## 无线宝 bt5 来破解 wpa wpa2 加密

此教程为使用 <u>无线宝</u>bt5 来破解wpa加密、wpa2 加密,请勿使用在非法途径,其主要目的供测试您自己家无线路由是否安全。请自行参考内部教程打开bt5 程序。

- 1、系统启动啦,这就是桌面! 咋样? 熟悉吧? 很像win的! 很容易上手
- 2、然后打开第二排的第一个软件minidwep-gtk~~出现此对话框,直接点ok!就过去了

| 📄 minidwep-gt          | k-20522          |          |        |      |      |        |    |             |
|------------------------|------------------|----------|--------|------|------|--------|----|-------------|
| 无线网卡                   | 路由MAC            | 名称       | 强度     | 信道   | 加密方式 | 客户端MAC | :  |             |
| wlan0 🔻                | D8:5D:4C:2C:7    | D:32_FAS | T_2C7D | 32   | 484  | WPA2WP | A  | <u>S</u> 扫描 |
| wlan0 RTL8187<br>r8187 |                  |          |        |      |      |        |    |             |
| 信道                     |                  |          |        |      |      |        |    |             |
| All                    |                  |          |        |      |      |        |    |             |
| 加密方式                   |                  |          |        |      |      |        |    |             |
| WPA/WPA2 🔻             |                  |          |        |      |      |        |    | D跑字典        |
| 古武体权                   |                  |          |        |      |      |        | 24 |             |
| 1110551+               | 15:42:10>等待;     | 命令中      |        |      |      |        |    | L启动         |
| Aireplay-ng -2         |                  |          |        |      |      |        |    |             |
| Aireplay-ng -3         |                  |          |        |      |      |        |    | A停止         |
| Aireplay-ng -4         |                  |          |        |      |      |        |    |             |
| Aireplay-ng -6         |                  |          |        |      |      |        |    |             |
| Aireplay-ng -7         |                  |          |        |      |      |        |    |             |
| 注入速率                   |                  |          |        |      |      |        |    |             |
| 500                    |                  |          |        |      |      |        |    | E退出         |
| http://421860256.gz    | L∰<br>an≣idqicom |          | IVS    | 数量:( | 0    |        | 1  |             |

