钥长度减去 24 位的 IV 后，实际上有效的密钥长度为 104 位，虽然这对其他一些缺陷也无能为力，但还可以接受。

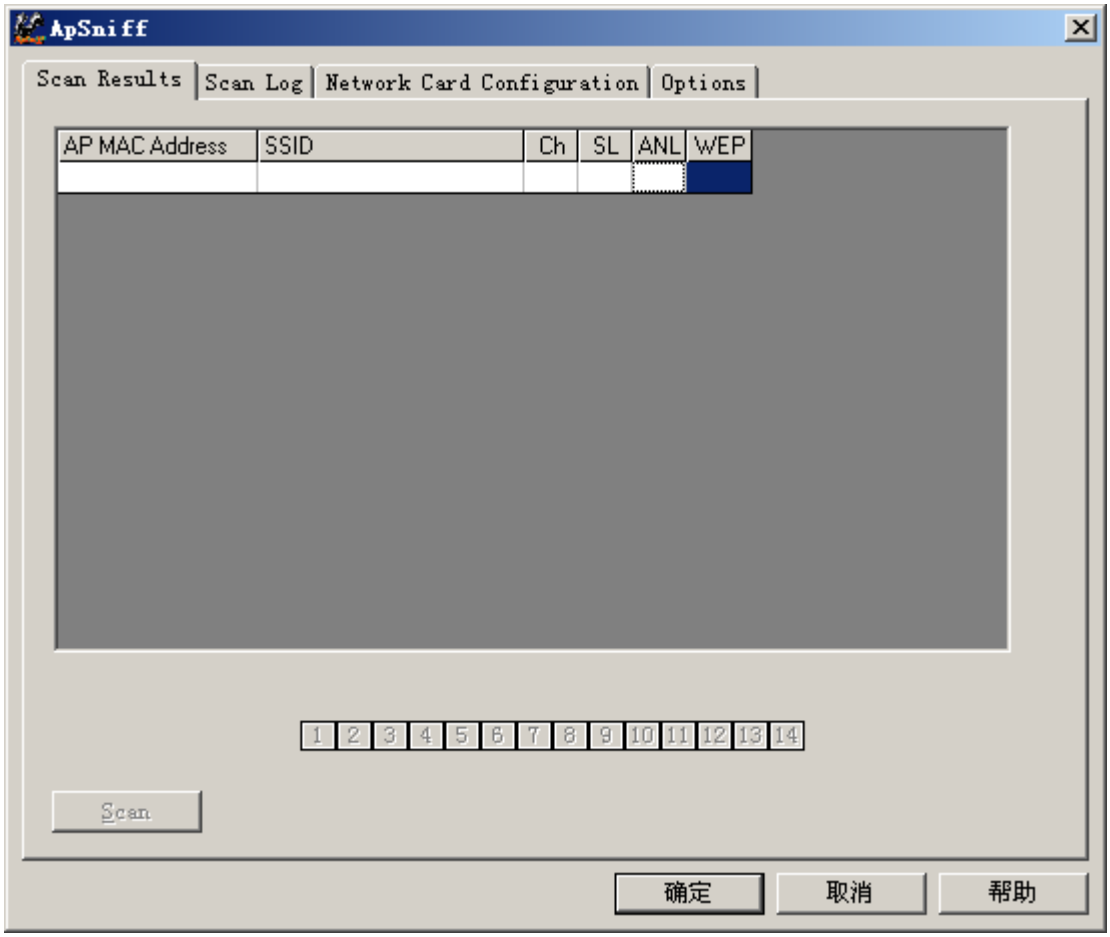
这些缺陷增加了三个以上的攻击隐患，但 WEP 也不是一无是处——有还是比什么都没有强，只是您必须理解 WEP 并不是无懈可击。

3、WI-FI（无线网络）攻击

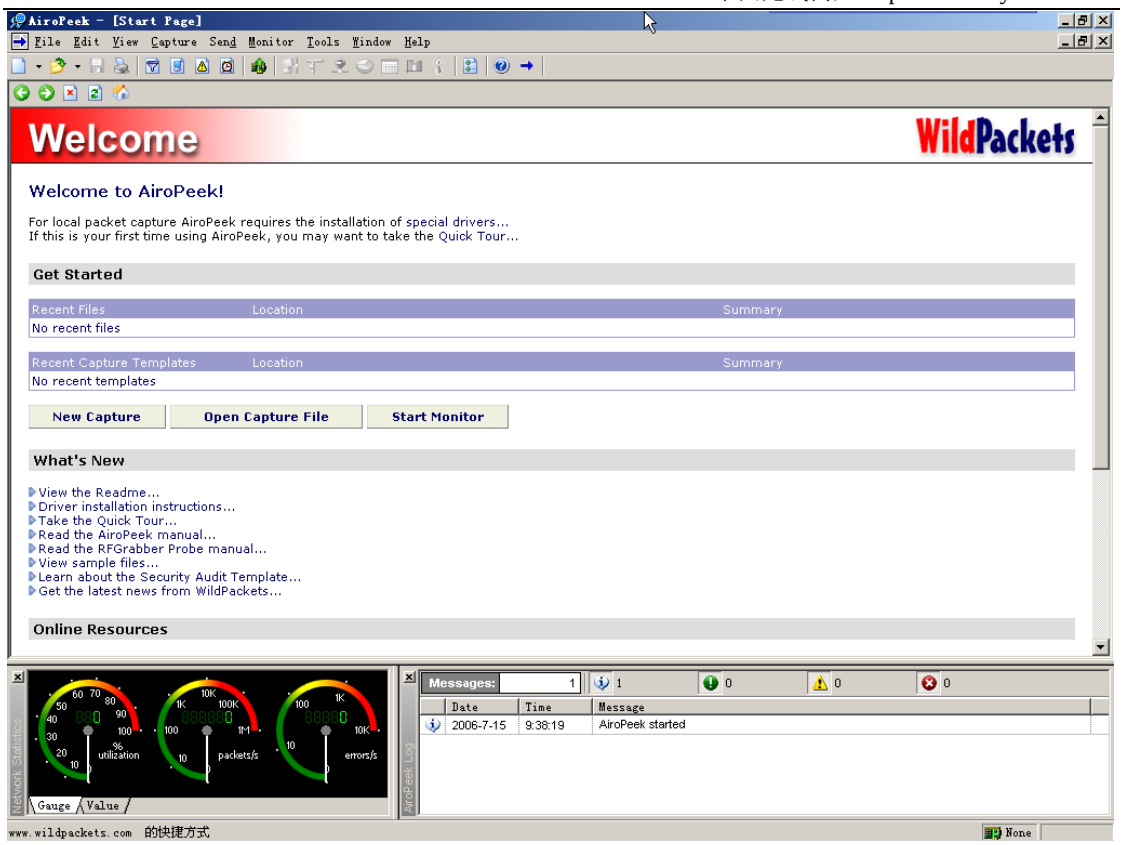
（1）针对无线网络的信息帧测工具介绍以及对于攻击目标的踩点

要针对目标进行入侵的话，我们必须要捕抓到目标的 AP 覆盖区以及信号的频道，而且这些得到的信息，是取决于我们所使用的软件是否能够很好的帮助我们，而我们可以利用 NetStumbler、Apsniff、AiroPeer 等等的软件进行测量，根据软件所返回的信息去判断我们所攻击目标的类别。有一点要注意的是每款软件的使用都不同，而且对于无线网卡的支持也有分别，所以本文会介绍 NetStumbler 的使用，而对于 Apsniff 以及 AiroPeek 我们就粗略的介绍一下。

