无线网络设备攻击技术白皮书

图/文：**杨 哲**/Longas 【ZerOne Security Team】

（注：本文已发表在《黑客防线》杂志 2010 年第 1 期上，引用时请注明出处，谢谢）

前言：记得在参加一些安全会议交流的时候，期间经常有朋友问起我家庭及办公用无线路由器会面临什么样的攻击，而在做一些安全项目的时候，渗透组的同事也会有这样的疑问，所以特地整理了一下，希望能对朋友们有所帮助。

鉴于目前无线安全愈来愈任重而道远的趋势，不光是无线网络协议算法存在着隐患，同样地，无线网络设备也同样面临着各式各样的风险。本文给出常见的无线网络设备攻击技术分析及实例，望有助于国内无线安全技术的发展和吸引更多的高手交流。PS：本文所提及的无线网络设备包括我们常说的无线路由器及无线 AP，但对于其它一些无线设备也同样适用。

1．无线路由器识别

对于内部网络而言，查找当前存在的无线路由器标志着无线攻击的开始，作为一些熟练的无线黑客而言，这也是进行伪造 AP 攻击扰乱内网的前期准备工作。所以，如何有效地识别无线路由器目标，也是无线黑客们正在不断研究的目标之一。这里我就介绍几种简单的判断无线路由器的方法。

■方法 1：端口扫描

由于基本上大多数无线接入点/路由器都是支持 WEB 进行配置,所以其 80 端口都是开放的，那么通过使用端口扫描器扫描内网所有主机的 80 端口，查找所有开放 80 端口的主机，排除掉正常提供 WEB 服务（如 IIS、Apache 等）的主机，其余的就是可疑的无线路由器或无线接入点了。当然，这里面也有传统的路由器等有线网络设备，所以，就需要进一步地确认。该方法适用于目前市面上主流的 TP-LINK、Dlink 及 Linksys 等多款无线路由器。

一般来说，无线黑客们会先对全网段扫描开放 80 端口的设备，然后在扫描的结果基础上，对开启 80 端口的设备进行具体版本识别，此版本识别依赖于 Nmap 自带的操作系统/

Blog：http://bigpack.blogbus.com
Email：longaslast@126.com
欢迎拍砖、交流、合作及其它事宜，
新书《无线网络安全攻防进阶》筹备中，即将推出！感谢一直以来的支持！！

网络设备指纹库。

扫描结果如下图 1 所示，黑框内标出了探测到的端口信息，可以看到，该地址为一台无线路由器所有，该无线路由器型号为 DLINK DWL-900AP+，版本号为 2.56，为人为非法搭建 AP。通过在网关上设定规则可以屏蔽该无线路由器上外网，此时即可配合无线搜寻设备来定位该无线路由器。

图 1

对于一些设计不严谨的无线接入点，甚至可以直接在浏览器中输入怀疑的地址，在弹出的登陆界面上，也能够查看到对方的版本提示。如下图 12 在登录框上面显示为 TP-LINK WR541G 无线路由器。

图 2

需要注意的是，通过端口扫描判断无线路由器或者接入点时，一般不仅仅依赖于对 80 端口的判断，一些无线网络设备除了 80 端口之外，也会开启一些很少见的端口，这些也将是我们判断无线设备的依据。这些端口就需要平时的经验及总结，我在下面表 1 中给出部分实例以供大家参考。

表 1

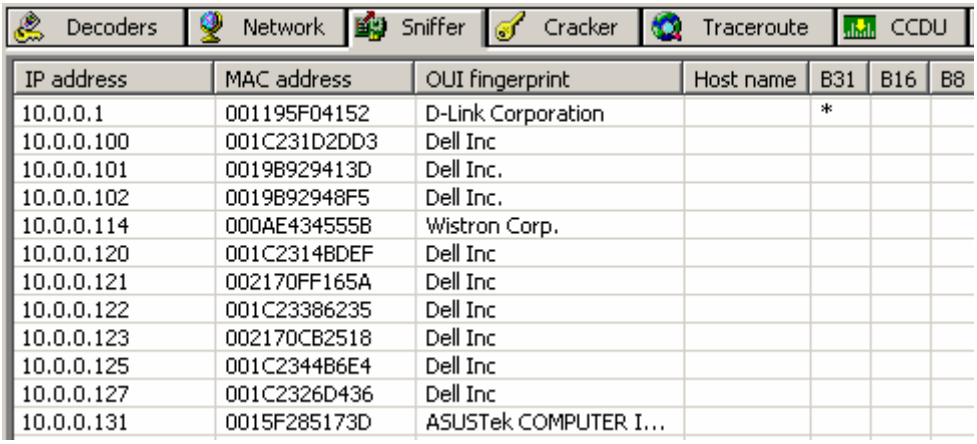
无线路由器品牌	默认开放端口	特殊开放端口（个别）	市面主流产品
Belkin（贝尔金）	80	53	F5D7230
Linksys（思科）	80	2869	WRT54G
Dlink	80	52869	DI-524、DI-624

当然，也并不是所有的无线设备默认下都支持从外部网络访问到其配置页面，这点尤其要注意，所以就需要更多的方法来确认，比如方法 2：特定 ARP 报文探测。

■方法 2：特定 ARP 报文探测

在正常情况下，一台没有安装任何嗅探工具的 Windows 系统主机，只会对特定 ARP 数据报文作出响应。用过 Sniffer 的朋友都知道，一旦在系统下安装了嗅探工具并且激活处于工作状态时，其监听的网卡便进入到混杂模式下，就会拦截所有发至该网卡的数据，而不再丢弃目的地址不是本机的数据报文。同时，此模式下的网卡也将对广播位为 31bit 的 ARP 报文作出响应。

通过发送特定的 ARP 数据报文，能够探测出疑似路由设备。使用 Cain 进行内网 ARP 扫描，选择广播位为 31bit 的 ARP 数据报文扫描，在扫描结果中凡是出现*号的均为疑似路由器，再使用扫描工具进行特定扫描或者直接登录对方 80 端口即可确认结果。如下图 3 所示。



IP address	MAC address	OUI fingerprint	Host name	B31	B16	B8
10.0.0.1	001195F04152	D-Link Corporation		*		
10.0.0.100	001C231D2DD3	Dell Inc				
10.0.0.101	0019B929413D	Dell Inc.				
10.0.0.102	0019B92948F5	Dell Inc.				
10.0.0.114	000AE434555B	Wistron Corp.				
10.0.0.120	001C2314BDEF	Dell Inc				
10.0.0.121	002170FF165A	Dell Inc				
10.0.0.122	001C23386235	Dell Inc				
10.0.0.123	002170CB2518	Dell Inc				
10.0.0.125	001C2344B6E4	Dell Inc				
10.0.0.127	001C2326D436	Dell Inc				
10.0.0.131	0015F285173D	ASUSTek COMPUTER I...				

图 3

进行特定扫描或者直接登录对方 80 端口以确认结果的方法很简单，比如，在浏览器里输入 http://10.0.0.1 后，就可以看到如下图 4 所示无线路由器登录验证框，即目标为 DI-604+无线路由器。

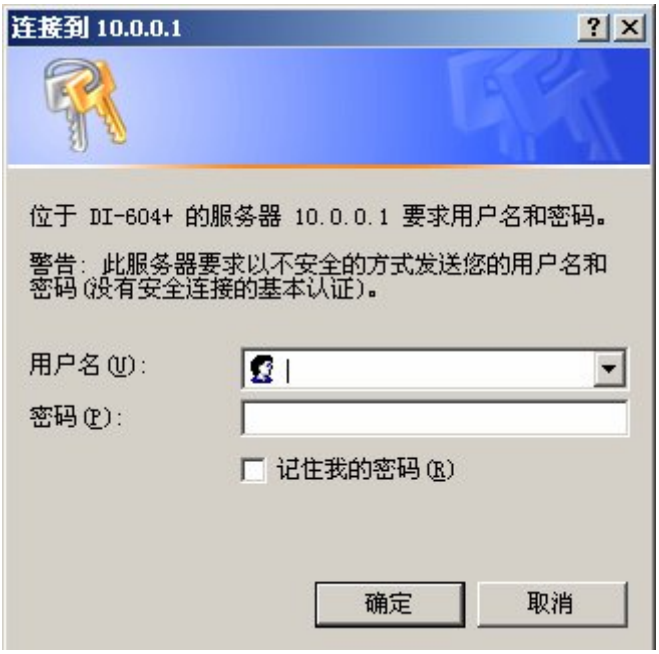


图 4

■方法 3：无线定位

根据对比无线信号的强弱，也能够为搜寻无线路由器/AP 的位置提供有力依据。出于实际情况的考虑，这里就不讨论过于高端的无线探测硬件设备，只讨论相对便于实现且成本较低的方法。

这里需要简单提及一下天线的知识，无线网卡使用的天线主要有两种，分别是全向天线和定向天线。如下图 5 所示笔记本电脑用 PCMCIA 接口无线网卡采用的都是全向天线。而大家常用的笔记本内置的 Intel、Dell 等无线网卡使用的也是全向天线。在实际工作及生活中，无论电脑的朝向如何，全向天线的信号强度都保持不变，因而使用特别方便。

