无线网攻击工具进攻方法及防范技巧

对无线网安全攻防有兴趣的人应该都需要一套工具,英特网上有很多免费的工具。本文不求全面，但求能提供一些指导和建议。

1. 找到无线网络

找到无线网络是攻击的第一步，这里推荐两款常用工具:

1.1Network Stumbler a.k.a NetStumbler

这个基于 Windows 的工具可以非常容易地发现一定范围内广播出来的无线信号，还可以判断哪些信号或噪音信息可以用来做站点测量。

1.2Kismet

NetStumbler 缺乏的一个关键功能就是显示哪些没有广播 SSID 的无线网络。如果将来想成为无线安全专家，您就应该认识到访问 点(Access Points)会常规性地广播这个信息。Kismet 会发现并显示没有被广播的那些 SSID，而这些信息对于发现无线网络是非常关键的。

2. 连上找到的无线网络

发现了一个无线网络后，下一步就是努力连上它。如果该网络没有采用任何认证或加密安全措施，你可以很轻松地连上它的 SSID。如果 SSID 没有被广播，你可以用这个 SSID 的名称创建一个文件。如果无线网络采用了认证和/或加密措施，也许，你需要以下工具中的某一个。

2.1Airsnort

这个工具非常好用，可以用来嗅探并破解 WEP 密钥。很多人都用 WEP，当然比什么都不用要好。在用这个工具时你会发现它捕获大量抓 来的数据包，来破解 WEP 密钥。还有其它的工具和方法，可以用来强制无线网络上产生的流量去缩短破解密钥所需时间，不过 Airsnort 并不具有这个功 能。

2.2CowPatty

这个工具被用作暴力破解 WPA-PSK，因为家庭无线网络很少用 WEP。这个程序非常简单地尝试一个文章中各种不同的选项 ,来看是否某一个刚好和预共享的密钥相符。

2.3ASLeap

如果某无线网络用的是 LEAP ,这个工具可以搜集通过网络传输的认证信息，并且这些抓取的认证信息可能会被破解。LEAP 不对认证信息提供保护，这也正是 LEAP 可以被攻击的主要原因。

不管你是不是直接连到了无线网络，只要所在的范围内有无线网络存在，就会有信息传递。要看到这些信息，你需要一个工具。

这就是 Ethereal。毫无疑问，这个工具非常有价值。Ethereal 可以扫描无线和以太网信息 ,还具备非常强的过滤能力。它还可以嗅探出 802.11 管理信息，也可被用作嗅探非广播 SSID。

前面提高的工具，都是你无线网络安全工具包中所必须的。熟悉这些工具最简单的办法就是在一个可控的实验环境下使用它们。这些工具都可以在英特网上免费下载到。

3. 防范这些工具

知道怎样使用上述工具是非常重要的，不过，知道怎样防范这些工具、保护你的无线网络安全更重要。

防范 NetStumbler:不要广播你的 SSID，保证你的 WLAN 受高级认证和加密措施的保护。

防范 Kismet:没有办法让 Kismet 找不到你的 WLAN，所以一定要保证有高级认证和加密措施。

防范 Airsnort:使用 128 比特的，而不是 40 比特的 WEP 加密密钥，这样可以让破解需要更长时间。如果你的设备支持的话，使用 WPA 或 WPA2，不要使用 WEP。

防范 Cowpatty:选用一个长的复杂的 WPA 共享密钥。密钥的类型要不太可能存在于黑客归纳的文件列表中，这样破坏者猜测你的密钥就需要更长的时间。如果是在交互场合，不要用共享密钥使用 WPA，用一个好的 EAP 类型保护认证，限制账号退出之前不正确猜测的数目。

防范 ASLeap:使用长的复杂的认证，或者转向 EAP-FAST 或另外的 EAP 类型。

防范 Ethereal:使用加密，这样任何被嗅探出的信息就很难或几乎不可能被破解。WPA2，使用 AES 算法，普通黑客是不可能破解的。WEP 也会加密 数据。在一般不提供加密的公共无线网络区域，使用应用层的加密，像 Simplite，来加密 IM 会话，或使用 SSL。对于需要交互的用户，使用 IPSec VPN，并关闭分隧道功能。这就强制所有的流量都必须通过加密隧道，可能是被 DES、3DES 或 AES 加密的。