Aireplay-ng 1.2 rc4 - (C) 2006-2015 Thomas d'Otreppe

http://www.aircrack-ng.org

格式: aireplay-ng <options> <replay interface>

Filter options:

-b bssid : 地址，接入点

-d dmac : 地址，目的地

-s smac : 地址，源代码

-m len : 最小数据包长度

-n len : 最大包长度

-u type :帧控制，类型字段

-v subt :帧控制，亚型场

-t tods : 帧控制，到 DS bit

-f fromds : 帧控制，从 DS bit

-w iswep : 控制框架，wep bit

-D :禁用ap检测

回放选项:

-x nbpps :每秒数据包数

-p fctrl : 设置帧控制字（十六进制）

-a bssid : 设置访问点的地址

-c dmac : 设置目的地的地址

-h smac : 设置源地址

-g value : 变更环缓冲区大小（默认值：8）

-F : 选择第一个匹配数据包

fakeauth攻击选项：:

-e essid : 设定目标AP的SSID

-o npckts :每突发的数据包数（0 =自动，默认值：1）

-q sec :之间的连接保持秒

-Q :发送关联请求

-y prga : 共享密钥认证密钥

-T n : 退出后重试假认证请求N次

ARP欺骗攻击的选项:

-j : 注入FromDS:包

碎片攻击选项：

-k IP : 在设置目的IP碎片

-l IP : 设置碎片中的源代码

试验选择攻击:

-B : 激活码率测试

源选择:

-i iface : 从这个接口捕获数据包

-r file : 从这个PCAP文件提取数据包

其他选项:

-R : 禁用/ dev / RTC用法

--ignore-negative-one : 如果界面的通道不能被确定，忽略不匹配，未打补丁的cfg80211需要

攻击模式（数字仍然可以使用）:

--deauth count : deauthenticate 1或全部站（0）

--fakeauth delay : fake authentication with AP (-1)

--interactive : 交互式帧选择（- 2）

--arpreplay : 标准的ARP请求回放（3）

--chopchop : 解密/ chopchop WEP数据包（4）

--fragment :生成有效的密钥（5）

--caffe-latte : 查询一个新IVS客户端（6）

--cfrag : 对客户的碎片（- 7）

--migmode : 攻击WPA迁移模式（8）

--test :测试注射和质量（- 9）

--help :显示此使用屏幕