图 5

其次，判断无线信号的强弱还需要使用信号强度工具。信号强度工具用于测量来自 AP 的 RF 射频信号。信号越强，与 AP 的距离就越近。信号强度探测器有多种类型。最常见的类型是软件实用程序，通常随安装在笔记本电脑中的网卡一起提供。不过除了这些不同网卡制造厂商配套的无线搜索工具外，为更清楚地查看信号衰减或者递增的情况，也可使用第三方软件，这些软件通常具有更强的信号强度测量功能。第三方应用程序可提供更为具体的度量，图表也更大、更便于使用，比如 NetStumbler、Commview for WiFi 之类的软件就可以实现无线信号源的搜索。下图为使用 Netstumble 进行无线信号探测的效果图，在下图 6 中可以清楚地看到随着无线网卡距离 AP 的接近，无线信号明显的增强。

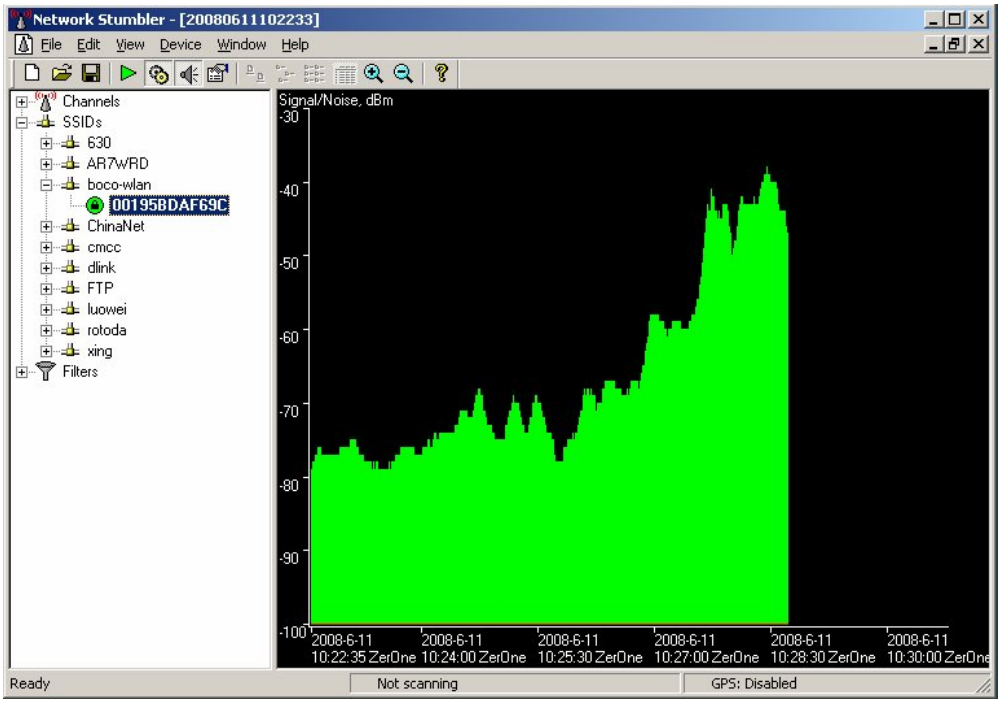


图 6

关于无线设备探测的工具和方法还有很多，但限于篇幅，这里仅抛砖引玉地介绍其中常见的几种。

2．MITM 中间人攻击

一旦确认了内部的无线路由器或者无线 AP 的具体 IP 及 MAC，比如连入办公网或者小

区内网的无线路由器，无线黑客就可以发动 MITM 中间人攻击来进行数据的拦截、伪造和破坏。这样，通过该无线路由器进行上网操作的资料和信息就会泄露在该设备所处的上层网络，从而被外部的无线黑客得手。关于中间人攻击的具体方法有很多文章都早已提及，这里就不再多言。依此延伸，DNS 欺骗、DHCP 欺骗等均可实现，限于篇幅，这里也就不再一一举例。如下图所示为对内网的一台无线路由器与网关的通信进行中间人攻击以截获交互的资料和上网内容。

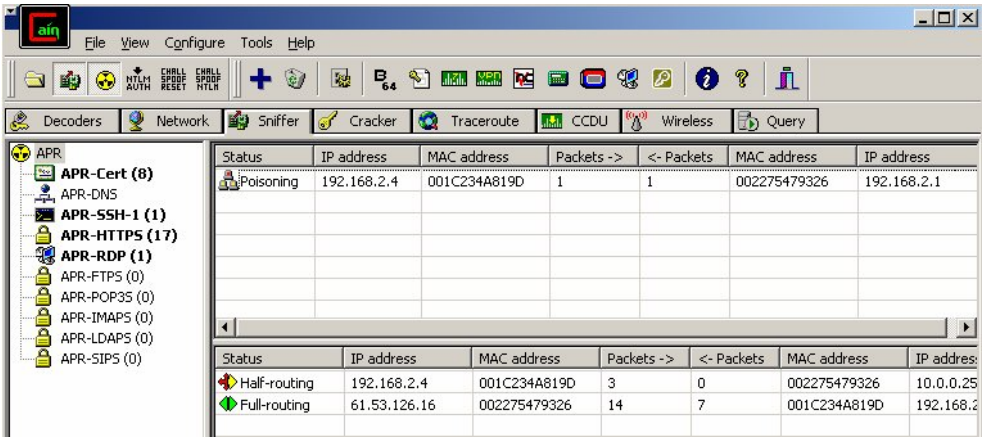


图 7

3．会话劫持攻击

作为无线路由器而言，也存在一些不同层面的漏洞，只要利用得当，无线黑客就可以轻而易举地劫持管理员的会话，这就是我们常说的会话劫持攻击，不过这里的受害者不再是主机，而是无线路由器。讲原理之前要强调一点会话劫持的前提是无线黑客已经具备连接目标无线网络的能力，即已经破解 WEP 或者 WPA-PSK 连接加密 !!! 若没有无法进行劫持。

■漏洞原理

由于一些无线路由器在对管理员进行认证时，仅仅是依据 IP 地址来区分合法管理员身份，所以只要无线黑客能够在合法用户使用管理员身份登录无线路由器后，在 timeout 时间未过期前，劫持其 IP 地址再次登录，就可以劫持已经认证的会话，从而获取管理员身份。

该漏洞最早被发现在 Belkin F5D8233-4 这款无线路由器上，但 Belkin 其它型号的无线路由器也疑似存在该漏洞。如下图 8 所示，这里我就使用目前市面上比较流行的型号为 F6D4230-4 这款 Belkin 无线路由器为例。

图 8

关于无线路由器认证会话劫持漏洞的使用并不难，不过顺序和思路尤为重要。无线黑客先使用多种无线分析工具对当前无线网络进行抓包分析，比如下图 9 所示，使用 airodump-ng 来对当前所有无线网络分析,在图 9 中上部分,我们可以看到存在一个 SSID 名为“ Belkin_ZerOne ”的无线网络，启用加密为 WPA-PSK；而在右下角，我们可以看到当前有两个连接至该无线路由器的无线客户端。其中，

00：0E：E8：D3：BF：71 是

00：1F：3C：45：56：00 是

以上两者都已经连接至 SSID 名为“ Belkin_ZerOne ”的无线网络。

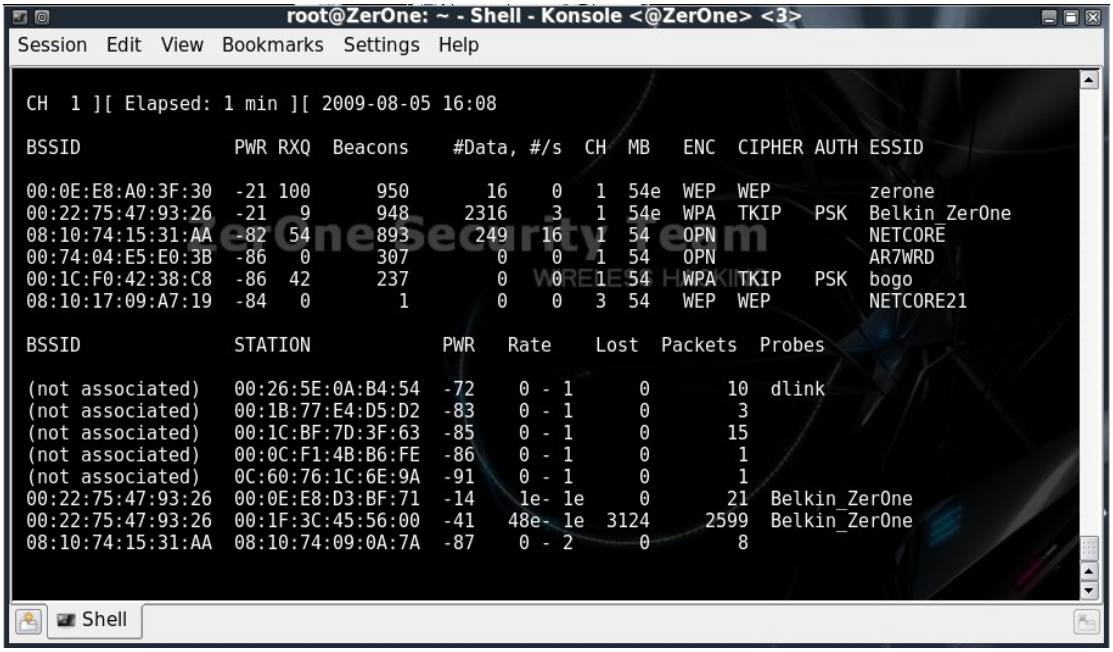


图 9

通过简单的无线 D.O.S 可以对该无线网络进行一段时间扰乱攻击，之后无线黑客会不断尝试登陆 Belkin 无线路由器管理页面来核查合法用户是否登录。当合法用户已经登录无线路由器进行操作时，Belkin 会“ 很友好 ”地给出如下图所示的提示：