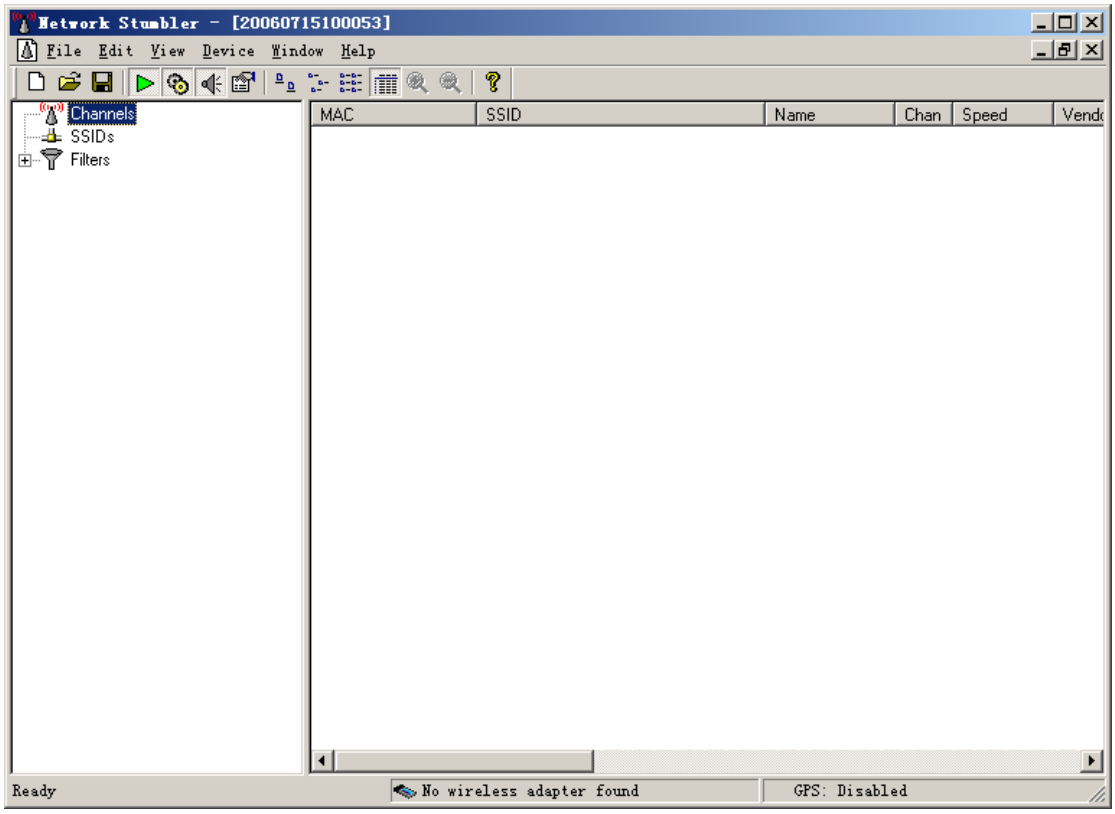
ApSniff 是一款绿色的软件，我们下载之后就可以直接使用了，拥有 NetStumbler 大部分的功能，有一点突出的是 Apsniff 支持 14 个频道（Channel），而 NetStumbler 只是支持 12 个而已，Apsniff 对于国内来说会比较好，但是因为它只能够显示无线 AP 的 MAC 地址、SSID、Channel 以及是否加密而已，所以对于我们来说这个可能并不能够完全合适，当然如果你只是希望知道 AP 的部分资料，这个已经可以绰绰有余了。



AiroPeek 是国外 Wildpacket 公司所开发的无线网络分析器，其公司有着 25 年的历史，而 AiroPeek 是现有最全面的 WLAN 分析工具，而且它的功能是没有任何一种工具可以相比的，对于多网卡的实时分析，应用程序响应时间分析，802.11 协议解码，接入点（AP)的信号强弱显示，警报，触发器监控和报告等等，这是令 NetStumbler 都没有办法实现的功能，说到这里大家都应该会猜想，这个软件不会是免费的吧？哈哈哈哈，大家的猜想是错误的！这个软件光是销售价就不是我们可以支付的，而且软件本身有很多的限制，特别就是对于使用者本身的网卡是有一定的限制性，就是说不是完全所有的网卡都可以使用！告诉大家一个“好”消息，这个软件是不支持 Intel 芯片组的！哈哈哈



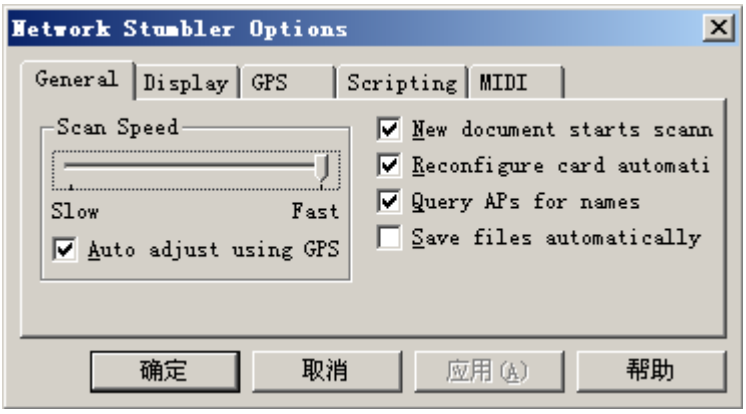
NetStumbler 最有名的免费寻找无线接入点工具，它支持 PCMCIA 无线网卡，同时还支持带有 GPS 全球卫星定位系统的无线网卡功能，但只限制在 windows 下运行，是属于 Free Sofeware 系列。与 AiroPeek 不一样的地方是，该软件是只针对 Scan 部分的，并没有好像 AiroPeek 是属于分析以及对于信号等等的有一系列的报告，但是软件是免费，所以受到很多人的欢迎，对于我们来说这也算是一个好处之一。Apsniff 和 Netstumbler 是属于不需要设置就可以马上进行 Scan 的软件，当你启动软件之后，软件会自动根据无线网卡的种类去搜索无线网络信号，如果你没有无线网卡的话，软件是不会进行任何的操作。而且软件支持任何系列的无线网卡芯片，与 AiroPeek 不一样。



