【连载】WiFi安全技术 四:突破防护机制

ms0x0 / 2017-01-12 07:37:39 / 浏览数 3368 安全技术 漏洞分析 顶(0) 踩(0)

______wifi____wifi

1. 无线路由器MAC地址过滤

2. 隐藏无线网络SSID

面对上述两种较为常见的防护机制,利用无线安全工具和一定的技巧即可破解绕过,这两种防护机制比较初级,在此我们依然利用Kali操作系统内置的工具进行破解。 1.突破MAC地址过滤

首先简单介绍一下什么是MAC地址。MAC地址是网络设备的唯一网络地址标示,本意为媒体访问控制,可以理解为网络设备的物理地址,对于每台网络设备,MAC地址MAC地址过滤防护机制,即通过预先在无线路由器内设定允许或者禁止访问本地网络的设备MAC地址列表,以白名单/黑名单的方式来控制网络设备的接入权限。这项安无线路由器设置界面中常见的MAC地址过滤设置界面如下图所示:

上图中的"允许"和"禁止"就相当于白名单/黑名单的过滤机制。如果本地网络的网络终端比较固定,最好采用"允许"即白名单的方式,固定化终端MAC地址,也就是本地网MAC地址过滤的突破方法可以参考下图(图片来自网络):

主要的突破思路,就是通过修改本地的网络设备MAC地址,绕过目标路由器的过滤名单达到突破的目的。前文我们讲到,MAC地址虽然理论上唯一,但可以通过软件修成。

- •探测合法无线客户端的MAC地址,可以使用airodump-ng工具实现
- •修改攻击网卡的MAC地址,这个步骤可以在Windows或Linux中进行
- •重新装载网卡设备,并检查是否已经更改成功
- •连接无线接入点,完成突破防护的目的

在此提示大家,伪造完MAC地址后,接入目标网络,虽然突破的目标MAC地址过滤的限制,但可能由于同时有两个相同的MAC地址客户端,很容易出现数据包丢失、传首先打开Kali系统,打开一个终端,查看一下目前攻击环境的网络配置情况,使用ifconfig –a命令,如下图:

此处可以将我们使用的无线网卡MAC地址做一个记录,作为后续操作过程中的对比依据。按照之前的文章中介绍的,还需要将网卡激活至监听状态,如下图所示:

激活监听状态后,使用airodump-ng wlan0mon命令对周围信号进行探测:

此时,下方界面中的STATION,也就是已连接目标无线路由器的终端MAC地址,就是在启用MAC地址过滤时的"合法客户端",这时探测到这个终端的MAC地址后,将其下一步就是突破MAC地址过滤的重点了,在Kali中,将我们所使用的无线网卡的MAC地址修改为刚才抓取到的合法客户端的MAC地址。目前无线网卡还在监听模式,首stop wlan0mon:

使用ifconfig -a命令检查一下:

修改无线网卡的MAC地址,在Kali中可以使用命令:

ifconfig wlan0 hw ether XX:XX:XX:XX:XX (需要修改的合法客户端MAC地址)

此时可能会提示设备或资源忙:

原因是由于此时无线网卡虽然不处于监听状态,但还在工作状态,这种情况下需要对无线网卡进行一次"卸载"操作,使用命令ifconfig wlan0 down,再使用ifconfig –a命令,仍然可以看到wlan0无线网卡,但其已经不再处于工作状态。这时我们再运行一次ifconfig wlan0 hw ether XX:XX:XX:XX:XX:XX:XX:XX:XX:

对比一下前面的截图,wlan0无线网卡的MAC地址已经从尾号C9:C4修改为84:99的新MAC地址。说明我们修改成功了,此时的无线网卡对目标无线路由器来说,已经 后续的攻击操作,使用ifconfig –a wlan0 up加载无线网卡、使用airmon-ng start

wlan0将无线网卡激活至监听状态,按照前文的无线破解操作进行连接即可,特别提醒,最好在探测到目标同MAC地址客户端不在线的时候进行攻击破解操作,在这里不在Kali中还可以使用另一个工具修改网卡MAC地址,使用命令macchanger—m XX:XX:XX:XX:XX:XX

wlan0,这里wlan0也是在不工作非监听状态,和上一种方法所述一致。如果大家在修改网卡MAC地址后重新加载至监听模式后,MAC地址又恢复了原本的MAC地址,并在Windows操作系统中也有修改网卡MAC地址的工具,这里给大家简单介绍一款名叫SMAC的工具,如下图:

这个工具的操作很简单,在选中目标网卡,输入需要修改的MAC地址后,点击修改即可。在这里特别提醒,如果大家使用VMware虚拟机的Windows并且使用了桥接 2.隐藏无线网络SSID

在无线路由器的设置中,如果目标使用了隐藏SSID选项,那么正常情况下,打开手机、平板的无线网络,是搜索不到目标的网络名称的,如下图所示:

这种情况下只有知道了网络SSID名称和密码并且手动添加输入才能够连接。但是要特别强调,关闭SSID广播功能仅仅是关闭了无线路由器广播信标帧中的SSID部分,并对于这种隐藏了SSID的无线网络,在这里给大家介绍几种方式去获取SSID的名称。首先第一种使用airodump-ng和aireplay-ng进行DeAuth攻击获取SSID,这和前文

图中标出的部分,就是本应显示SSID的无线网络,这里显示了一个长度为0的标示,也就是说目标无线网络的SSID是隐藏的,没有开启SSID广播功能,请注意,虽然SS 新建一个终端窗口,使用aireplay-ng工具对已连接目标无线网络的无线客户端进行DeAuth攻击,反复多尝试几次,如下图:

攻击过程中,注意观察之前打开的airodump-ng工具的终端窗口,攻击成功后,原先的监控窗口中能够自动显示出原先未显示出来的SSID名称,如下图:

还可以通过一种被动探测的方式进行SSID获取,比较流行的一种工具就是kismet,这款工具也在Kali中集成了。被动探测相对于主动探测,隐蔽性更好,而且探测通信 打开终端,输入kismet,运行,点击OK等,在启动过程中,需要启用kismet服务:

点击start后,进入Kismet,提示no sources时选择yes加入一个接口,在intf栏中填写wlan0mon,也就是监听状态的无线网卡名称,点击add,即可开始探测过程,

被动探测的速度是相对比较慢的,需要花更多的时间去等待探测结果,等待的时间足够长,kismet能够帮忙探测到隐藏SSID的信号:

<hidden

SSID > 就是设置了隐藏SSID的无线网络信号,相对于主动发起DeAuth攻击不同,kismet提供了一种静默等待客户端连接目标无线网络时抓取SSID的能力,所以耐心是使

在Kali中,还可以使用wireshark和tcpdump等工具进行SSID的抓取,使用tcpdump的命令为tcpdump –n –e –vvv –i wlan0mon,运行效果如下:

这个过程中根据所处环境信号的数量,会显示大量的无线网络信号的信息,对于隐藏的SSID,需要在其中仔细寻找。对于针对特定目标网络的SSID,并不推荐这种方

这种方法和使用tcpdump类似,采取盲抓的方式,适用于目标环境中无线信号较少的情况。使用这两款工具给大家提供了其他的获取思路,如果讨论实用性,获取特点击收藏 | 0 关注 | 0

上一篇:阿里巴巴直播防控中的实人认证技术下一篇:阿里巴巴直播内容风险防控中的AI力量

1. 1条回复



helloworld 2017-01-12 12:48:24

学习

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