“ 复制管理员，A user at 192.168.2.3 is managing the router. ”意思就是说当前已经有一个管理员登录进无线路由器进行操作了，而该管理员来自 192.168.2.3。如下图 10 所示。

图 10

这样，无线黑客就拿到了具备管理员能力的客户端 IP，并且确认当前该客户端用户正在以管理员身份登录无线路由器。对照一下之前图所示的内容，无线黑客就找到了该 IP 对应的 MAC 地址。接下来无线黑客只需要迅速修改自身 IP 与之前已连接客户端 IP 一致，并连接无线路由器。如下图 11 所示，在 Linux 下的无线网络连接界面中会显示已经成功连接，在下方的状态栏中显示出“Connected to Belkin_ZerOne at 77%（IP：192.168.2.3）”，即无线黑客已经以 192.168.2.3 这样的 IP 连接到了该无线网络。

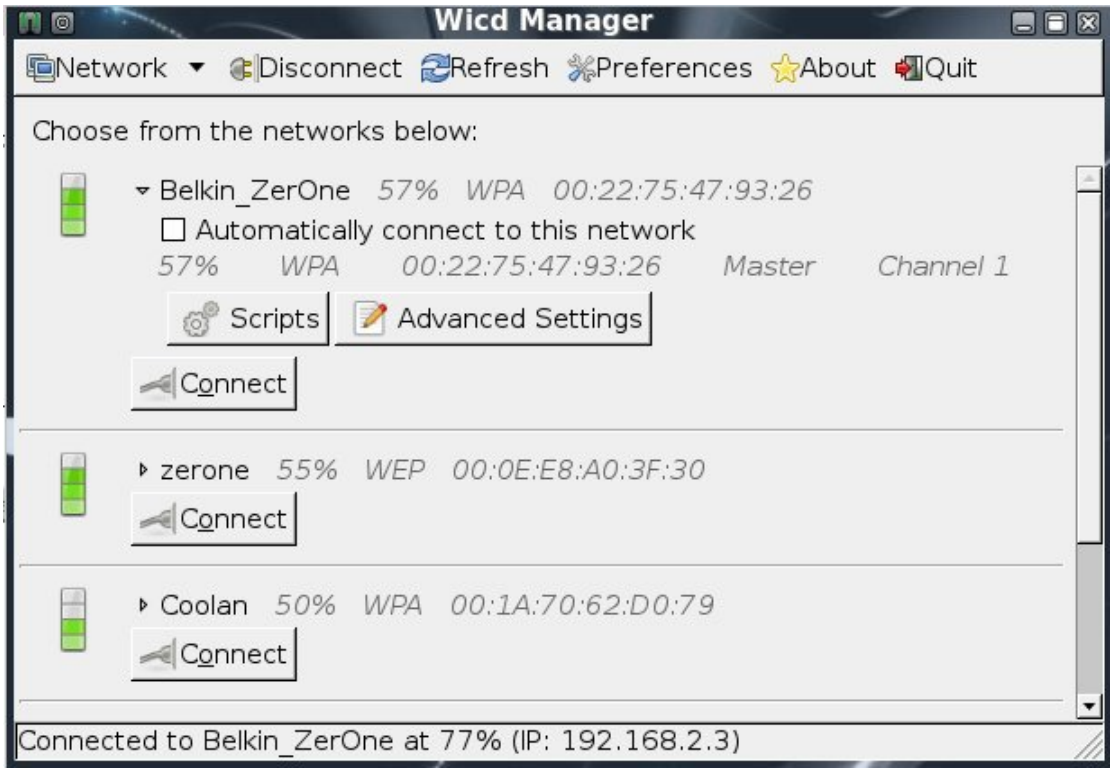


图 11

此时，无线黑客在浏览器中输入 192.168.2.1 来访问 Belkin 无线路由器，会发现已

经直接打开管理页面而无须输入密码，可以任意操作了。到此，无线黑客成功完成会话劫持，并以管理员身份登录无线路由器可以进行任意配置。

4．默认 WPA-PSK 连接密钥

对于一些特定型号的无线路由器，在默认情况下，其提供的无线网络支持 WEP 或者 WPA-PSK 加密方式，并且提供了出厂就设置好的默认 WEP 或者 WPA-PSK 加密密码。比较典型的如 FON。

作为非常有名的 FON 无线路由器，其建立全球免费无线热点网络的构想可以算得上是伟大，作为其提供的 FON 无线路由器，在默认情况下使用名为“Myplace”这样的 SSID 来提供无线网络，并且该网络默认就要求 WPA-PSK 加密方式。其密码是在出厂时就设定好的，并标注在其产品背面。如下图 12 所示，这台 FON 无线路由器的默认 WPA-PSK 密码为 7130000877。

这样的话，对于无线黑客而言，一旦发现名为“Myplace”这样 SSID 的无线网络，就可以进行 Deauth 攻击来获取其 WPA 握手包，并导入本地字典破解。由于 FON 在默认情况下使用纯数字作为 WPA-PSK 加密密码使用，所以只要构建这样的 10 位纯数字字典，就可用于快速的破解。

图 12

关于破解 WPA-PSK 的过程及步骤就不再演示了，最早在 2007 年 12 月的黑防上我那篇破解 WPA-PSK 一文就已经登出了具体的方法。唯一的区别在于，对于使用 FON 这样默认 WPA-PSK 密码的用户而言，上述威胁更大些。

5．验证绕过攻击

我们都知道，即使 WEP 或者 WPA-PSK 连接密码已经被破解，但是由于登录密码的限制，无线黑客们仍然无法轻易地访问无线路由器的配置页面进行修改，这也是很多网管员所

庆幸的。不过貌似令人遗憾的是，对于个别厂商的某些型号无线设备而言，攻击者甚至无需验证即可直接下载该设备几乎全部的配置页面。如下图 13 所示，使用某款整站下载工具将该设备配置页面全部强制下载到本地，除了个别报错外，其它主要的页面都已经下载到本地。

图 13

打开管理页面的源代码，如下图 14 所示，在黑框处可以看到在“ http_passwd ”旁，“ value= ”后面显示的就是加密过的管理员密码“ Y2pjaG53cw== ”

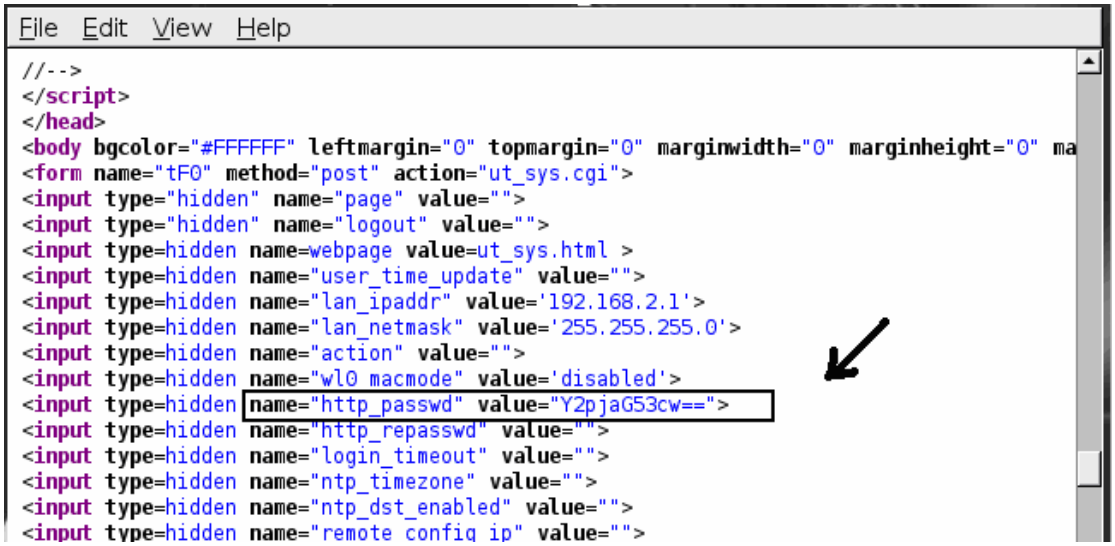


图 14

在源文件中上下拉动查找“ http_passwd ”相关的定义信息，可以看到如下图 15 所示内容，在对于“ http_passwd ”的加密方式有着明确的定义，即使用 base64 编码方式。