介绍完三款比较常用的而且功能强大的工具之后，大家是否觉得无线网络的使用以及维护等等的一切都比较麻烦呢？其实无线网络的乐趣是很多的。如果大家想对无线网络有深入的了解，可以看看有关的书籍。对了！如果大家是使用 Linux 系统的话，可以试试用 kismet 喔！这个可是开源的喔，而且功能也不差啊！

对于攻击目标的踩点

介绍完工具，我们就要实际的使用了，接下来我们是会用 NetStumbler 进行介绍的，启动 NetStumbler 之后，程序会自动根据本地主机所使用的无线网卡进行搜索，如果本地主机没有无线网卡的话，程序会在下方提示“No Wireless Adapter Found”，如果我们的无线网卡有 GPS 功能的话，记得在“View”－“Options”－“General”设置“Auto adjust using GPS”

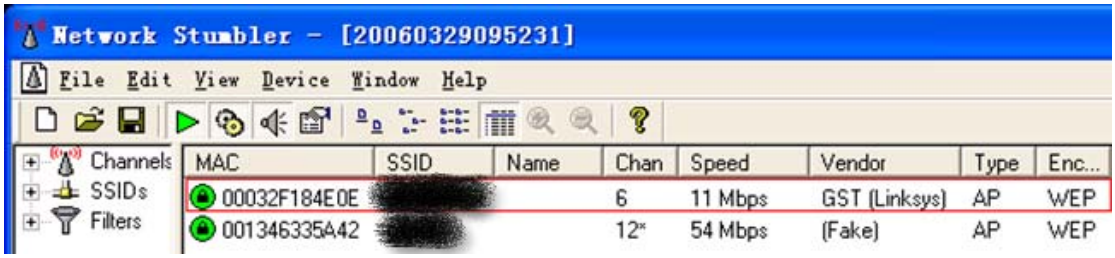


而“Scan Speed”是设置程序对于 AP 的扫描速度，扫描速度总共分为五种。每 1.50 秒对于 AP 进行扫描，这是属于 Slow 的，而最快的就是每 0.50 秒扫描一次。剩下的三种就是相对的递增或者递减，以下就是 Scan Speed 的速度表格，是包括了开放了 GPS 模式的。

Scan interval (seconds)	Slow	- - -	- - -	- - -	Fast

Without GPS speed	1.50	1.25	1.00	0.75	0.50
GPS, Stationary	3.00	2.50	2.00	1.50	1.00
GPS, 25 mph / 40 km/h	2.74	2.07	1.48	0.98	0.57
GPS, 50 mph / 80 km/h	2.31	1.63	0.96	0.46	0.25
GPS, 75 mph / 120 km/h	1.55	1.20	0.50	0.38	0.25
GPS, 100 mph / 160 km/h	1.16	0.76	0.50	0.38	0.25

设置完毕之后，就可以开始针对目标进行扫描了，一切都归于自动化，我们是不需要动任何的东西，程序就会确认客户端所在的 AP 覆盖区内，并且通过 AP 信号的参数进行数据搜集。

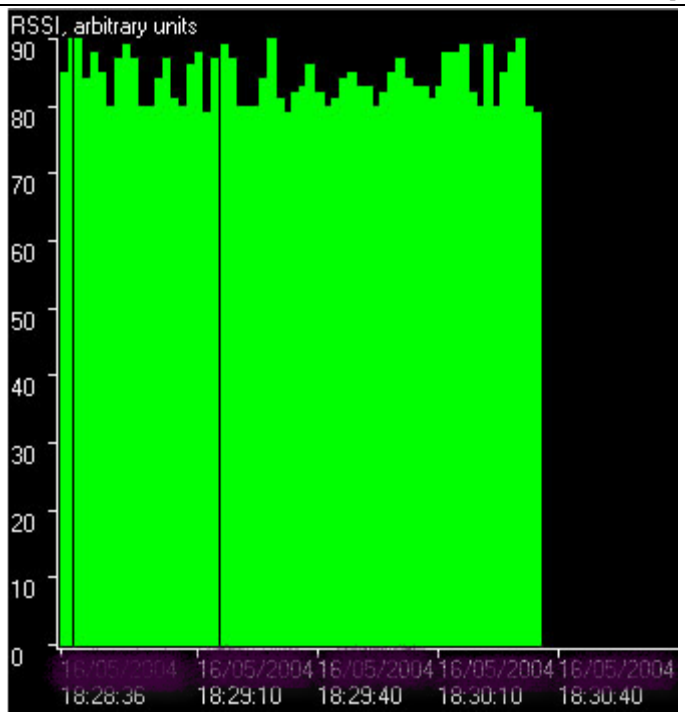


通过上图的标明部分内容确定目标的 SSID 为 802.11b 类型设备，Encryption 属性为‘已加密’，根据刚刚前面的介绍，我们可以确定目标的加密算法是 WEP。

注意：NetStumbler 对使用加密算法的 STA（802.11 无线站点）都会在 Encryption 上标识为 WEP 加密模式。

还有一点大家要注意的喔，NetStumbler 在 War driving 的时候是一个非常好的帮手来的喔。

[War driving：也称为接入点映射，这是一种在驾车或者步行方式围绕企业或住所邻里时扫描无线网络的活动。要想进行驾驶攻击你就要具备一辆车、一台电脑（膝上型电脑）、一个工作在混杂模式下的无线以太网网卡，还有一个装在车顶部或车内的天线，你也可以利用掌上电脑、一个背包、一个小型的天线，因为用背的方式去进行扫描也是可行的喔。利用全方位天线和全球定位系统，驾驶攻击者就能够系统地将 802.11b 无线接入点映射地址映射，并记录该接入点的地址以及接入点是否采用加密协议等等的信息]因为 NetStumbler 是可以针对无线接入点的信号强弱进行搜索的，我们可以根据接入点的强弱大小去设置我们对于该接入点的 War Driving 路线喔，只要双击所搜索到的接入点名称就会看到相关的信号强弱图表了