3、看左上角那个下拉菜单,找到自己的网卡!!! 然后右上角!! 扫描!!! 然后就开始激动人心了!~

| And a start of the  | 路由MAC   | 名  | 称强  | 度信   | 道加                         | 密方                                     | 式                           | 客户  | 端MAC                                    |           |                                     |                           |   |
|---|---|--|---|--|----------------------------|--|-----------------------------|---|---|-----------|-------------------------------------|---------------------------|---|
| vlan0 🔻   | Scanning  |  |   |  |                            |  |                             |   |   |           |                                     | <u>S</u> 扫描               |   |
| lan0 RTL8187<br>3187  |   |  |   |  |                            |  |                             |   |   |           |                                     |                           | , |
| 信道  |   |  |   |  |                            | _                                      |                             | _   |   |           |                                     |                           |   |
| All III   | airodump-ng   |  |   |  |                            |  |                             |   |   |           |                                     |                           | - |
| 加密方式  | CH 3 1[ Elapsed:  | 8 s 1[   | 2010-09-1   | 0 14:37  |                            |  |                             |   |   |           |                                     |                           |   |
| 2244 1.222 7 3 24 9   | out o 11 cropoent   | JL   |   |  |                            |  |                             |   |   |           |                                     |                           |   |
| NED   | 12121212121   | 122623   | 22  | A 22/51/2  | 1000                       | 1201                                   | 100                         | 0110120                                       | 22220000                                | 722322007 | 2012/02/02/07                       |                           |   |
| WEP   | BSSID   | PUR  | Beacons   | #Data,   | #/s                        | CH                                     | MB                          | ENC   | CIPHER                                  | AUTH      | ESSID                               |                           |   |
| WEP   | BSSID<br>94:0C:6D:14:5A:F0  | PWR<br>32  | Beacons<br>2  | #Data,<br>0  | #/s<br>0                   | CH<br>6                                | MB<br>54                    | ENC   | CIPHER                                  | AUTH      | ESSID<br>FAST_1                     | 45AF0                     |   |
| WEP<br>方式选择——   | BSSID<br>94:0C:6D:14:5A:F0<br>00:27:19:7D:36:10   | PWR<br>32<br>82  | Beacons<br>2<br>12  | *Data,<br>0<br>28  | */s                        | CH<br>6<br>11                          | MB<br>54<br>54              | ENC<br>OPN                                    | CIPHER                                  | auth      | ESSID<br>FAST_1<br>FAST_7           | 45AF0<br>103610           |   |
| WEP<br>方式选择——<br>┛ Aireplay-r   | BSSID<br>94:0C:6D:14:5A:F0<br>00:27:19:7D:36:10<br>94:0C:6D:63:1A:6C  | PWR<br>32<br>82<br>50  | Beacons<br>2<br>12<br>5   | *Data,<br>0<br>28<br>0   | */s<br>0<br>0              | CH<br>6<br>11<br>5                     | MB<br>54<br>54<br>54        | ENC<br>OPN<br>OPN                             | CIPHER                                  | auth      | ESSID<br>FAST_1<br>FAST_7<br>FAST_6 | 45AF0<br>103610<br>131A6C |   |
| WEP<br>方式选择——<br>2 Aireplay-r<br>2 Aireplay-r                                 | BSSID<br>94:0C:6D:14:5A:F0<br>00:27:19:7D:36:10<br>94:0C:6D:63:1A:6C<br>BSSID   | PWR<br>32<br>82<br>50<br>STATI                                     | Beacons<br>2<br>12<br>5<br>ON   | *Data,<br>0<br>28<br>0<br>PWR                                      | #/s<br>0<br>0<br>Rat       | CH<br>6<br>11<br>5<br>te               | MB<br>54<br>54<br>54<br>Lo: | ENC<br>. OPN<br>. OPN<br>. OPN<br>st Pa       | CIPHER                                  | AUTH      | ESSID<br>FAST_1<br>FAST_7<br>FAST_6 | 45afo<br>103610<br>31A6C  |   |
| WEP<br>方式选择——<br>Aireplay-r<br>Aireplay-r<br>Aireplay-r                       | BSSID<br>94:0C:6D:14:5A:F0<br>00:27:19:7D:36:10<br>94:0C:6D:63:1A:6C<br>BSSID<br>00:27:19:7D:36:10  | PWR<br>32<br>82<br>50<br>STATI<br>00:21                            | Beacons<br>12<br>5<br>ON<br>:00:CF:C0:  | *Data,<br>0<br>28<br>0<br>PWR<br>84 -1                             | #/s<br>0<br>0<br>Rat       | CH<br>6<br>11<br>5<br>te<br>- 0        | MB<br>54<br>54<br>54<br>Lo: | ENC<br>OPN<br>OPN<br>OPN<br>st Pa             | CIPHER<br>ackets<br>2                   | AUTH      | ESSID<br>FAST_1<br>FAST_7<br>FAST_6 | 45AF0<br>13610<br>31A6C   |   |
| NEP<br>方式选择——<br>Aireplay-r<br>Aireplay-r<br>Aireplay-r                       | BSSID<br>94:0C:6D:14:5A:F0<br>00:27:19:7D:36:10<br>94:0C:6D:63:1A:6C<br>BSSID<br>00:27:19:7D:36:10<br>00:27:19:7D:36:10   | PWR<br>32<br>82<br>50<br>STATI<br>00:21<br>00:27                   | Beacons<br>2<br>12<br>5<br>0N<br>:00:CF:C0:<br>:19:AC:3A:                             | *Data,<br>0<br>28<br>0<br>PWR<br>84 -1<br>65 100                   | */s<br>0<br>0<br>Rat<br>54 | CH<br>6<br>11<br>5<br>te<br>- 0<br>-18 | MB<br>54<br>54<br>54<br>Lo: | ENC<br>OPN<br>OPN<br>OPN<br>st Pi<br>0<br>3   | CIPHER<br>ackets<br>2<br>25             | AUTH      | ESSID<br>FAST_1<br>FAST_7<br>FAST_6 | 45AF0<br>103610<br>31A6C  |   |
| WEP<br>方式选择——<br>? Aireplay-r<br>? Aireplay-r<br>? Aireplay-r<br>? Aireplay-r | BSSID<br>94:0C:6D:14:5A:F0<br>00:27:19:7D:36:10<br>94:0C:6D:63:1A:6C<br>BSSID<br>00:27:19:7D:36:10<br>00:27:19:7D:36:10<br>00:27:19:7D:36:10<br>00:27:19:7D:36:10 | PWR<br>32<br>82<br>50<br>STATI<br>00:21<br>00:27<br>00:25<br>00:25 | Beacons<br>2<br>12<br>5<br>0N<br>:00:CF:C0:<br>:19:AC:34:<br>:56:81:BD:<br>:59:29:46: | •Data,<br>0<br>28<br>0<br>PWR<br>84 -1<br>65 100<br>55 41<br>20 55 | */s<br>0<br>0<br>Rat<br>54 | CH<br>6<br>11<br>5<br>te<br>-18<br>-18 | MB<br>54<br>54<br>54<br>Lo: | ENC<br>OPN<br>OPN<br>OPN<br>St Pi<br>36<br>36 | CIPHER<br>ackets<br>25<br>38<br>2<br>25 | Probes    | ESSID<br>FAST_1<br>FAST_7<br>FAST_6 | 45AF0<br>13610<br>31A6C   |   |

