登录

【连载】WiFi安全技术　三：WiFi密码的破解

ms0x0 / 2016-12-12 07:37:54 / 浏览数 5551 安全技术 漏洞分析 顶(0) 踩(0)

■■■■■■■■■■■■■■■■■■■■4■■■Wifi■■■■■■■■■■■■WEP■■■WPA2-PSK■■■■■WPS■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■Kali Lin
■■■■■■■■■■■Kali Linux■■■■■■■■■■■■■■■■■■Wifi■■■Kali Linux■■■■W

■■Kali■■“■■■”■■■■■“■■■■■■■”■■■■■■■■Kali■■■■■■■■■■■Kali■■■■■■■■■
■■■■■■■Kali■■■■■■■■■■■■■■■■■■■■■■■■■■apt-get update■apt-get upgrade■■■■■■■
■■■■■■■■Wifi■■■■■■■■■■■■■Kali■■■

■■wlan0■■■■■■■■■■■■eth0■■■■■■■■■VMware■■■■lo■■■■■■■■■127.0.0.1■■■■■■■■■■■■■■■■■■■■■■■■

这里ifconfig wlan0 up
就是确认激活无线网卡为可用状态，此时没有异常提示的情况下，无线网卡就正式启动了。如果有疑虑，还可以使用专门查看无线网卡状态的命令iwconfig进行查看，如下图

■■■

■■■■■airmon-ng start wlan0■■■■Aircrack-ng■■■■■■■■■■WiFi■■■

■■■iwconfig■■■■■■■■■■■■■■■■■■:

■■■■■■■■wlan0■■wlan0mon■■■■■■■■■■■■■■■■■■■■■■■■■■■Kali Linux 1.x■■■■■■■■■■■■■■■■mon0■2.0■■■■■■wlan0mon■■■■■

1.WEP密码破解
前面的连载文章中我们已经介绍过WEP加密，WEP是一种比较老的加密方式，现在已经被淘汰。作为技术讲解，还是觉得有必要加入进来。这里我们使用两种工具进行演示
Linux系统下，一种是大名鼎鼎的Aircrack-ng工具套件，另一种是Fern WIFI
Cracker。首先我们使用Aircrack-ng讲解一下破解过程。这里笔者预置了一个SSID为target的无线路由器，采用WEP加密方式。
破解过程的第一步，就是需要搜索无线网卡能够接收探测到的周围无线网络信号，这里使用Aircrack-ng套件中的airodump-ng工具，命令如下图：

■■■■■airodump-ng wlan0mon■■

■■■■■■■■■■■■■■

BSSID：无线路由器的MAC地址
PWR：无线路由器的信号强度（负值的绝对值越低信号越强，绝对值50以上的信号就一般了，70以上的信号算是比较差的）
CH：无线路由器工作信道
MB：无线路由器速率
ENC：加密方式
ESSID：无线网络的名称，也就是打开终端搜索到的无线网络名
STATION：连接某无线路由器的一个客户端，例如笔记本电脑、手机等
这里我们将这个终端放在这里不要关闭，重新打开一个新的终端，输入使用新的命令，如下图：

airodump-ng –ivs –w wep –c 1 wlan0mon■■■■■--ivs■■■WEP■■■■■■■■WEP■■■iv■■■■■■■■■■■■-c 1■■■■■■■■■■■■1■■■■■■■■■■■■■■

■■WEP■■■■■■■■■■■■■iv■■■■WEP■■■■■■■■■■■■iv■■■■■■■■■■■■■■■■■■■■■WEP■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■

这里aireplay-ng是套件中的一个工具，参数设置为-3，是设置做ARP
REQUEST攻击，-b后面设置无线路由器的MAC地址，-h后面设置当前与目标无线路由器连接的一个终端的MAC地址（破解WEP需要有个合法终端已经连接在目标无线路由

■■■■■■■■■■■■■■■5■■■■■■■■■■■1■■■■■■■■■■■■■■■ARP REQUEST■■■

■■■iv■■■■■■■■■■■■■■■■■■■■■■iv■■■■■■■■■■■■■iv■■■■■■■■■■/home■■■

■■■■■■■■iv■■■■■■■■■■

■■■■■■■■aircrack-ng wep-01.ivs■■■■■■aircrack-ng■■■■■■■■■ivs■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■target■■■■■■
■■■■3■■■■■■■■■■■■■■■■■

■■■■■■■■■■■■■■■WEP■■1234567890123■■■■■■■■■■■■■■■■■■100%■WEP■■■■■■■■■■■■■■
■■■■■■Fern WIFI Cracker■■■■■■■■■■■■

■■■■■■■■■wlan0■■■■■■■■■■■■refresh■■■■■■■■■■■■“Scan for access point”■■■■■■■■■■■■■■■■■■■WEP■■■WiFi■■■■■■■■■■

■■■■■■■WiFi■■■■■■■■■■■■Attack■■■■■■■■■■■■■■■■■ivs■■■■■■ARP REQUEST■■■■■■■■■■■■■■■■■■■■■■■■■■■■■

WiFi密码的数据包抓取，受限于无线路由器和无线网卡的质量、距离、障碍、信号强度等多种因素，所以破解未必能一次成功，破解需要足够的耐心、更好的信号质量。WE
2.WPA2-PSK密码破解

首先简单讲解一下WPA/WPA2和WPA-PSK/WPA2-PSK的区别。

WPA/WPA2是一种比WEP强壮的加密算法，挑选这种安全类型时路由器将选用Radius服务器进行身份认证并得到密钥。因为要架起一台专用的认证服务器，成本相对较高并