按照信号的强弱，我们就可以知道目标的信号覆盖区大概是在那个位置，根据信号的强弱我们可以覆盖信号区从而架设虚假 AP 作为攻击之用。

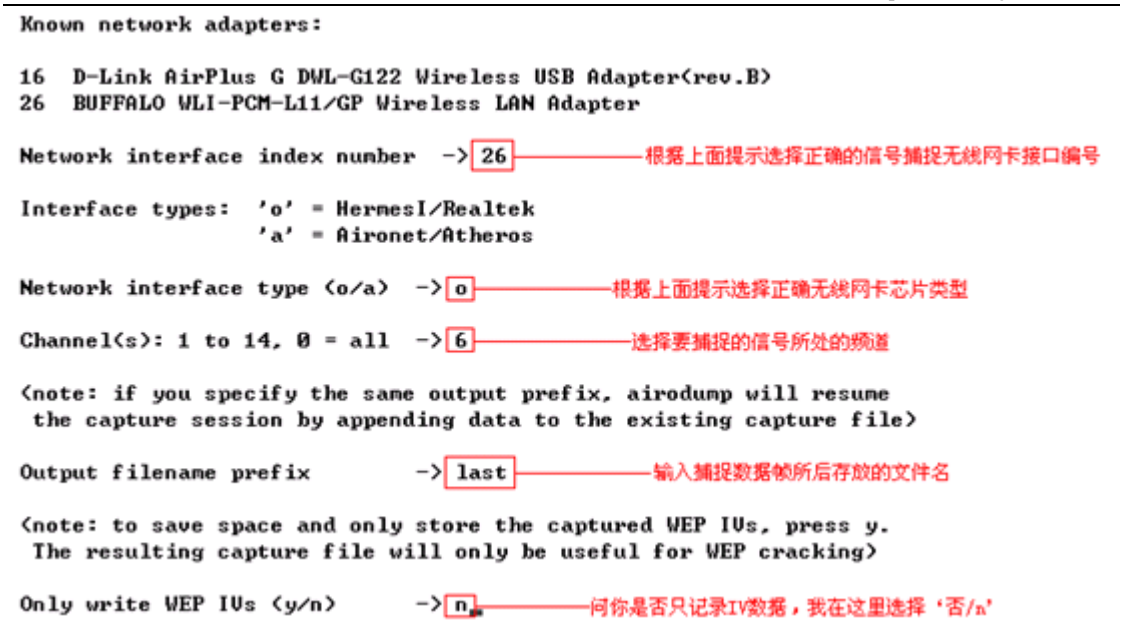
（2）针对目标进行嗅探以及 Winaircrack 的使用介绍

当我们得知目标的有关信息之后，我们就可以利用特定的软件去进行破解工作了，当初 WEP 被传出有缺陷的时候，国外就开始利用 Winaircrack 进行 WEP 以及 WPA 的破解了。而 Winaircrack 其实是一组多功能的破解程序组，不光是可以破解相关的密码算法，而且还可以利用自身的功能去捕抓数据帧。以下就是关于这个工具组的软件功能介绍咯：

aircrack.exe　　Win32 下使用的主程序
airdecap.exe　　WEP/WPA 解码程序
airodump.exe　　数据帧捕捉程序
Updater.exe　　WIN32 下升级程序
WinAircrack.exe　　WIN32 下的图形前端
wzcook.exe　　本地无线网卡缓存中的 WEPKEY 记录程序

而我们就是利用通过捕捉当前 AP 传输的数据帧进行 IV（初始化向量）暴力破解，所以我们不必要完全使用所有的工具组，只要利用 airodump（捕捉数据帧）与主程序就可以了。

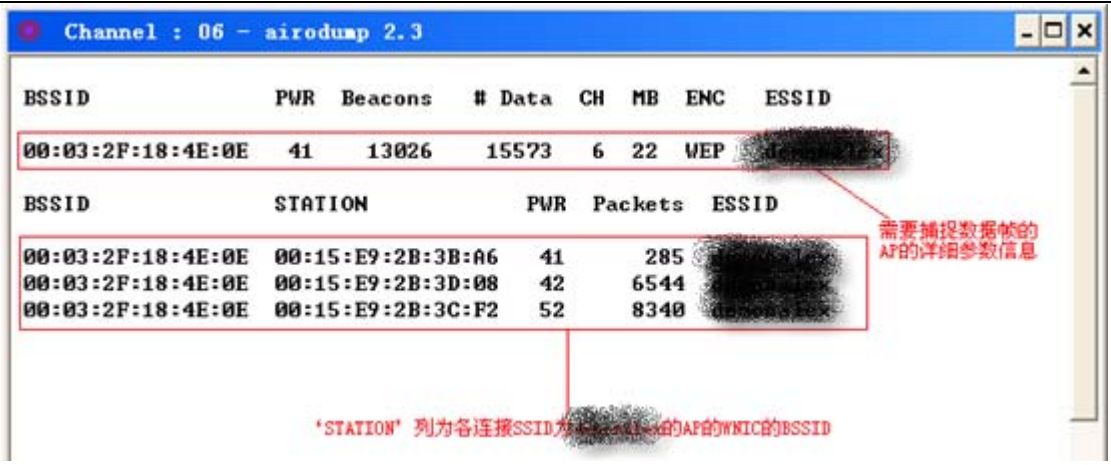
当我们利用 airodump 进行数据帧捕抓的时候，界面会出现很多的选择项目



程序会自动检测本地所存在的所有无线网卡型号，按照所检测到的网卡列表选择适当的网卡进行捕捉数据帧，当我们在选择“Network Interface index number”的时候，必须要清楚自身使用的无线网卡驱动编号，避免导致无法正常使用。然后“Network interface type”（选择当前所选择的无线网卡的类型），目前大多国际通用芯片都是使用‘HermesI/Realtek’子集的，**大家要记住喔，千万不要以为每个网卡都可以使用喔，待会我会解释为什么不行？因为程序有所限制，所以并非完全所有的无线网卡类型都可以驱动本程序。我们通常所使用的 Intel 无线网卡也只有 8 种型号可以破解 WEP 的喔**。然后“Channel<s>”输入要捕捉的信号所处的频道，我们根据之前用工具捕捉的 AP 所处的频道信息填入。而“Output filename prefix”（捕抓数据帧后所保存的文件名）就按照自身的需要而填写，但不写绝对路径的话，文件将会保存在 winaircrack 的安装目录下以.cap 结尾。而最后的项目“Only write WEP Ivs”（是否只写入 IV 初始化向量到 cap 文件当中？），这个也是可以按照个人的需要而进行选择。