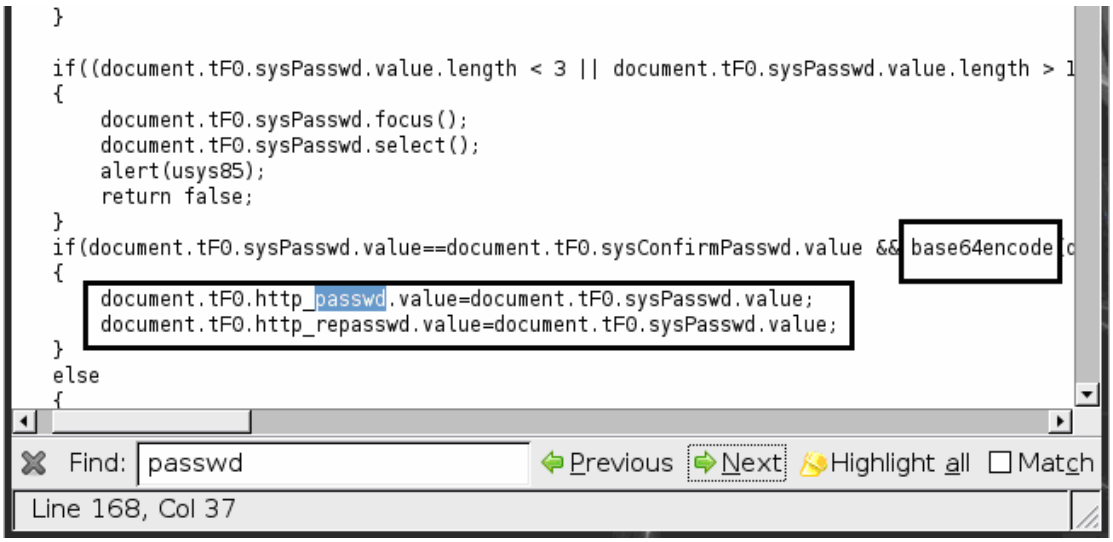


图 15

既然已经获知了管理员密码“ Y2pjaG53cw== ”是经过 base64 加密的，那么接下来只需要使用 base64 的解码工具即可还原出密码。如下图 16 所示，在“ Base64 encrypted password ”栏输入之前获取的管理员密码“ Y2pjaG53cw== ”，在其下方的“ Decrypted password ” 栏就会立即显示出实际对应的密码为 “ cjchnws ”。这样，我们就成功地得到了无线路由器的管理员密码。

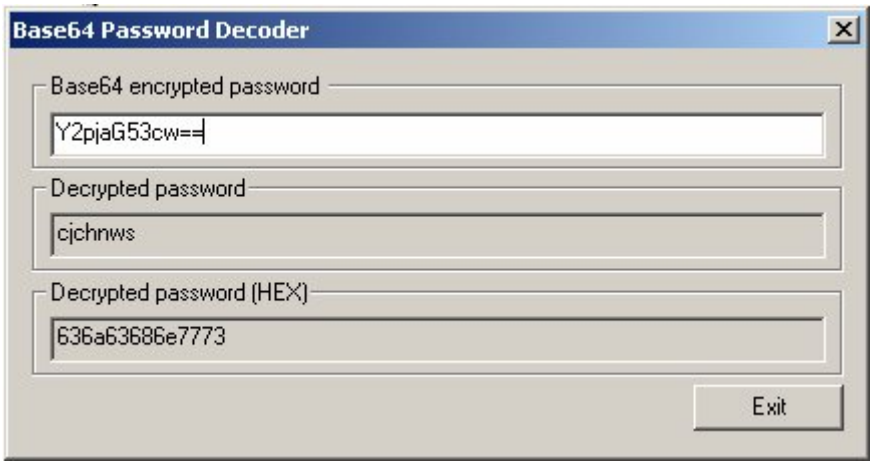


图 16

那么，作为攻击者而言，真正的渗透就可以开始了。不但可以在以后随意登录无线路由器，还可以设定端口映射，设置多个 SSID 广播，设置多个备选 WEP 加密密码等。这个无线路由器从此也就宣告着彻底地陷落，而对于该无线网络而言，只是出现了一个临时中断的情况，这在平时也是偶然会发生的情况，所以绝大多数无线用户还根本不知道发生了什么事！

6. UPNP 攻击

微软给出的解释：通用即插即用(UPnP)是一种用于 PC 机和智能设备(或仪器)的常见对等网络连接的体系结构，尤其是在家庭中。UPnP 以 Internet 标准和技术(例如 TCP/IP、HTTP 和 XML)为基础，使这样的设备彼此可自动连接和协同工作，从而使网络(尤其是家庭网络)对更多的人成为可能。关于 UPNP 的结构和作用我就不再废话了，这方面的资料很多，大家可以 Google 或者 baidu 一下会有很多收获。这里我要提示的是，要知道，对于

绝大多数无线路由器而言，UPNP 默认是开启的。

无线黑客们除了可以使用 UPNP 工具轻松地查看无线路由器的基本信息外，还可以查看详细的网络设备资料，比如公司名称、产品类型、设备型号、内部设计号等。该参数将有助于无线黑客判断出具体的无线网络设备型号。为了方便大家查看及参考，下面我就以目前市面上较为流行的日产 BUFFALO 无线设备为例。

■查看 BUFFALO 无线设备资料

由下图 17 所示，在最上面“ InternetGatewayDevice ”标识下，可以看到在“ manufacturerURL ”即制造商网址处给出了 buffalo 厂商的日本官网，而在下方“ modelName ”处显示为 WHR-HP-G54，即该设备的具体型号。在“ friendlyName ”和“ modeDescription ”处，可以看到显示为 BUFFALO WHR-HP-G54 Router，即为 BUFFALO 的无线路由器产品，该型号可以在网上直接查到。同样地，知道了具体型号，对于无线黑客而言，就可以根据该型号进行其它漏洞的查询。

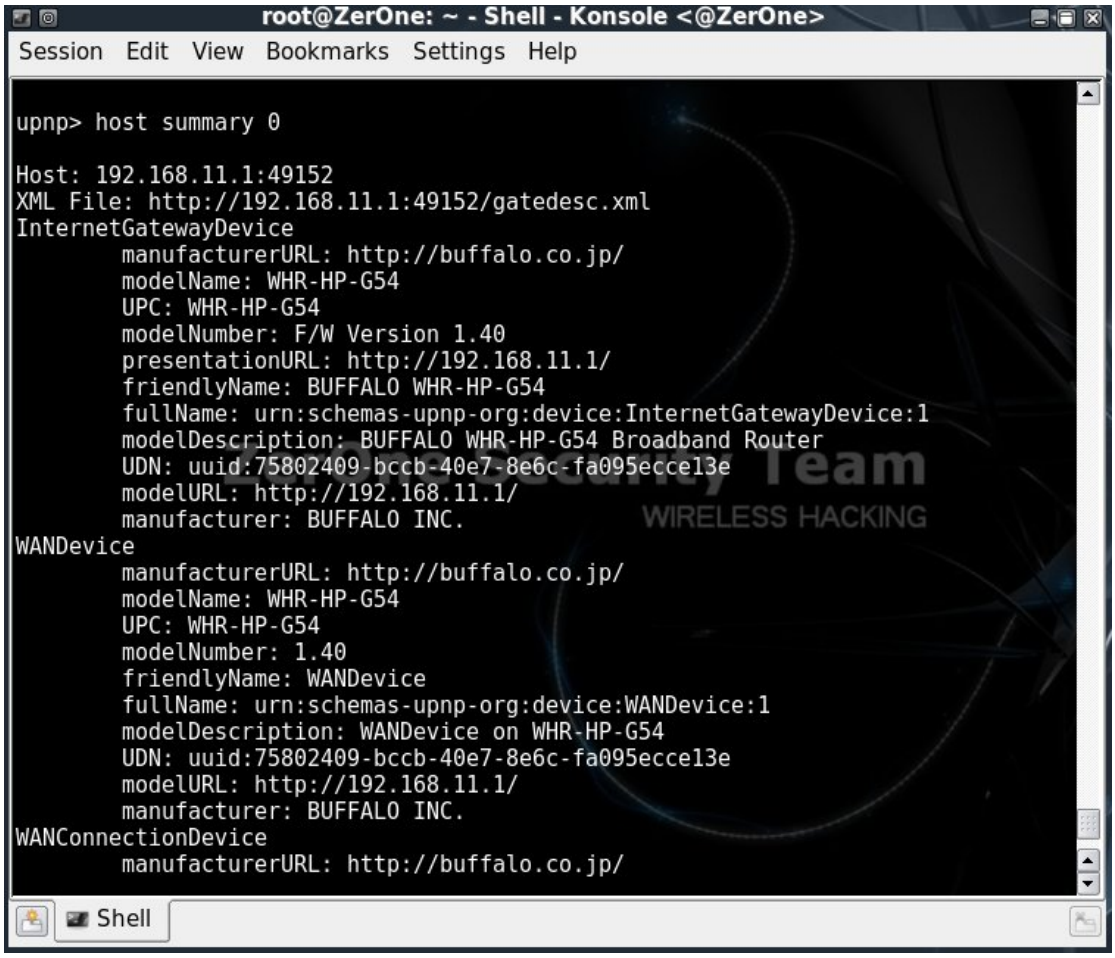


图 17

■获取外网连接状态

无线黑客可以通过 UPNP 获取当前路由器外部网络连接状态，如下图 18 所示内容。其中，在“ NewConnectionStatus ”处显示为 Disconnected，即没有与外部网络连接。

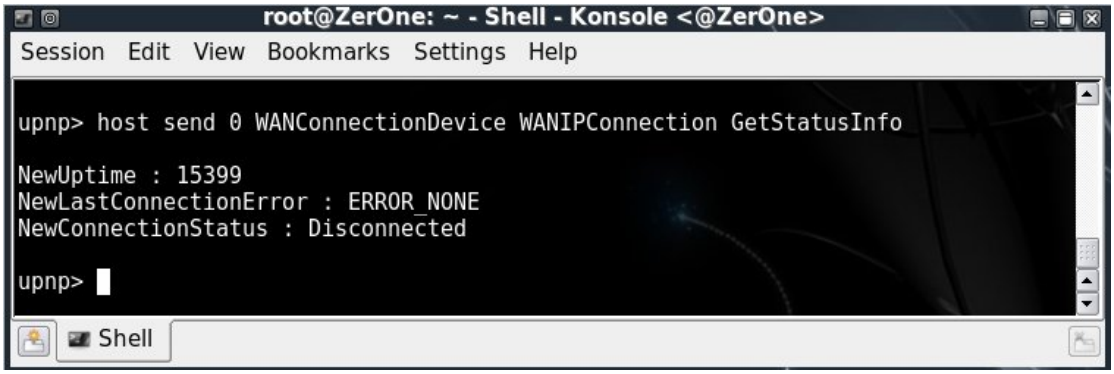


图 18

■查看路由器外网连接 IP

无线黑客可以通过 UPNP 获取当前路由器外部网络连接 IP 地址，如下图 19 所示内容。其中，在“ NewExternalIPAddress ”处显示为 10.0.0.129，这个就是该无线路由器接入的外部地址，也就是真正的企业/机构内部网络地址。