WPA-PSK/WPA2-PSK安全类型其实是WPA/WPA2的一种简化版别，它是依据同享密钥的WPA形式，安全性很高，设置也对比简单，合适普通家庭用户和小型企业运用，[illegible]

认证类型：

该项用来选择体系选用的安全形式，即自动、WPA-PSK、WPA2-PSK。若挑选自动选项，路由器会依据主机请求自动挑选WPA-PSK或WPA2-PSK安全形式。

加密算法：

该项用来挑选对无线数据进行加密的安全算法，选项有自动、TKIP、AES。默许选项为自动，选择该项后，路由器将自动挑选TKIP或AES加密办法。这里需要注意802.11n版

PSK密码： 该项就是WPA-PSK/WPA2-PSK的初始密钥了，在设置时，需求为8-63个ASCII字符或8-64个十六进制字符，这里也可以理解为设置的无线网密码。

组密钥更新周期：该项设置播送和组播密钥的定时更新周期。

下面的路由器设置界面截图，大家可以清晰的看到相关选项：

[illegible]WPA2-PSK[illegible]Aircrack-ng[illegible]windows[illegible]EWSA[illegible]

[illegible]WEP[illegible]Kali Linux[illegible]airodump-ng

[illegible]SSID[illegible]target[illegible]WPA2-PSK[illegible]11[illegible]MAC[illegible]F8:06[illegible]-40[illegible]11

```
airodump-ng –c 11 –w wpa2 wlan0mon
```

[illegible]-c 11[illegible]11[illegible]-w wp2[illegible]wpa2[illegible]WEP[illegible]WPA2[illegible]“[illegible]”[illegible]

[illegible]MAC[illegible]F8:06[illegible]STATION[illegible]

[illegible]WEP[illegible]WPA2-PSK[illegible]

[illegible]

[illegible]“[illegible]“[illegible]DeAuth[illegible]Aircrack-ng[illegible]aireplay-ng[illegible]WEP[illegible]

[illegible]aireplay-ng –0 5 –a APMAC –c clientMAC wlan0mon[illegible]-0[illegible]DeAuth[illegible]5[illegible]

[illegible]

上图中展示了在发起攻击时可能出现的提示，这和破解WEP时一样，可能由于信道未同步的问题造成攻击失效，在此，攻击命令也是需要多次执行多次尝试，待到工作信道[illegible]

[illegible]5[illegible]DeAuth[illegible]“[illegible]“[illegible]

[illegible]WPA handshake[illegible]SSID[illegible]

[illegible]wpa2-01.cap[illegible]Kismet[illegible]kismet[illegible]

```
aircrack-ng –w dic wpa2-01.cap
```

[illegible]dic[illegible]WEP[illegible]

[illegible].cap[illegible] [illegible]CPU[illegible]GPU[illegible]GPU[illegible]

[illegible]

GPU[illegible]SLI[illegible]

[illegible]

3.利用WPS功能破解

首先提示：为了安全考虑，实际使用中请在无线路由器配置中关闭WPS功能！！

利用WPS功能破解无线路由器也就是人们常说的跑PIN码破解。WPS（Wi-Fi Protected Setup）是Wi-Fi保护设置的英文缩写。WPS是由Wi-Fi联盟组织实施的认证项目，主要致力于简化无线局域网安装及安全性能的配置工作。WPS并不是一项新增的安全性能

WPS提供了一个相当简便的加密方法。通过该功能，不仅可将都具有WPS功能的Wi-Fi设备和无线路由器进行快速互联，还会随机产生一个八位数字的字符串作为个人识别号

WPS[illegible]WPS[illegible]WPS[illegible]PIN[illegible]

PIN[illegible]8[illegible]WPS[illegible]PIN[illegible]WPS PIN[illegible]8[illegible]checksum[illegible]

[illegible]PIN[illegible]([illegible])[illegible]PIN[illegible]([illegible]4[illegible])[illegible]([illegible]3[illegible])[illegible]PIN[illegible]EAP-NACK[illegible]

[illegible]Kali Linux[illegible]reaver[illegible]wifite[illegible]PIN[illegible]airc

[illegible]CH[illegible]3[illegible]reaver[illegible]

[illegible]PIN[illegible]

[illegible]-i[illegible]MAC[illegible]-b[illegible]MAC[illegible]-a[illegible]-S[illegible]DH keys[illegible]-vv[illegible]-c[illegible]

[illegible]PIN[illegible]PIN[illegible]1[illegible]2[illegible]PIN[illegible]WPS[illegible]PIN[illegible]PIN[illegible]

[illegible]PIN[illegible]PIN[illegible]

[illegible]wifite[illegible]Kali Linux[illegible]

[illegible]WEP[illegible]WPA/WPA2[illegible]PIN[illegible]WEP[illegible]WPA/WPA2-PSK[illegible]aircrack-ng[illegible]W

[illegible]

[illegible]WPS[illegible]WPS[illegible]PIN[illegible]wifite[illegible]WPS[illegible]wifi

[illegible]

[redacted]PIN[redacted]WPA2-PSK[redacted]WEP[redacted]

4.本地破解历史连接记录
这一节简单介绍在windows系统下，利用软件读取本地存储的已连接WiFi密码的方法。我们使用到的工具是一款名叫WiFipasswordDecryptor的工具，使用方法非常简单：

[redacted]Start Recovery[redacted]

[redacted]
WiFi[redacted]WiFi[redacted]

点击收藏 | 0 关注 | 0
上一篇：CSP Level 3浅析&amp... 下一篇：如何破解Syscan360会议胸牌
1. 1 条回复


笑然 2016-12-13 02:01:26

这篇连载越来越深入啦，后面几张图片要补充下

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