4、够激动吧?看到没有?

sssid--- 就是扫描到无线接入点的mac地址 pwr: 信号强度 data: 这句是所谓的数据包 最后面的 essid就知道了吧?那就是你扫描到的路由名称! 这样就明白了吧? 当然了,如果没有数据包 的话,你还是省省吧! 毕竟是破解! 没有数据包代表抓不 到握手包,抓不到握手包怎样破解 呢? 所以还是需要数据量的! 然后抓到握手包以后就开始破解啦!



5、怎么样?嘿嘿,看到了吧?软件已经搜索到了wpa2加密的方式的路由器!当然了,软件的搜索方式是一起搜索,也就是wep,wpa2一起搜索,看看软件左边栏的"加密方式"你选择wep就会显示wep方式加密的路由,你选择wpa2就会显示wpa2方式加密的路由,咱们这儿讲的是破解wpa2加密方式的路由!所以wep一笔带过!如果是破解wep的路由,直接右边栏的"启动"按钮,剩下的几乎不用动手自动搜索密码(前提是有数据包哦!)

|       | airodump     | o-ng               |       |                      |                  |        |       |         | -       |      | X |
|-------|--------------|--------------------|-------|----------------------|------------------|--------|-------|---------|---------|------|---|
| A     | CH 4 ][ E1a  | apsed: 20 :        | s][2  | 010-09-10            | 15:46            |        |       |         |         |      |   |
| n     | BSSID        | PW                 | r RXQ | Beacons              | #Data,           | , #/s  | CH MB | ENC     | CIPHER  | auth | E |
| 쇍     | D8:5D:4C:2C: | :7D:32 49          | 9 100 | 196                  | 21               | 0      | 4 54  | . WPA2  | CCMP    | PSK  | F |
|       | BSSID        | ST                 | ATION |                      | PWR F            | Rate   | Lost  | Packets | s Probe | es   | 1 |
| R     | D8:5D:4C:2C: | :7D:32 00:         | 21:00 | :CF:C0:84            | 23               | 0 - 1  | 0     | 3       | 30      |      | 1 |
| 信察の「  |              |                    |       |                      |                  |        |       |         |         |      |   |
| anlar | 15:4         | 6:20>等待            | 寺40秒  | 以便获得i                | 人证握手             | 包!     |       |         |         |      |   |
| sbj97 | /-ng 3 15:4  | 6:17>启西<br>6:17>抓到 | 则一个   | athenticati<br>客户端MA | ion<br>C: 00:21: | 00:CF: | C0:84 |         | 👰 连接    | 到网络  | 络 |

6、接下来开始抓取握手包,看图片最后面一行字,抓到一个握手包,正在等待认证,等待认证后就会给你提示!告诉你已经抓到一个握手包,然后就可以破解啦!(当然,抓取握手包是需要耐心的,有时候rp暴增,没准上来就能抓到,我这儿抓了十几分钟才抓到)

| ۲ | Yes |
|---|-----|
| 0 | No  |
|   |     |
|   |     |

7、基本上已经成功,剩下的就是破解啦!这里开始进入破解第一部,跑包,开始测试密码!



8、接下来,把你的字典贡献给minidwep-gtk! 嘿嘿,这个都会了吧?我给他一个默认的字 典,就是最后一个wordlist.txt。你可以根据情况来选择字典,其实我上藏了 3g多的字典呢! 嘿 嘿,不过这个路由是弱口令的!所以这个字典足够了!



