Airbase-ng 1.2 rc4 - (C) 2008-2015 Thomas d'Otreppe

Original work: Martin Beck

http://www.aircrack-ng.org

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

参数:

-a bssid : 设置访问点的地址

-i iface : 从这个接口捕获数据包

-w WEP key : 使用WEP密钥EN /解密数据包

-h MAC :对于中间人模式源MAC

-f disallow : 允许指定客户端MAC地址（默认允许）

-W 0|1 : [不要]在0 |信标1套WEP旗（默认：自动）

-q : 安静（不打印统计）

-v : 冗长（打印更多的信息）

-A : 特设模式（允许其他客户同行）

-Y in|out|both : 外部包处理

-c channel : 设置正在运行的信道的信道

-X : 隐藏essid

-s :强制共享密钥身份验证（默认：自动）

-S : 设置共享密钥长度（默认值：128）

-L : 拿铁WEP攻击（如果司机不能把碎片）

-N : cfrag WEP攻击（推荐）

-x nbpps : 每秒数据包数（默认值：100）

-y :禁用广播探头的响应

-0 : 设置所有WPA，WEP，打开的标签。不能使用- Z和Z

-z type : 继承 WPA1 标签. 1=WEP40 2=TKIP 3=WRAP 4=CCMP 5=WEP104

-Z type : 同为Z，但对于WPA2

-V type : fake EAPOL 1=MD5 2=SHA1 3=auto

-F prefix : 写所有发送和接收的帧到pcap文件

-P :应对所有探头，即使指定ESSIDs

-I interval : 在毫秒内设置信标间隔值

-C seconds :使信标探测ESSID值（需要- P）

-n hex : 用户指定的ANonce做的四次握手时

滤波器的选择:

--bssid MAC : 设置bssidfilter/use

--bssids file :读取该文件的列表bssids

--client MAC : 客户端过滤的麦克

--clients file : 读取该文件的MAC地址清单

--essid ESSID :指定一个单一的网络名称（默认：默认）

--essids file : 读取该文件的列表ESSIDs

--help : 显示此使用屏幕