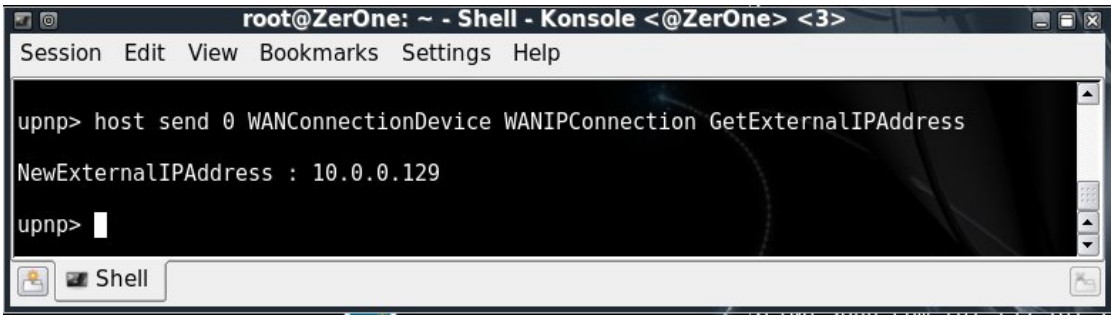


图 19

■查看端口映射状态

在成功添加完毕端口映射后，无线黑客可以通过 UPNP 获取当前路由器端口映射情况，如下图 20 所示内容。

图 20

7. SNMP 攻击

SNMP (Simple Network Management Protocol,简单网络管理协议)是专门设计用于在 IP 网络管理网络节点（服务器、工作站、路由器、交换机及 HUB 等）的一种标准协议，它是一种应用层协议。SNMP 使网络管理员能够管理网络效能，发现并解决网络问题以及规划网络增长。通过 SNMP 接收随机消息（及事件报告）网络管理系统获知网络出现问题。

由于 SNMP 的效果显著，所以网络硬件厂商开始把 SNMP 加入到它们制造的每一台设备。今天，各种网络设备上都可以看到默认启用的 SNMP 服务，从交换机到路由器，从防火墙到网络打印机，无一例外。

那么目前在 SNMP 上造成威胁的主要问题是许多厂商安装的 SNMP 都采用了默认的通信字符串，这些通信字符串是程序获取设备信息和修改配置必不可少的。采用默认通信字符串的好处是网络上的软件可以直接访问设备，无需经过复杂的配置。

通信字符串主要包含两类命令：GET 命令，SET 命令。GET 命令从设备读取数据，这些数据通常是操作参数，例如连接状态、接口名称等。SET 命令允许设置设备的某些参数，这类功能一般有限制，例如关闭某个网络接口、修改路由器参数等功能。但很显然，GET、SET 命令都可能被用于拒绝服务攻击（DoS）和恶意修改网络参数。

■修改网络设备参数

最常见的默认通信字符串是 public（只读）和 private（读/写），除此之外还有许多厂商私有的默认通信字符串。几乎所有运行 SNMP 的网络设备上，都可以找到某种形式的默认通信字符串。如下图 21 所示，在默认情况下，该网络设备名称为“ 2_WAN_QOS_Router ”

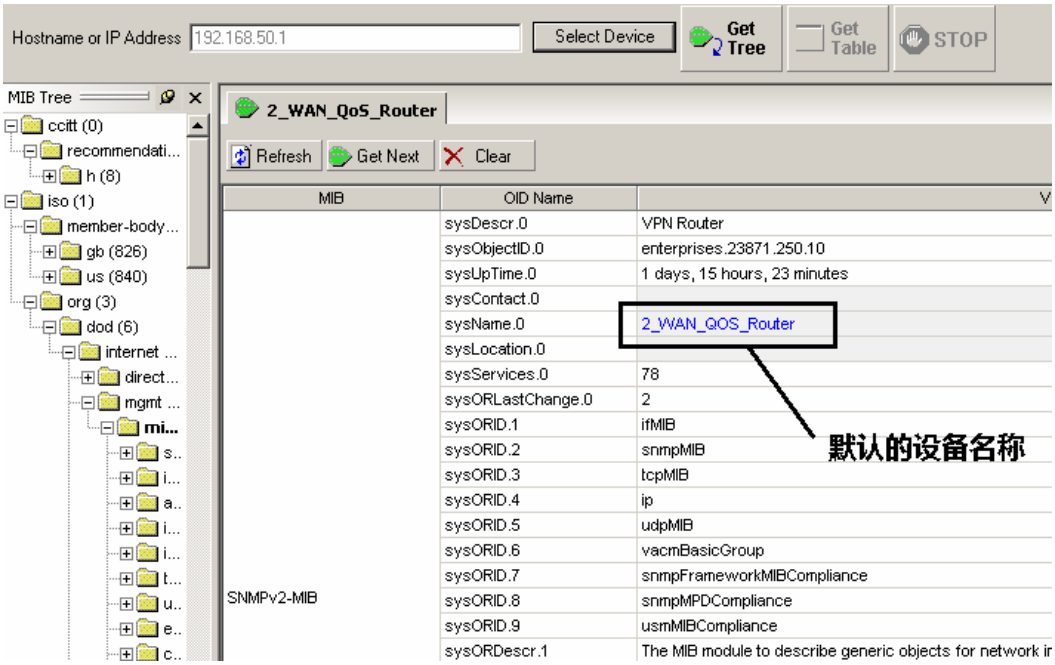


图 21

如下图 22 所示为使用默认字符串修改后的无线网络设备名称，可以看到，名称已经改为“ 2_WAN_ZerOne_Router ”，并且所在位置一栏也被修改为“ ZerOne Security Team ”，甚至联系方式也被改为 longaslast@gmail.com。

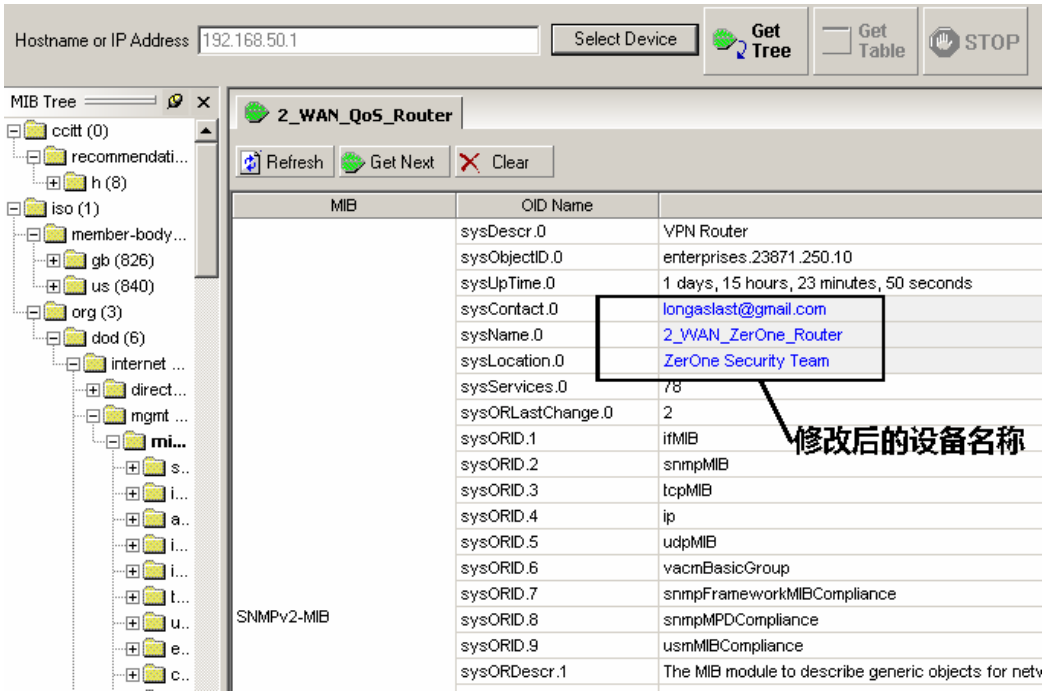


图 22

■截获 SNMP 字符串

SNMP 2.0 和 SNMP 1.0 的安全机制比较脆弱，通信不加密，所有通信字符串和数据都以明文形式发送。无线黑客一旦捕获了网络通信，就可以利用各种嗅探工具直接获取通信字符串，即使用户改变了通信字符串的默认值也无济于事。如下图 23 所示为在一个 2 层无线网络环境中截获用户对上层设备配置的 SNMP 字符串。