9、这下子就解密啦,成功啦!!!嘿嘿,哈哈!!!看见wpakey: 0123456789 这就是密码! 这个密码牛屄吧?够弱智吧?!哈哈哈

10、昨天写的仓促,忘了告诉的大家,虚拟机运行cd是不支持内置网卡的,所以需要设置一下的!很简单,我就不上图了!打开vm以后,看上面菜单栏里面有个"虚拟机"然后下来看到"可移动设备",然后看到你的usb网卡,然后打上对勾就ok了!简单吧!嘿嘿

嘿嘿,同志们别拍砖,别骂!破解wpa不是开玩笑!关键是你的机器是否够强悍!字典是不是够多!!!

如果你的机器够强悍,跑包跑到几十万的话!字典收藏几百G,估计你不能破解的密码不多 了!有很多"大侠"告诉我说破解不了,说我骗人的!后来问人家,你字典多大?人家说了,我 字典超牛逼!!!有 3m的txt文件作字典!!!!同志们啊!!!这样的"大侠啊"您觉得他能 破解吗?

本次教程所使用软件下载地址:

VMware6.0.rar(本教程所用软件)http://u.115.com/file/f758c8914b

VMware7.0: http://bbs.yowao.com/read.php?tid=26

EWSA.rar: http://u.115.com/file/f37ce4a120#Download

cdlinux\_-0.9.6.1\_ISO无线破解系统.iso 传说中的奶瓶: http://u.115.com/file/f3651329a9#Download

Beini-1.2.1 集成 500W密码增强版.iso 附上我收藏的字典: 压缩后 80 多mb, 解压缩后 3g空间! http://u.115.com/file/f7d8f179da

wpa2 破解字典(解压后 3g文件): http://u.115.com/file/f3d90f8b9f

all\_birth(vip).rar: http://u.115.com/file/f3168451ef

Beini-1.1\_中的新字典.rar http://u.115.com/file/f33b6b3771\_

http://u.115.com/file/f760ed169e 14365003.rar

http://u.115.com/file/f742663269 142183.rar

http://u.115.com/file/f7bc03925f 133127.rar

<u>http://u.115.com/file/f7533611f</u> 0-9.8 位纯数密码.rar

http://u.115.com/file/f7d077303a 3+sr.rar

http://u.115.com/file/f76a7b09c8 生日 1980-2010 年.rar

<u>http://u.115.com/file/f74d658ab6</u> 弱口令集.rar <u>http://u.115.com/file/f7cd77abab</u> 超级字典.rar

<u>http://u.115.com/file/f7e9e85619</u> WPA英文字典.rar

http://u.115.com/file/f720ee3656 wordlist.rar

<u>http://u.115.com/file/f7a42521bf</u> 10 位数字.rar

关于破解字典

其实破解是最简单却也是最复杂的,简单的是只需要几个步骤设置好以后就可以暴力破解,复杂的是需要极好的耐心与运气才能破解成功,机器配置越高,字典越多,你跑包的速度就越快,你破解的几率就越高,所以不要问我多久能破解一个wpa2,我是回答不了的,因为破解有很多因素的吗!下面开始告诉大家如何在 win下跑包! 首先需要准备的软件: EWSA (老规矩,懒得下载的后面留言,我发送)字典若干 首先打开EWSA

| ●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●● | 新项目 打开项目 | ₩<br>★ 保存项目 | <b>府</b><br>开始攻击 暂                 | PP 位置更新 | ⑦<br>风云007<br>制作 |    |
|---------------------------------------|----------|-------------|------------------------------------|---------|------------------|----|
| 字典总数:<br>已用时间:<br>当前速度:<br>正在扫描:      |          |             | 等待的字典:<br>剩余时间:<br>平均时速:<br>处理器负载: |         |                  |    |
| SID                                   | 哈希       |             | 密码                                 | 状态      |                  | 评论 |
| 「」                                    | 消息       | m           |                                    |         |                  |    |