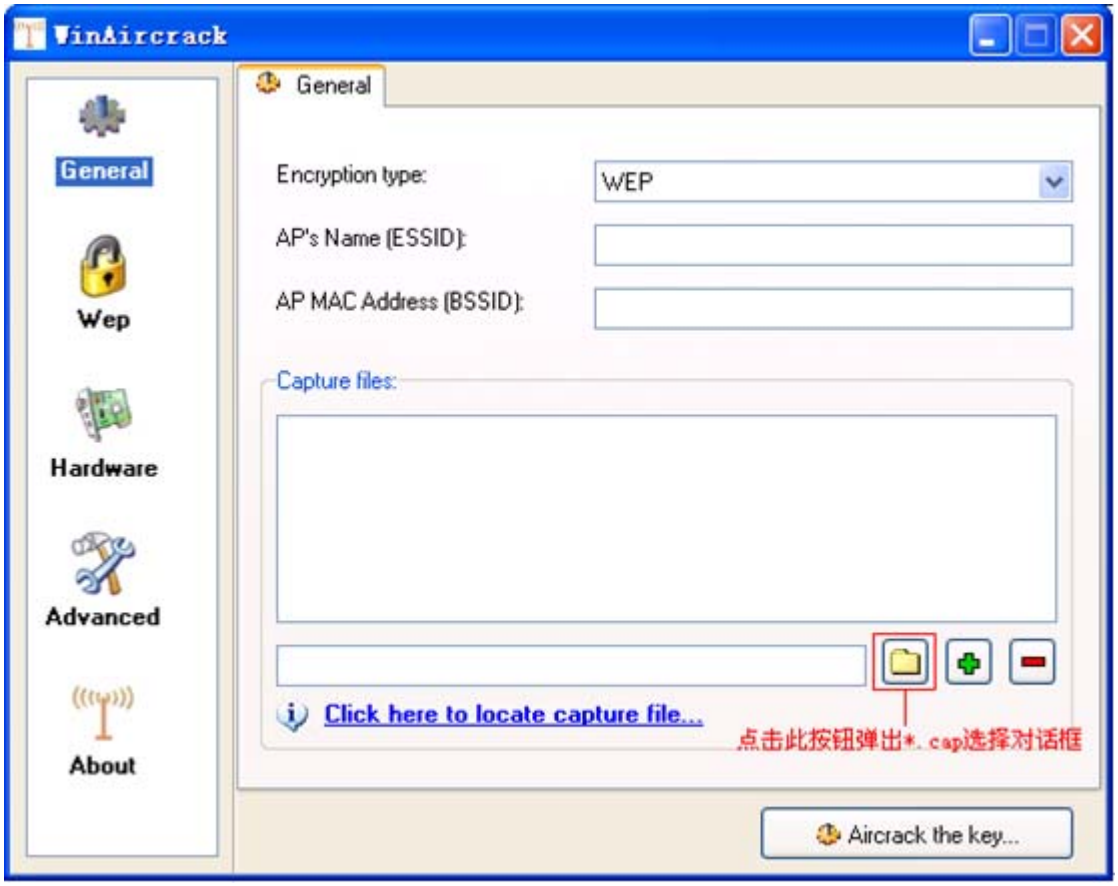
注意：有些资料在破解 WEP 的时候注明是不需要无线网卡的芯片支持的，只要支持 802.11b 就可以。但是当我们实际测试的时候，发现并非如此。整个过程的主要关键就是无线网卡的类型，所以在此就提供部分的无线网卡芯片支持列表给大家

厂家		型号	类型	芯片		备注
Abocom	802.11b	CWB 1000	CF	Prism2/2.5/3		
Abocom		802.11b	WUB 1500	USB	Atmel	
Abocom		802.11b	WMB 2000	mini-PCI		
Abocom		802.11b	WP 2000	PCI	ADMtek	
Abocom		802.11b	WB1500	PCMCIA	Prism2/2.5/3	
Abocom		802.11b	WB 1500H	PCMCIA	Prism2/2.5/3	high power
Abocom		802.11b	WB 1500S	PCMCIA	Prism2/2.5/3	MMCX ext.antenna connecters
Abocom		802.11b	WB 1500SH	PCMCIA	Prism2/2.5/3	High power w/ext.antenna connectors
Abocom		802.11b	WB 2000	Cardbus	ADMtek	
Abocom		802.11b	WB 2500	Cardbus	Realtek	



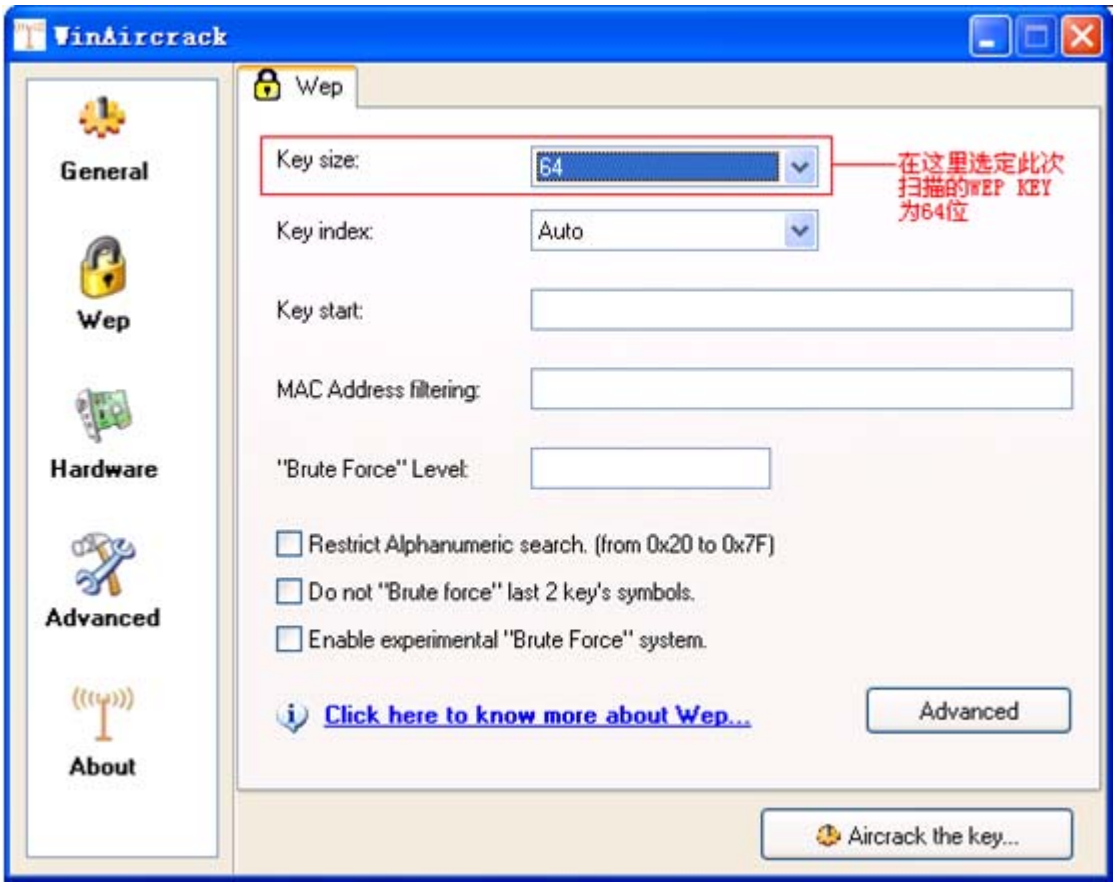
因为捕抓数据帧的过程会很费时，所以在此大家可以喝喝茶，因为我们都在热点测试，那时候我正和 Alex 在喝茶啊！等待程序所以显示的“Packets”总数为 300000 时，就可以开开心心的去破解我们的 WEP Key 咯。根据实验的教训啊！最好找个很多人使用 WI-FI 的热点，然后进行 WEP Key 的破解测试，因为如果你只是针对单一个 AP 或者只是你单一用户进行连接的话，这样子起码要等上几个或者十几个小时，方可使得所捕抓的数据帧满足破解条件。当我们完成捕抓的过程之后，程序会在程序的目录留下后缀为 Cap 以及 Txt 的两个文件。而 Cap 文件为通用嗅探器数据包记录文件格式，是可以使用 ethereal 程序打开查看相关信息的喔。另 Txt 后缀文件就是当前任务的最后统计数据。