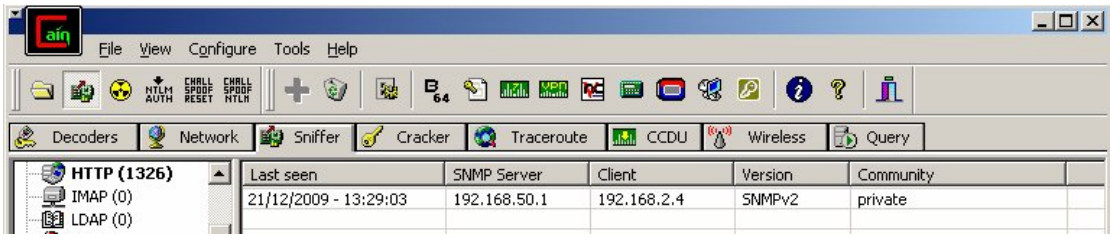


图 23

近几年才出现的 SNMP 3.0 解决了一部分问题。为保护通信字符串，SNMP 3.0 使用 DES（Data Encryption Standard）算法加密数据通信；另外，SNMP 3.0 还能够用 MD5 和 SHA（Secure Hash Algorithm）技术验证节点的标识符，从而防止无线黑客冒充管理节点的身份操作网络。

虽然 SNMP 3.0 出现已经有一段时间了，但目前还没有广泛应用。如果设备是 2、3 年前的产品，很可能根本不支持 SNMP 3.0；甚至有些较新的设备也只有 SNMP 2.0 或 SNMP 1.0。即使设备已经支持 SNMP 3.0，许多厂商使用的还是标准的通信字符串，这些字符串对黑客组织来说根本不是秘密。因此，虽然 SNMP 3.0 比以前的版本提供了更多的安全特性，如果配置不当，其实际效果仍旧有限。

8．Config 文件泄露

对于无线路由器来说，所有已经执行的设置都已经保存在备份文件中，而一些不够严谨的设备，对于内网中发出的下载请求会默认允许通过，如目前市面上流行的多款韩国的 IPTime 无线路由器都存在这样一个漏洞，就是未经验证即可下载配置文件。

无线黑客只要输入下述地址：http://192.168.0.1/config.cfg，就可以从没有登录的无线路由器上直接下载该路由器的配置备份文件。如下图 24 所示。

图 24

而在对 config 文件进行分析后，虽然绝大多数路由器厂商都使用了自己的加密措施，但是在使用一些分析工具后，还是能够获取到一些敏感的配置信息，甚至是一些该网络设备的具体配置参数。如下图 25 为在 Linux 下进行简单的 16 进制码查看。

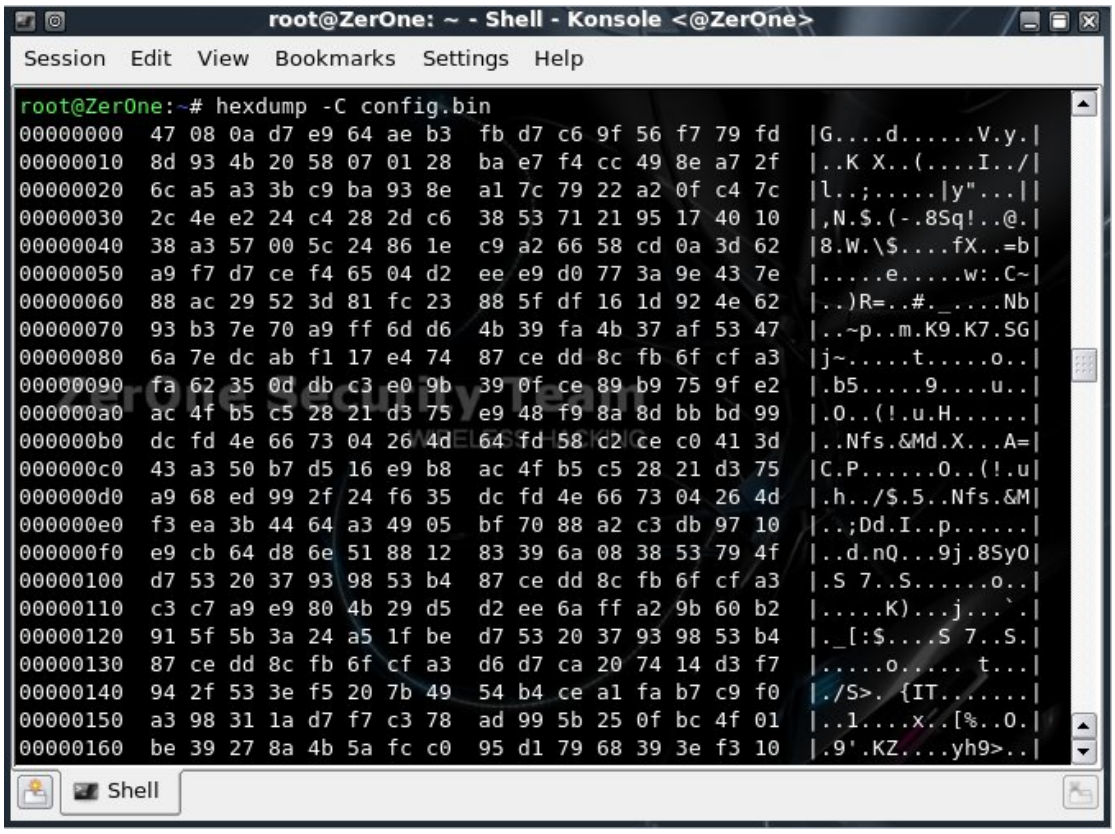


图 25

再抛砖引玉一下，自行制作设置好的 config 文件，在攻击时直接覆盖目标无线设备的原配置文件，是一种极为快速的入侵方式和技巧，请感兴趣的朋友仔细体会。

9．无线 D.O.S 攻击

和传统的有线网络一样，无线路由器也会面临无线 D.O.S 攻击的威胁。先简单说明一下原理。IEEE 802.11 定义了一种客户端状态机制，用于跟踪工作站身份验证和关联状态。无线客户端和 AP 基于 IEEE 标准实现这种状态机制，如下图 11-16 所示。成功关联的客户站停留在状态 3，才能进行无线通信。处于状态 1 和状态 2 的客户站在通过身份验证和关联前无法参与 WLAN 数据通信过程。

在下图 26 中，无线客户端根据它们的关联和认证状态，可以为 3 种状态中的任意一种。如下表 2 内容所示。

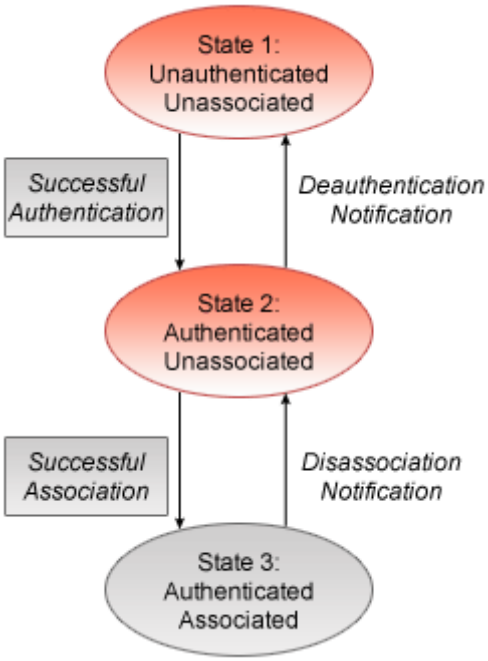


图 26

表 2

状态机制	客户端状态	客户端具体表现	备　注
State 1	Unauthenticated Unassociated	没有通过验证，没有和 AP 建立关联	无线客户端处于搜索及试图连接 AP 阶段
State 2	Authenticated Unassociated	通过验证，没有和 AP 建立关联	无线客户端已经输入正确的连接密码并等待
State 3	Authenticated Associated	通过验证，和 AP 建立关联	无线客户端被允许连接（AP 自动分配地址）

在获知了无线网络连接原理后，无线 D.O.S 原理也就很好理解了，不过由于无线 D.O.S 的分类太多，为方便大家查看，下面我举几个常见的无线 D.O.S 类型。

■取消验证洪水攻击

取消验证洪水攻击，国际上称之为 De-authentication Flood Attack，全称即取消身份验证洪水攻击或验证阻断洪水攻击，通常被简称为 Deauth 攻击，是无线网络拒绝服务攻击的一种形式，它旨在通过欺骗从 AP 到客户端单播地址的取消身份验证帧来将客户端转为未关联的/未认证的状态。对于目前广泛使用的无线客户端适配器工具来说，这种形式的攻击在打断客户端无线服务方面非常有效和快捷。一般来说，在无线黑客发送另一个取消身份验证帧之前，客户站会重新关联和认证以再次获取服务。无线黑客反复欺骗取消身份验证帧才能使所有客户端持续拒绝服务。

为方便大家理解，我绘制了取消身份验证洪水攻击原理图，在下图 27 中可看到无线黑客为了将所有已连接的无线客户端“踢下线”，对整个无线网络发送了伪造的取消身份验证报文。