| 9) KH - HA                            | 1990 - 1990                  | 1 1900 10 10 10 10 10 10 10 10 10 10 10 10 1 |      | 2<br>(AL2007<br>8615 |   |   |  |
|---------------------------------------|------------------------------|--|------|----------------------|---|---|--|
| 等入AP目标数据文件<br>导入PSPR日本<br>导入遗信设备和日本部日 | Ctrl+T<br>Ctrl+P<br>E Ctrl+V | 举持约字典,<br>剩余时间,<br>平均时递,<br>是埋器负载;           |      |                      |   | 10500 mm(42400050) #1937<br>那就赶紧跑包<br>93年10(15(10)2050 #1943<br>我自己的网络 字典里面有我的密码  |  |
| 手动动动WPAPSKip#<br>新作动起HR面WPAPSKi       | Ctrl+W<br>読希 Ctrl+U          | 84   | it a |                      |   | 2005年—###4218602560 #1952<br>Mr.Chad(113148392) #1956<br>違印初祝県要设置外面向卡可是一设置,卡王就<br>"可移称",这作整。<br>和時6(136101208) #1959<br>它说找不到密码 |  |
| NE (N                                 | in 8:                        |  |      |                      | Ť | A O 19 16 2 16 17 16 - States   |  |
|                                       | 214                          | ŧ  |      |                      |   | ThinkPad  |  |

## 然后导入你抓到的握手包

| <b>日本</b>                        | * * | Toggle工具栏<br>Toggle的StatusBar   |                            | R R                                |      | 0<br>842:007 |     |   | 2              |
|----------------------------------|-----|---|----------------------------|------------------------------------|------|--------------|-----|---|----------------|
| 学典总数,<br>已用时间,<br>当在建度,<br>正在目睹, |     | <ul> <li>西古法祥     <li>CPU的选项     <li>GPU的选项     <li>新建学具表项     </li> </li></li></li></ul> | Ctrl+C<br>Ctrl+G<br>Ctrl+I | 举持的字典,<br>剩余时间。<br>平均时道,<br>矩埋器负载; |      | BUT P        |     | 1955-1889(42)588(556) 51957<br>形就赶紧缩包<br>34846(350)2050 81943<br>我自己的网络 字典里面有我的密码       | A 8            |
| SSID                             | 1   | 85944 党的选择<br>且地记录选择  | Ctrl+m<br>Ctrl+L           | #41                                | it e |              | r 2 | 20次示 単単421860256) 81952<br>Mr.Child(113148392) 81956<br>地球の10 回転の開始と開始と開始上 マロニー10 第 上下の |                |
|                                  |     |   |                            |                                    |      |              |     | □ 司務後,这件書。<br>和時(36)0209 81959<br>○ 從投太到家研  | 1.<br>21<br>21 |
| •                                | -   |   | 17                         |                                    |      | _            |     |   | 16.6.          |
| *21%                             |     |   |                            |                                    |      |              | P   | YODESS'P G. SHOK  | *              |
|                                  | -   |   |                            |                                    |      |              |     | 关闭口 家道  | 5 -            |
| action.                          | U 1 | linated Green   |                            |                                    |      |              |     | ThinkPad  |                |

然后新建字典选项

| ✔ D:\程序备份\破                  | 解字典\弱口令集\wordlist.txt                        | *      | 添加                            |
|------------------------------|--|--------|-------------------------------|
| ☑ D:\程序备份\碳                  | f解字典\WPA英文字典\wordlist.TXT                    | E      |                               |
| ✓ D:\程序备份\破                  | (解字典\10位数字\wordlist.txt                      |        | 删除                            |
| ✓ D:\程序备份\碳                  | (解字典\生日1980-2010年\wordlist.txt               |        | Contra a serie de la compañía |
| ✔ D:\程序备份\破                  |  | 同主移动子典 |                               |
| ✓ D:\程序备份\破<br>図 D:\用度名公\3   |  | 向下移动字典 |                               |
| ▼ D:\程序备份\破<br>▼ D.\程序备份\破   | (胖子典)(1-100W),1X)<br>:                       |        |                               |
| ☑ D:\程序备访\破 ☑ D:\程序备访\破      | (解字典)(301W-700W).1X1<br>;解字曲)(401W-500W).1X1 |        | 选择全部                          |
| ▼ D.1程序备份100                 | (解字典)14365003 byt                            | *      |                               |
| •                            | III  | •      | 取消所有                          |
| 十加选项<br>引忽略少于8个或制<br>「码变动的选择 | 置过64个字符的密码                                   |        |                               |

然后添加你字典所在路径 然后ok就可以开始攻击握手包进行破解了

当然,除了无线宝bt5 来破解wpa加密、wpa2 加密 您还可能感兴趣的是: <u>无线宝可以蹭哪些</u> <u>网?</u> - <u>全向天线和定向雷达的区别</u>