（3）使用 Winaircrack 进行数据帧捕抓文件进行 WEP Key 破解

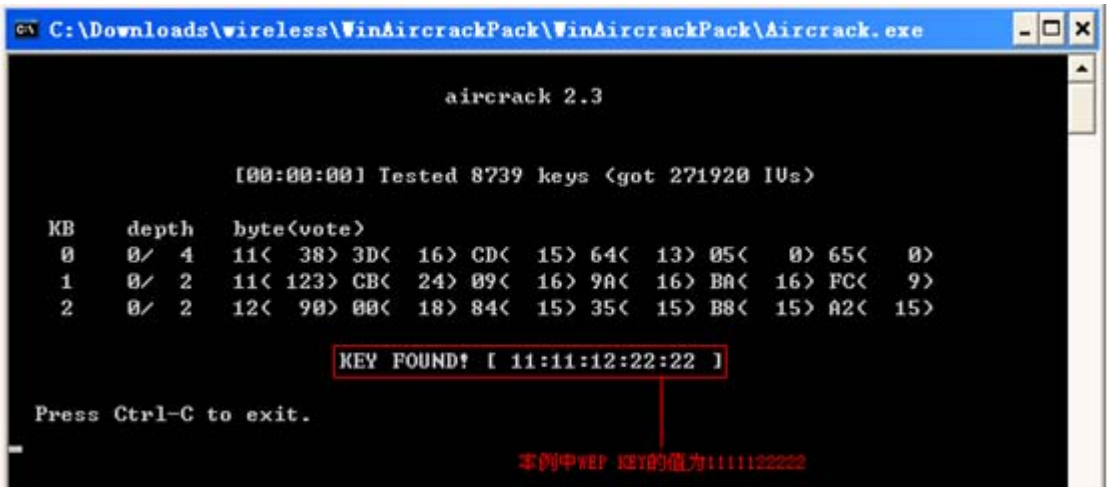


完成了捕抓数据帧的步骤之后，接下来就是破解所捕抓到的数据帧了。利用主程序把刚刚在

dump 捕抓到的数据 Cap 文件导入。单击上图标示部分的按钮，选择刚刚捕抓到的 Cap 文件，然后通过点击右方的‘Wep’按钮切换主界面至 WEP 破解选项界面：



记住我们要选择“Key Size”为 64 位加密。因为我们没有办法估计是否是以 64 位数加密的，所以如果不是 64 位数的话，我们就要重新选择下选择项。最后单击主界面右下方的‘Aircrack the key…’按钮，这个时候程序会弹出一个内嵌在 cmd.exe 下运行的进程对话框，整个破解过程就会开始进行了。因为我们所捕抓的数据帧数量足够，所以不到一分钟的功夫，我们所需要破解的 WEP Key 就已经成功的破解完毕了。



利用刚刚破解成功的 WEP Key，在无线网卡的连接参数设置参数为：SSID：*****、频道：6、WEP Key：1111122222（64 位），这样子我们就可以利用该 AP 进行无线网络的使用了，你可以在主机架设非法 AP 或者是利用嗅探器嗅探同网段主机的信息喔！千万不要做违法的

