登录

WiFi安全技术 二：无线路由器配置和选择测试环境

ms0x0 / 2016-11-28 07:17:00 / 浏览数 2990 新手 入门资料 顶(0) 踩(0)

0x01 无线路由器基本原理

□

新手在买来一台新的路由器时，对照说明书上的设置步骤，在浏览器地址栏输入192.168.1.1时，可能并不能理解为什么要输入这样的数字。这样的数字组合就是我们常说的
这里我们不再解释OSI模型的由来，简单解释前文中我们提到的主机A和B的通信过程，用户将一封邮件发送给好友，好友读取到这条邮件的整个通信过程，就是在OSI模型中
路由器内部有一张路由表，用来作为转发的"地图"，在这个路由表中包含有该路由器掌握的所有目的网络地址，以及通过此路由器到达这些网络中的最佳路径，这个所谓最佳
路由器就是实现这一功能的硬件设备，它将不同的网段进行连接，使得网络通信得以穿越纵横交错密布的线路。无线路由器就是路由器家族的一个分支，在连接子网的终端中

0x02 无线路由器的各项配置

无线路由器不是调制解调器，在家庭中常见的拨号网络中，必须前置一台调制解调器才能够接入互联网。通常无线路由器在家庭网络连接中的物理连接方法如下：
目前由于宽带网路的提速和改进，前置的ADSL调制解调器（猫）的入户线缆已经改为光纤，并非过去使用的电话线，但主要功能结构不变。入户线缆通过调制解调器再通过
笔者在这里使用的是一款TP-LINK品牌的TL-WR842N型号无线路由器，根据说明书，在连接好网络线缆或设置好默认的无线连接账号，在浏览器的地址栏里输入192.168.0.
在说明书中寻找到初始的登录密码，进入下图所示的管理页面：
目前新款的无线路由器界面制作的相对旧款要图形化程度更高一些，可以清晰的显示目前无线路由器的各项连接状态。下面我们逐一介绍一下各项配置的功能作用。首先在主
这里清晰的显示了当前接入无线路由器的各项终端情况，设备前面的图标显示了设备是通过有线还是无线方式进行的连接。在这里分为主人网络和已禁设备，主人网络内即合
在这里显示了禁用设备的MAC地址，无线路由器禁用该设备的主要依据，就是禁止使用这个MAC地址的设备接入无线路由器的网络，这可以算作是一种安全保护机制，可防
在"应用管理"标签页面中，无线路由器给大家提供了多种扩展功能，如下图所示：
无线桥接：简单理解为路由器套接路由器，将同一个网络的无线信号覆盖范围扩大。 信号调节：调整无线路由器天线的发射功率，调整无线信号覆盖范围。
管理员身份限定：管理哪些终端可以登录设置路由器（像笔者现在这样） 虚拟服务器：作为端口映射功能，是一个重要的组建，设置界面如下：
这就相当于将指定IP地址终端的任意端口映射到无线路由器的WAN口上，所有连接此端口进入无线路由器的数据将转发给指定IP地址的终端。这在搭建WEB服务器、数据库
DDNS：简单解释为可以设置一个域名绑定在此无线路由器的公网IP地址上，将域名解析到本地无线路由器上。 访客网络：进行访客网络的相关设置。
IP与MAC绑定：重要的功能之一，将终端的MAC地址和与路由器连接的IP地址进行绑定，是一种控制接入网络终端授权的方式。 AP隔离：控制接入点是否隔离。
DMZ主机：将接入网络的终端绕过路由器直接暴露在WAN口连接的网络上，与公网的通信不再需要通过路由器的路由转发功能。
无线设备接入控制：管理接入终端的功能之一，可指定某些设备禁止接入无线路由器网络之中。
前文介绍了无线路由器给用户提供的各项扩展功能，下面简单介绍一下无线路由器自身的各项设置，首先第一项是上网设置，界面如下图所示：
无线路由器提供了三种联网方式的选择
，有宽带拨号上网，固定IP地址和自动获得IP地址。这里的上网设置实际是对无线路由器的WAN口进行设置，宽带拨号上网是代替了传统的在计算机中手动点击宽带连接上
数据包MTU即传输数据包的最大包容量，不同的网络连接方式协议具有不同的最佳值，这里可以让无线路由器根据环境自动选择默认的即可。WAN口的MAC地址通常默认
DHCP服务器是一项重要的功能，简单可以理解为在路由器中设置一个IP地址的范围，成为IP地址池，接入无线网络的终端设备将通过DHCP服务器进行IP地址分配，否则没
地址池的开始地址和结束地址可以自定义，这个范围内的IP地址时动态分配的，其余的IP地址可以根据需要进行与终端的绑定操作。地址池是一个重要的概念，在后续讲到的
无线设置的界面笔者不打算使用这款路由器的界面，大家可以参考下图所示的界面：
这里的SSID号就是无线网络的名称，用户可以自定义的设置一些个性化名字；频段可以设置无线信号传输时使用的信道；模式是指定无线传输的速率和802.11标准版本号。
安全类型中，WEP和WPA-PSK/WPA2-PSK是设置的无线密码加密方式，常见的为WEP和WPA/WPA2方式，用户可以自定义无线网络的密码，在这里提醒大家如果安全需求
WEP加密：全称有线等效加密，于上世纪90年代成为WiFi安全标准，是一种老旧的加密方式，并且由于加密算法的漏洞百出，已经被WiFi设备遗弃。但由于也是WiFi曾经使
RC4(Rivest Cipher) 串流加密技术达到机密性，并使用 CRC-32 验和达到正确性。标准的64比特WEP使用40比特的钥匙接上24比特的初向量(initialization
vector，IV) 成为 RC4 用的钥匙。这里IV的概念比较重要，需要读者重点记忆。钥匙长度不是 WEP
安全性的主要因素，破解较长的钥匙需要拦截较多的封包，但是有某些主动式的攻击可以激发所需的流量。WEP 还有其他的弱点，包括 IV
雷同的可能性和变造的封包，这些用长一点的钥匙根本没有用。
□
WPA加密：全称WiFi访问保护。WPA的出现是取代WEP加密标准，于2003年正式启用。WPA设置最普遍的是WPA-PSK（预共享密钥），使用256位密钥。WPA先期采用
□ WPA2加密：WPA 标准于2006年正式被 WPA2取代。 WPA 和 WPA2 之间最显着的变化之一是强制使用 AES 算法和引入 CCMP
（计数器模式密码块链消息完整码协议）替代 TKIP 。
□ 下面的表格总结了目前的路由器加密配置，安全性由上到下依次降低：
WPA2+AESWPA+AESWPA+TKIP/AES（TKIP作为备用）WPA+TKIPWEP不加密的开放网络
□
使用最新的WPA2加密进行无线网络连接的过程是一种网络的TCP握手过程，这个过程发生在用户使用终端选择WiFi网络输入密码到连接成功这一过程中。握手过程是一个重

