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

http://www.aircrack-ng.org

格式: aircrack-ng [options] <.cap / .ivs file(s)>

常见的选择：:

-a <amode> :洪水攻击模式（1 / 2 / WEP，WPA-PSK）

-e <essid> : 目标选择：网络标识符

-b <bssid> : 目标选择：接入点的mac

-p <nbcpu> : CPU使用（默认：所有的CPU）

-q : 启用安静模式 (无输出状态)

-C <macs> : 合并到一个虚拟的一个给定的APS

-l <file> : 写文件的关键

静态WEP破解选项：:

-c : 仅搜索字母数字字符

-t : 搜索二进制编码的十进制CHR只有

-h : search the numeric key for Fritz!BOX

-d <mask> : 使用掩蔽键(A1:XX:CF:YY)

-m <maddr> :用于过滤可用数据包的地址

-n <nbits> : WEP密钥长度 : 64/128/152/256/512

-i <index> : WEP密钥索引（1至4），默认值：任何

-f <fudge> : 强力的修正因子，默认值：2

-k <korek> : 禁用一个攻击方法（1至17）

-x or -x0 : 最后keybytes禁用暴力破解

-x1 : 最后keybyte bruteforcing（默认）

-x2 :使过去的2 keybytes bruteforcing

-X : 禁用强力多线程

-y :实验单强力模式

-K : 只使用旧Korek攻击（预PTW）

-s : 在ASCII码的关键而开裂

-M <num> : 指定要使用的IV型坦克的最大数量

-D : WEP decloak, skips broken keystreams

-P <num> : PTW的调试：1：禁用克莱因，2：PTW

-1 : 只有1尝试破解密钥与PTW

破解WEP和WPA-PSK选项：

-W <词>：路径表（S）的文件名（S）

WPA-PSK 选项:

-E <file> : 创建项目文件ewsa V3

-J <file> : 创建Hashcat捕获文件

-S : WPA破解速度测试

-r <DB> : 对airolib ng数据库路径

(Cannot be used with -w)

其他选项:

-u : 显示CPU和# MMX/SSE支持

--help :显示此使用屏幕