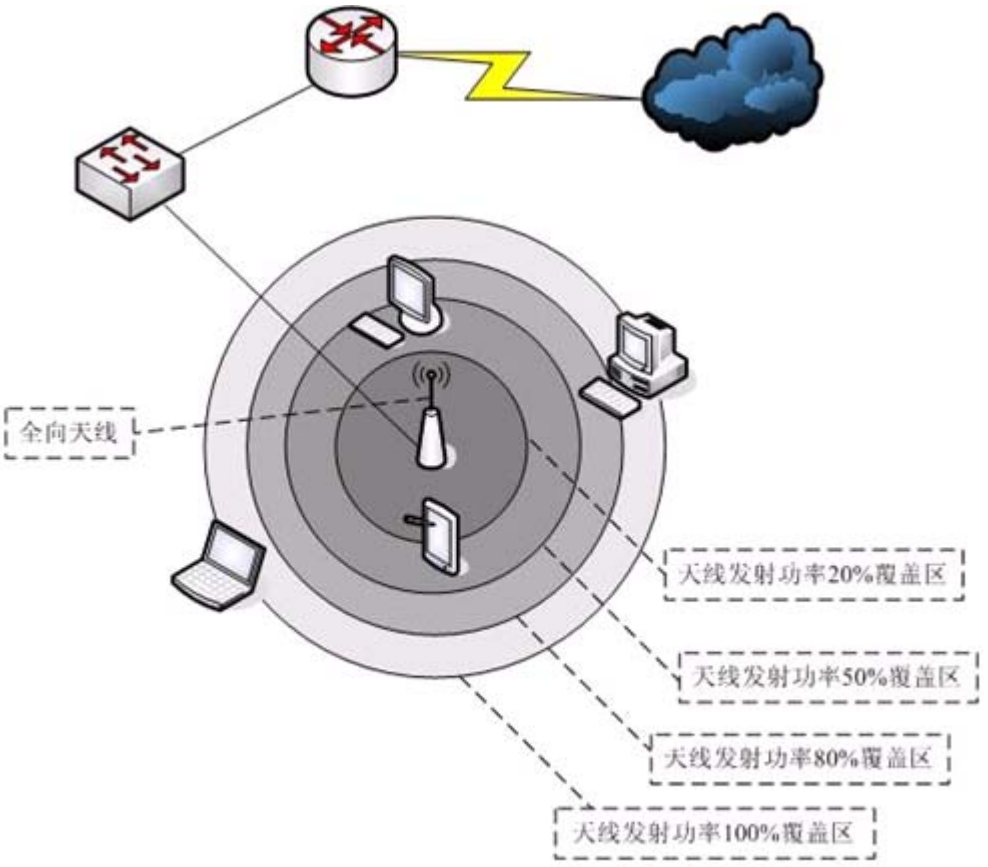
事情啊！

三、WI-FI（无线网络）防御部分

1、基于物理层的保护

（1）缩窄发射天线覆盖范围

攻击者在攻击前必须搜索到发射源的广播信标，也就是说必须进入发射源的覆盖范围，这样子才可以利用工具进行扫描得出有关的敏感信息，而作为防护的一方，我们可以通过设置天线的发射功率尽量控制发射源的覆盖范围，从而达到降低风险的目的。



*附:天线发射功率设置越低,AP信号的覆盖范围就越小

我们把 AP 的天线功率设置为 20%，使它覆盖区仅仅局限于我们所限制的区域，当 WarDriving 攻击者不停地在覆盖范围外进行“踩点”时就无法得到关于该 AP 的信号。但是这种方法只能够防御一些比较不懂得无线网络的攻击者，当我们将自身的天线发射覆盖区域缩小的情况下，攻击者可以利用自身架设的天线，从而将覆盖区加大范围，从而可以更有效的覆盖我们的所在位置，这样子就可以搭建无形的桥梁来进行攻击。

（2）使用定向天线

定向天线利用物理信号的传播特性实现覆盖范围的方向、距离定位，从而达至物理位置的访问控制机制，主要的产品类型有八目定向天线等。如果我们在经济情况允许下，可以考虑使用八目天线，虽然价格是一个必须考虑的因素。或者我们可以自行设计天线，做一个无线 DIY 者。

2、数据链路层保护

（1）高位 WEP Key

WEP 在 802.11b 中负责访问控制与通信数据加密两个过程，但由于 WEP 算法中初始向量出现严重的漏洞，导致攻击者能在捕捉到足够加密数据包的前提下就能破解 WEP Key，所以

我们推崇使用 128 位的 WEP Key（24 位初始向量），增大攻击者的破解难度。还有一点需要注意的是，通常我们在家庭使用 AP 的话，通常都会贪图一时的方便，将加密部分选择 OSSK（Open System Share Key）这样子就会很容易导致整个网络被入侵的危险性加大，所以不管你有多么的不情愿，也希望你使用 WEP Key 加密通信，而且不要使用弱密码，就算你有多少位加密，弱密码始终都是没有防护作用的。

（2）禁用 SSID 广播

广播信标在发射源以默认 100 毫秒发送一次的速度在覆盖区内广播，默认情况下它的头内容包括有该 WLAN 的 SSID（也称 ESSID），攻击者可以通过接收广播信标并解码内容就可以得到该 WLAN 的 SSID 了。

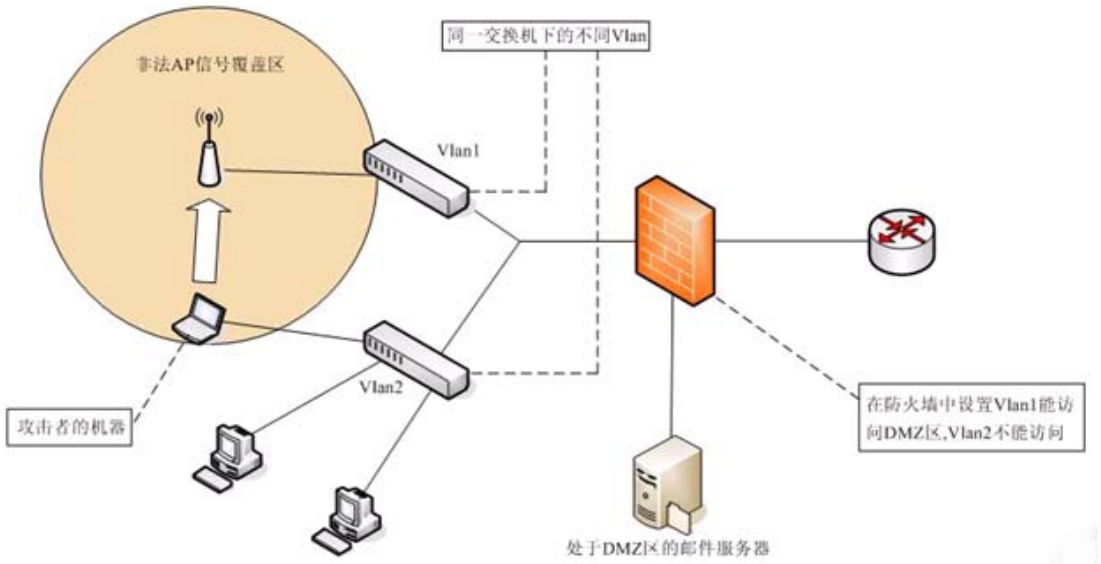
（3）MAC 地址过滤

MAC 地址过滤主要是通过 AP 的桥接功能对接入设备的 MAC 地址进行访问控制，实现合法 BSSID 地址正常访问，非法 BSSID 地址被隔离。常见的实施方式是，首先在 AP 上登记合法 BSSID 的 WNIC，然后设置非法 BSSID 不能访问的规则，达到 MAC 地址过滤的目的。