□
TCP的三次握手过程，简单可以解释为客户端发送一个SYN包给服务器（无线路由器）作为连接请求，无线路由器收到请求后发送一个返回数据包SYN+ACK，客户端接收到
0x03 测试环境的选择
□ 选择WiFi安全测试环境，也就是选择合适的无线网卡和合适的操作系统、选择制作合适完善的密码字典。
无线网卡的选择依据：驱动程序是选择无线网卡的主要依据。在破解WiFi的过程中，需要操作系统、网络设备无缝合作，操作系统对于无线网
卡的支持程度和兼容性就显得特别重要。在这里，推荐使用Atheros芯片的无线网卡，通常情况下，该芯片的性能和兼容性都很适合做WiFi攻击。同样雷凌芯片的网卡也有很
□
如果需要进行远距离的WiFi攻击，攻击者需要选择使用定向天线的大功率无线网卡。不仅需要考虑其芯片类型，更需要考虑大功率无线网卡的系统兼容性、抓包成功率、目标
操作系统的选择也是依据对无线网卡支持程度进行的。常见的操作系统有windows和Linux。在windows操作系统下，由于无线网卡驱动开发未能够做到如Linux般开源，从
Linux是一款专门为渗透测试和安全审计人员制作的Linux操作系统，集成了大量的渗透测试工具。综合比较之下，选择Kali
Linux操作系统作为破解WiFi是非常适合的：
□
字典也就是破解WPA2加密时需要使用的一类信息资源。字典可以简单解释为密码本或密码的集合文件。WPA2的密码破解是一种暴力破解的过程，使用不同的密码对抓取到
□ 对于WPA2密码的破解使用字典，是一个猜测的过程。提高破解成功率就是使用更合适的密码字典。目前给大家使用字典的建议为以下几点：
□

一：收集目标路由器管理员的信息，使用多种元素（例如手机号码、姓名缩写、门牌号码、英语名字、生日等）组合，自行制作密码破解的字典。这里制作字典的工具，不管
Linux也给我们提供了例如crunch这样的字典制作工具，大家多尝试，根据自己的使用需求可灵活选择。
□
二：下载密码字典。网络上提供了大量不同元素组合的字典，有的针对国内用户习惯有的针对国外用户习惯。大家可深入搜索寻找一些，慢慢积累成为自己的字典数据库，在
□
三：寻找外包破解团队。在搜索引擎中搜索"破解无线握手包"、"破解WiFi密码"等关键词，可以寻找到很多提供相关服务的商家。这个过程省去了用户自己进行大量高成本破

□ 网思科平-Sumia
□ Onescorpion

点击收藏 | 0 关注 | 1
上一篇：Php一句话后门过狗姿势万千之传输... 下一篇：黑产揭秘："打码平台"那点事儿

1. 2 条回复


笑然 2016-11-28 10:29:21

赞，这个连载系列不错，期待后续

0 回复Ta


hades 2016-11-28 12:32:44

让连载来的更猛烈些把

0 回复Ta

登录 后跟帖

先知社区

现在登录

热门节点

技术文章

社区小黑板

目录

RSS 关于社区 友情链接 社区小黑板