七点措施安全组建家庭无线网络小技巧 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/142/2021_2022__E4_B8_83_E7_82_B9_E6_8E_AA_E6_c101_142513.htm 1. 修改用户名和密码(不使用默认的用户名和密码) 一般的家庭无线网络都是通过一个无线路由器或中继器来访问外部网络。通常这些路由器或中继器设备制造商为了便于用户设置这些设备建立起无线网络，都提供了一个管理页面工具。这个页面工具可以用来设置该设备的网络地址以及帐号等信息。为了保证只有设备拥有者才能使用这个管理页面工具，该设备通常也设有登陆界面，只有输入正确的用户名和密码的用户才能进入管理页面。然而在设备出售时，制造商给每一个型号的设备提供的默认用户名和密码都是一样，不幸的是，很多家庭用户购买这些设备回来之后，都不会去修改设备的默认的用户名和密码。这就使得黑客们有机可乘。他们只要通过简单的扫描工具很容易就能找出这些设备的地址并尝试用默认的用户名和密码去陆管理页面，如果成功则立即取得该路由器交换机的控制权。 2. 使用加密 所有的无线网络都提供某些形式的加密。之前我跟大家提过，攻击端电脑只要在无线路由器/中继器的有效范围内的话，那么它很大机会访问到该无线网络，一旦它能访问该内部网络时，该网络中所有是传输的数据对他来说都是透明的。如果这些数据都没经过加密的话，黑客就可以通过一些数据包嗅探工具来抓包、分析并窥探到其中的隐私。开启你的无线网络加密，这样即使你在无线网络上传输的数据被截取了也没办法(或者是说没那么容易)被解读。目前，无线网络中已经存在好几种加密技术。通常我们选

用能力最强的那种加密技术。此外要注意的是，如果你的网络中同时存在多个无线网络设备的话，这些设备的加密技术应该选取同一个。 3. 修改默认的服务区标识符(ssid) 通常每个无线网络都有一个服务区标识符(ssid)，无线客户端需要加入该网络的时候需要有一个相同的ssid，否则将被“ 拒之门外 ”。通常路由器/中继器设备制造商都在他们的产品中设了一个默认的相同的ssid。例如linksys设备的ssid通常是“ linksys ”。如果一个网络，不为其指定一个 ssid或者只使用默认ssid的话，那么任何无线客户端都可以进入该网络。无疑这为黑客的入侵网络打开了方便之门。 4. 禁止ssid广播 在无线网络中，各路由设备有个很重要的功能，那就是服务区标识符广播，即ssid广播。最初，这个功能主要是为那些无线网络客户端流动量特别大的商业无线网络而设计的。开启了ssid广播的无线网络，其路由设备会自动向其有效范围内的无线网络客户端广播自己的ssid号，无线网络客户端接收到这个ssid 号后，利用这个ssid号才可以使用这个网络。但是，这个功能却存在极大的安全隐患，就好象它自动地为想进入该网络的黑客打开了门户。在商业网络里，由于为了满足经常变动的无线网络接入端，必定要牺牲安全性来开启这项功能，但是作为家庭无线网络来讲，网络成员相对固定，所以没必要开启这项功能。 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