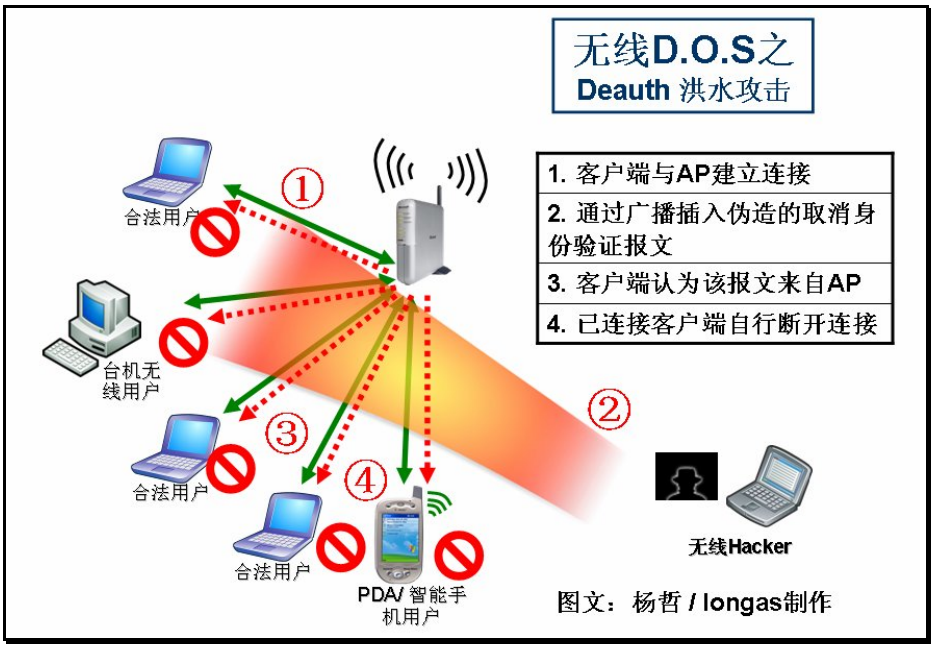


图 27

无线黑客们通过发送 Deauthentication 取消验证数据包文，达到中断已连接的合法无线客户端正常通信的目的，并在长时间持续大量发送此类报文的基础上，使得无线网络一直处于瘫痪状态。

可以使用的工具有很多，比如在 Linux 下比较有名的 MDK2/3，或者早一点的 Void11 等，我们也可以使用 aireplay-ng 的其中一个参数-0 配合实现。注意该攻击发包速率并不会维持在某个固定数值，而是根据网卡性能等情况维持在 15~100 个包每秒这样一个范围。如下图 28 所示，发包速率为 76 个每秒。

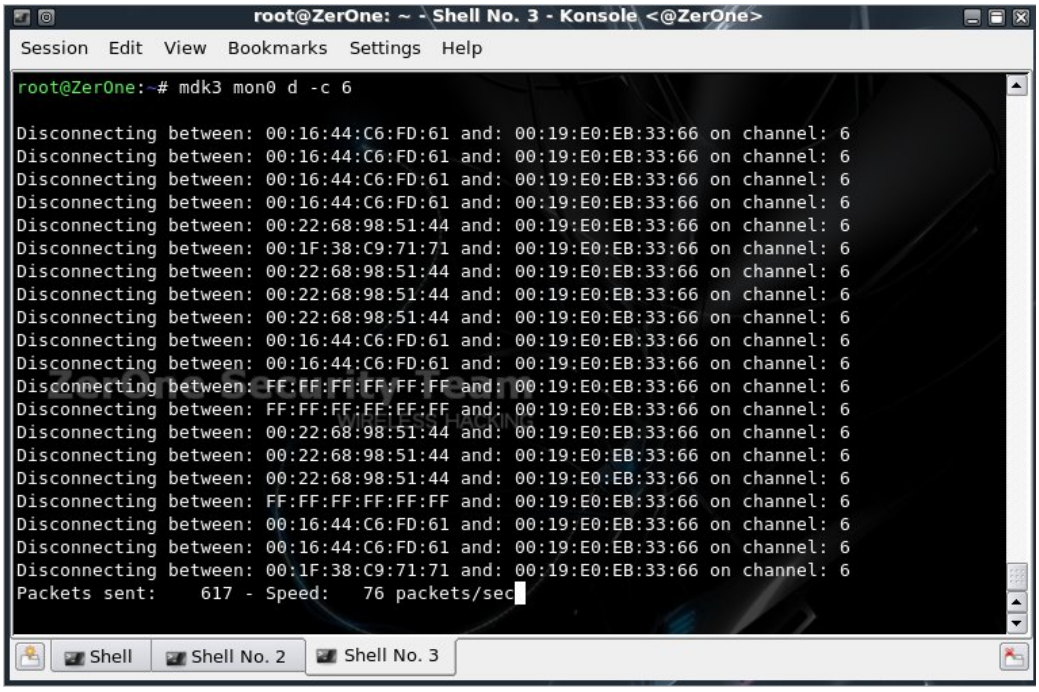


图 28

在察觉到网络不稳定时，管理员应该立即着手捕获数据包并进行分析，这样可以便于迅速判断攻击类型。下图 29 所示为无线网络在遭到 Deauth 攻击出现不稳定状况时，使用 Wireshark 抓包的结果分析，可以看到有大量连续的包含 802.11 Deauthentication 标示的数据报文出现。

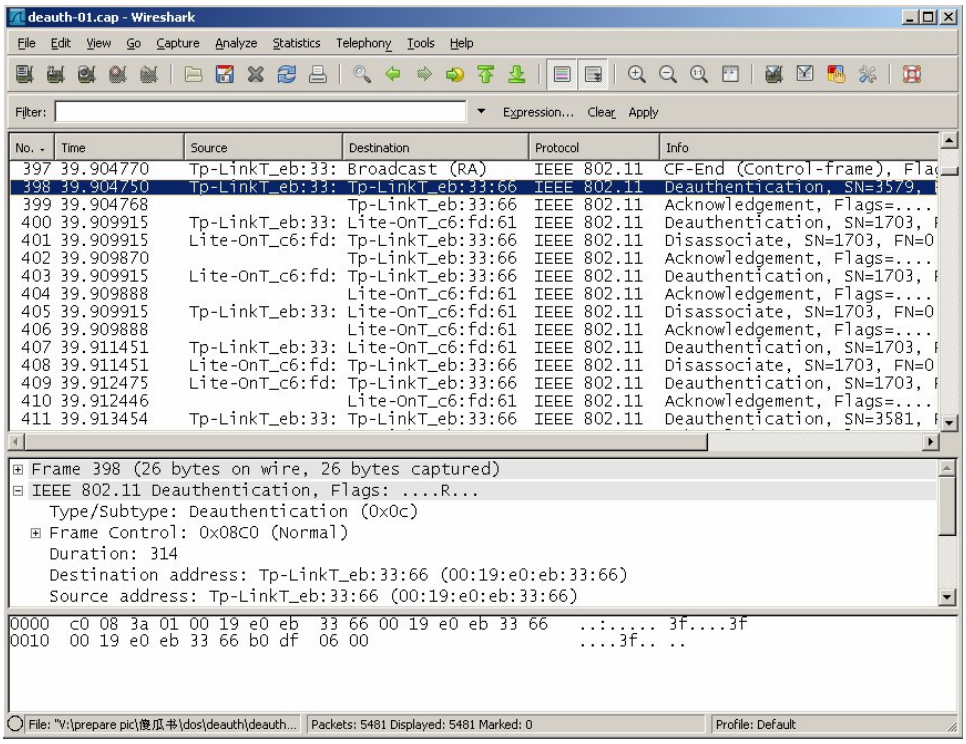


图 29

需要注意的是，伴随着 Deauthentication 数据包的出现，随之出现的就是大量的 Disassociation 数据包，这是因为先取消验证，自然就会出现取消连接，也就是断开连接的情况了。

■关联洪水攻击

关联洪水攻击，国际上称之为 Association Flood Attack，全称即关联洪水（泛洪）攻击，通常被简称为 Asso 攻击，是无线网络拒绝服务攻击的一种形式。它试图通过利用大量模仿的和伪造的无线客户端关联来填充 AP 的客户端关联表，从而达到淹没 AP 的目的。

恩，这么说吧，由于开放身份验证（空身份验证）允许任何客户端通过身份验证然后关联。利用这种漏洞的无线黑客可以通过创建多个到达已连接或已关联的客户端来模仿很多客户端，从而淹没目标 AP 的客户端关联表。同样为方便大家理解，可以参考下面我绘制的图 30 所示。可以看到，当客户端关联表溢出后，合法无线客户端将无法再关联，于是就形成了拒绝服务攻击。