（4）非法 AP 鉴别

非法 AP（rogur AP）是 WLAN 流行后的又一安全隐患，其原理是在某合法的 AP 的覆盖区内搭建一个不合法的 AP，其危害主要有两种：

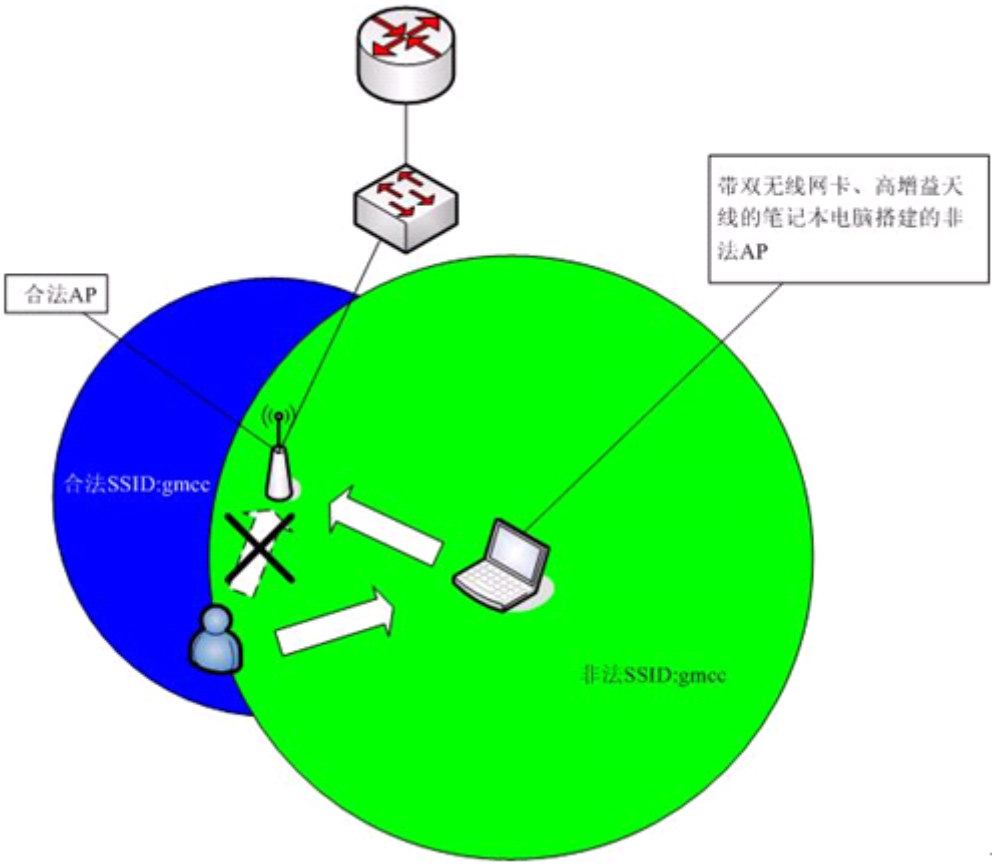
1） 绕过逻辑访问控制的物理制约，如下图：



2）

由于无线接入点的物理体积小，不容易被发现，且游动性强（类似易插拔设备），因此很容易被用作通过物理方式绕过网络的逻辑访问控制。防御此类型攻击的手法是对重要设备实施物理隔离控制。

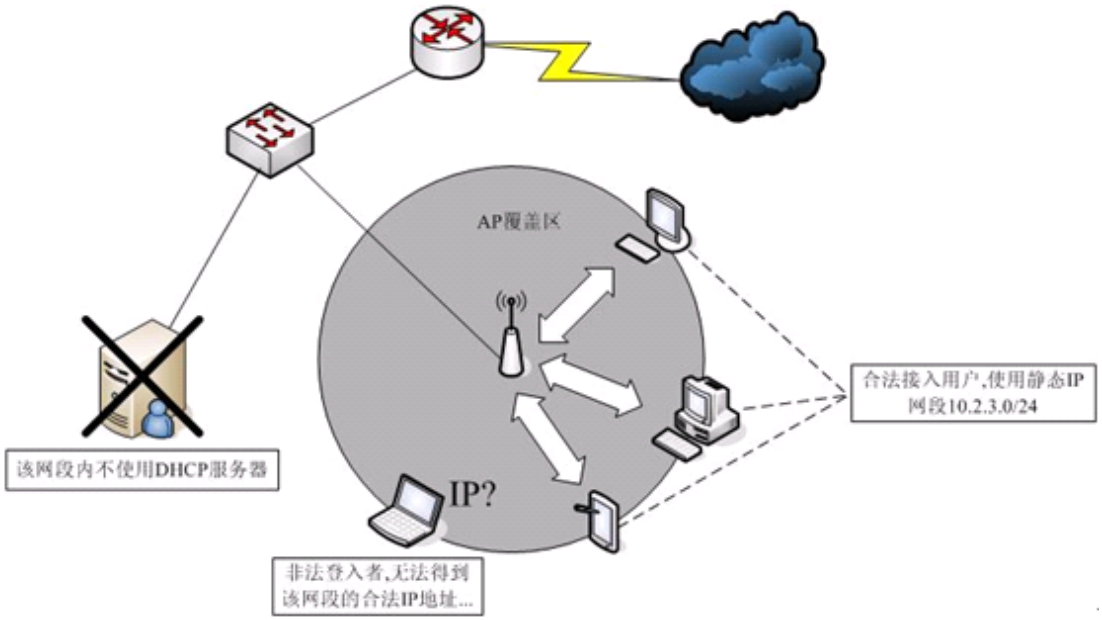
2）通过建立与合法 AP 相同的 SSID（或同时使用相同的频道）来迷惑无线接入者，实现钓



鱼攻击（Phishing）待接入者登入后使用中间人攻击得到使用者的通信数据。杜绝该类型的手法主要是通过合法 AP 与非法 AP 的 BSSID（BSSID 等于无线网络接口的 MAC 地址）来辨别。这个攻击手法就好像刚刚在前面所介绍的缩少信号覆盖范围是一样的，当我们缩少信息范围的时候，攻击者是可以利用自身的条件去令自身的天线达到一个较大的覆盖范围从而跨越我们的范围进行攻击的。

3、网络层保护

（1）禁用 DHCP



若在 WLAN 中启用 DHCP 协议，当攻击者登入 WLAN（接入无线网络）后就能通过 DHCP 得到合法的 IP 地址并直接使用网络，因此禁用 DHCP 是一个增加攻击者渗透难度的绝佳方式。

（2）IP 地址范围缩窄

缩窄 IP 地址的方式主要是通过网络号向主机号借位的方式进行的。打个比方：一个 192.168.1.1/24 的网段就有 254 台机器（主机号 1~254），但若通过网络号向主机号借位的话，将 24 借至 30 的话，192.168.1.0/30（子网掩码 255.255.255.252）就只剩下两台主机（192.168.1.1~2）了。通过对主机数量的定额缩减与分配，可以使攻击者无法及时得到合法的网络层地址，增加攻击者渗透的难度。

根据以上的设置，我们就可以较为安全的使用无线网络了，安全是没有绝对的，对于 WLAN 来说就算我们怎么缩小信号的覆盖范围也有可能会被入侵者扩大自身的信号覆盖区从而进行入侵。

本文针对无线网络设备所带来的攻击进行分析以及针对攻击进行的一系列安全防护介绍，感谢 alex 对于 WI-FI 网络的配置以及 WEP Key 的破解，谢谢。