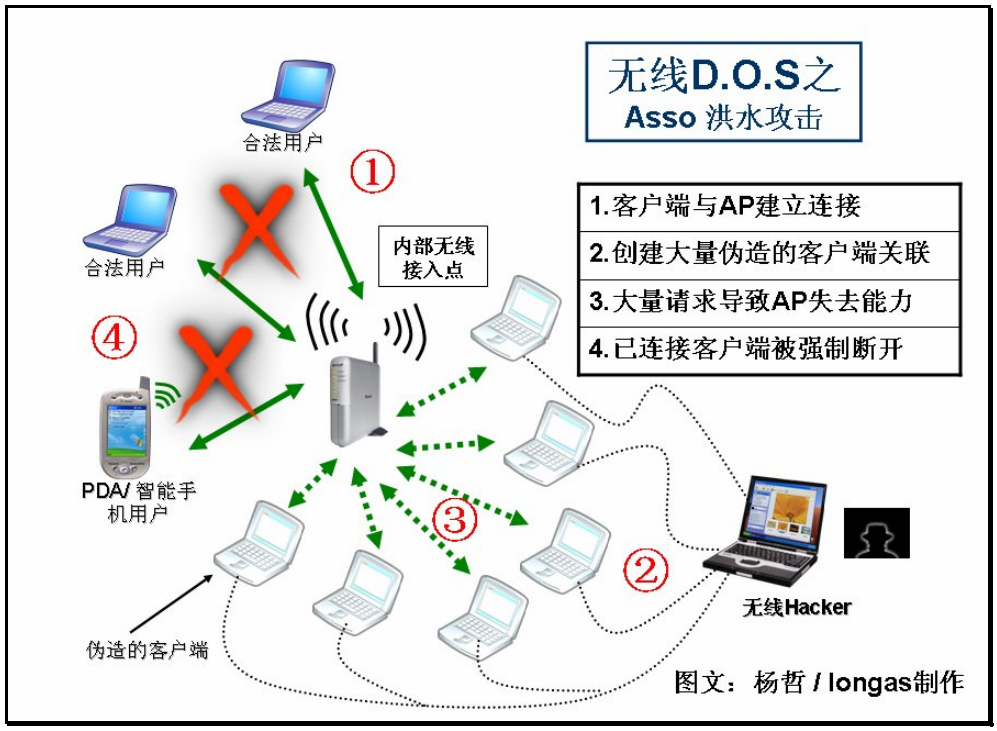


图 30

一旦无线路由器/接入点的连接列表遭到泛洪攻击，接入点将不再允许更多的连接，并会因此拒绝合法用户的连接请求。当然，还有一种可能是无线黑客集合了大量的无线网卡，或者是改装的集合大量无线网卡芯片的捆绑式发射机（类似于我们常说的“短信群发器”），进行大规模连接攻击的话，对于目前广泛使用的无线接入设备，也将是很有效果的。

当无线网络遭受到此类攻击时，我们可以对当前无线网络进行监测和分析，就能够看到如下图 31 所示的情形：遭到洪泛攻击的接入点网络数据，出现了大量无法验证的无线客户端 MAC 及请求。

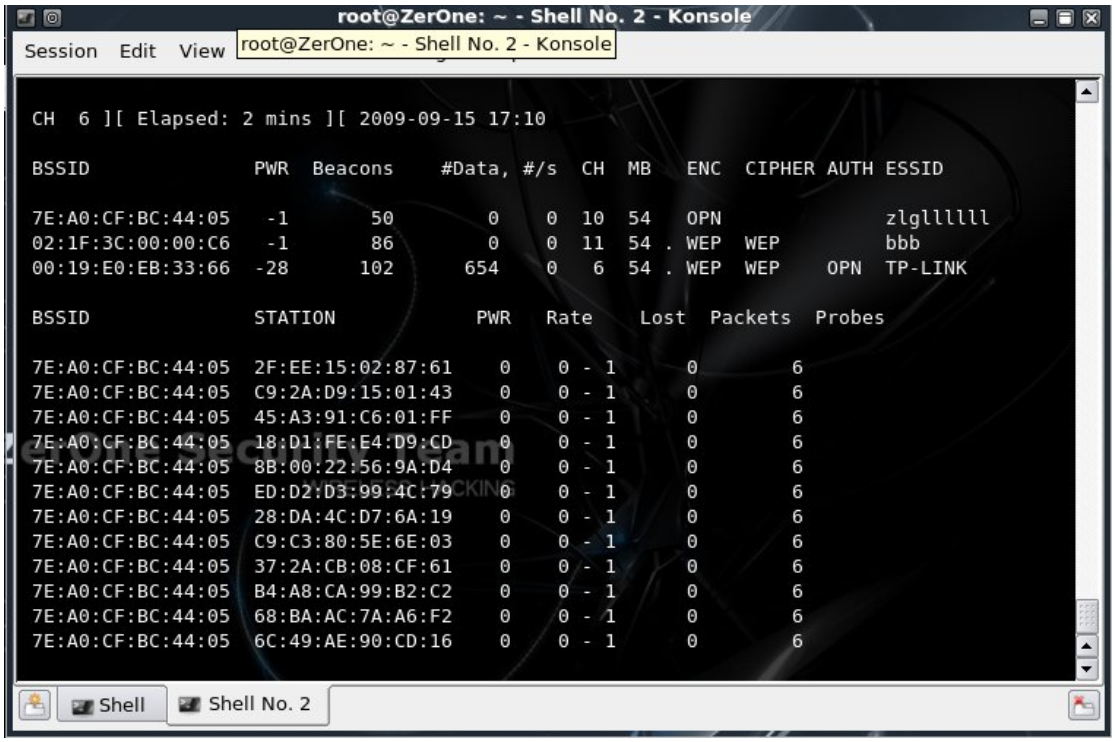


图 31

■RF 干扰攻击

如果说前面几种 D.O.S 攻击时还是主要基于无线通信过程及协议的话，那么 RF 干扰攻击就是完全不同的一种攻击方式了。

RF 干扰攻击，国际上称之为 RF Jamming Attack，在个别老外写的文章中有时也称之为 RF Disruption Attack，该攻击是通过发出干扰射频达到破坏正常无线通信的目的。其中，RF ，全称为 Radio Frequency ，即射频，主要包括无线信号发射机及收信机等。在通信领域，关于无线信号干扰和抗干扰对策一直是主要研究方向之一。

这个其实很好理解，这类工具大家也可能都见过或者听说过，就好比说考四六级英语，我们常看到报纸上提及的那个“ 手机信号屏蔽器 ”就是类似的东西，如下图 32 所示为国内目前正在使用的手机干扰机，只要一打开，就可以保证半径为几十或者几百米之内所有的手机无法连接基站，原理完全一样，只不过“ 手机信号屏蔽器 ”的覆盖频率只涉及了 GSM 或者 CDMA 工作频段而已。下图 33 所示为车载手机/GPS 多功能干扰机。

图 32

图 33

Ok，同样地，我也绘制了这样一幅无线 RF 干扰攻击原理图以供参考。如下图 34 所示。

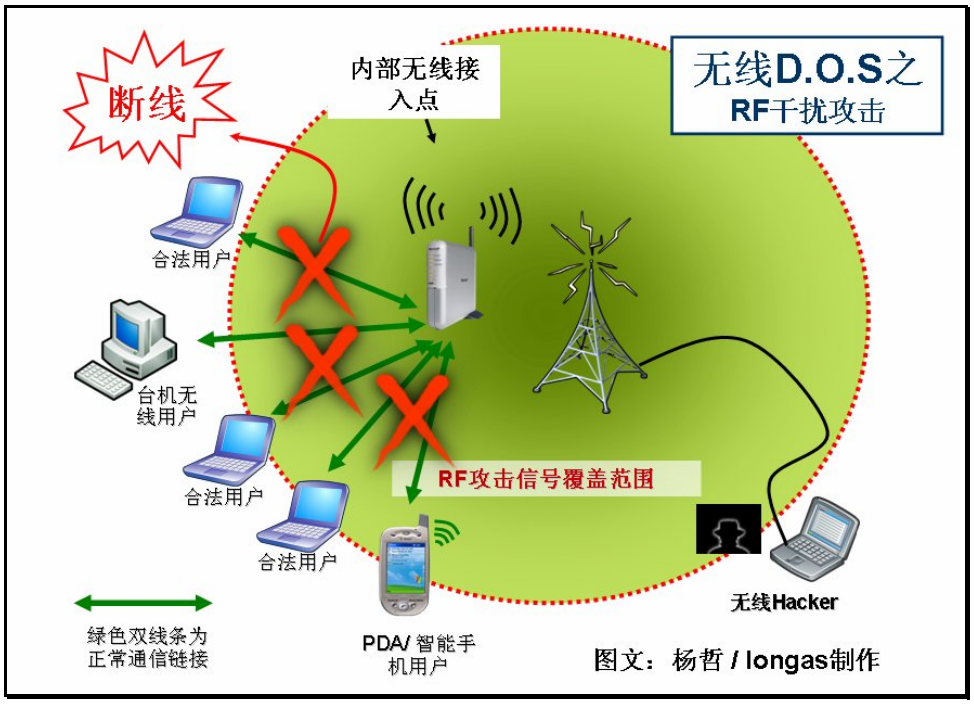


图 34

需要说明的是，由于目前我们普遍使用的无线网络都工作在 2.4GHz 频带范围，此频带范围包含 802.11b、802.11g、802.11n、蓝牙等，具体如下表 3 所示，所以针对此频带进行干扰将会有效地破坏正常的无线通信，导致传输数据丢失、网络中断、信号不稳定等情况出现。

表 3 无线网络工作频段

标准	速率	频率
802.11b	11 Mbps	2.4000 -- 2.4835GHz
802.11g	54 Mbps	2.4000 -- 2.4835GHz
802.11n	540 Mbps	2.4000 -- 2.4835GHz

10．小结

我们都知道一旦无线路由器被攻破，那就意味着该无线网络彻底地陷落，以上为目前针对无线路由器及无线 AP 的一些主要攻击手法，但并不是说除此之外就没有了，更多的方法我会在**《无线网络安全攻防实战》**后续的无线安全著作**《无线网络安全攻防进阶》**中给出实例和讲解，也欢迎感兴趣的朋友来我博客或者写信与我交流。本文诞生的另一个原因是，在过去的 3 年里，身为国内最早的无线安全板块超版，看到很多无线或者黑客类网站、论坛仍在大量转载一些破解 WEP 或者 WPA 破解的文章（有些甚至是我 07 年发的），一直觉得颇有些哭笑不得，难道无线安全就只是这点东西？这里我只想说：作为无线安全来说，不仅仅是破解 WEP 或者 WPA-PSK 密码那么简单，其涵盖的方面和内容远比表明呈现的丰富得多。

正如我们常说的：别被流言蒙蔽了双眼。