MDK3—无线拒绝服务攻击的开始

由于我们的无线 802.11b/g 网络使用公用 2.4 GHz 频段，因此每个无线网络都会受到周围无线电波的干扰，包括蓝牙、无线电话、微波炉和周边的无线局域网。这些由外界环境所造成的干扰或多或少会给无线网络的传输速率和稳定性造成一定的影响，在干扰严重的情况下也可能会造成对无线网络的拒绝服务的现象。那么本文所讨论的内容是作为一个恶意攻击者，主动对目标无线网络实施拒绝服务攻击，在短时间内造成目标无线网络或者数个无线网络完全瘫痪，希望让更多的无线使用者意识到无限网络的脆弱性，尽量避免在无线网络上进行高可用性的工作。

MDK3 是一款集成在 BackTrack3 上的无线 DOS 攻击测试工具，能够发起 Beacon Flood、Authentication DoS、Deauthentication/Disassociation Amok 等模式的攻击，另外它还具有针对隐藏 ESSID 的暴力探测模式、802.1X 渗透测试、WIDS 干扰等功能，对于后面几种功能模式，希望大家能一起探讨和参与测试，把测试的过程和经验分享出来。另外关于 MDK3 相关的的详细参考信息和最新发布的版本的信息可以参考 http://homepages.tu-darmstadt.de/~p_larbig/wlan/，接下来将围绕这三种 DOS 攻击模式进行测试。

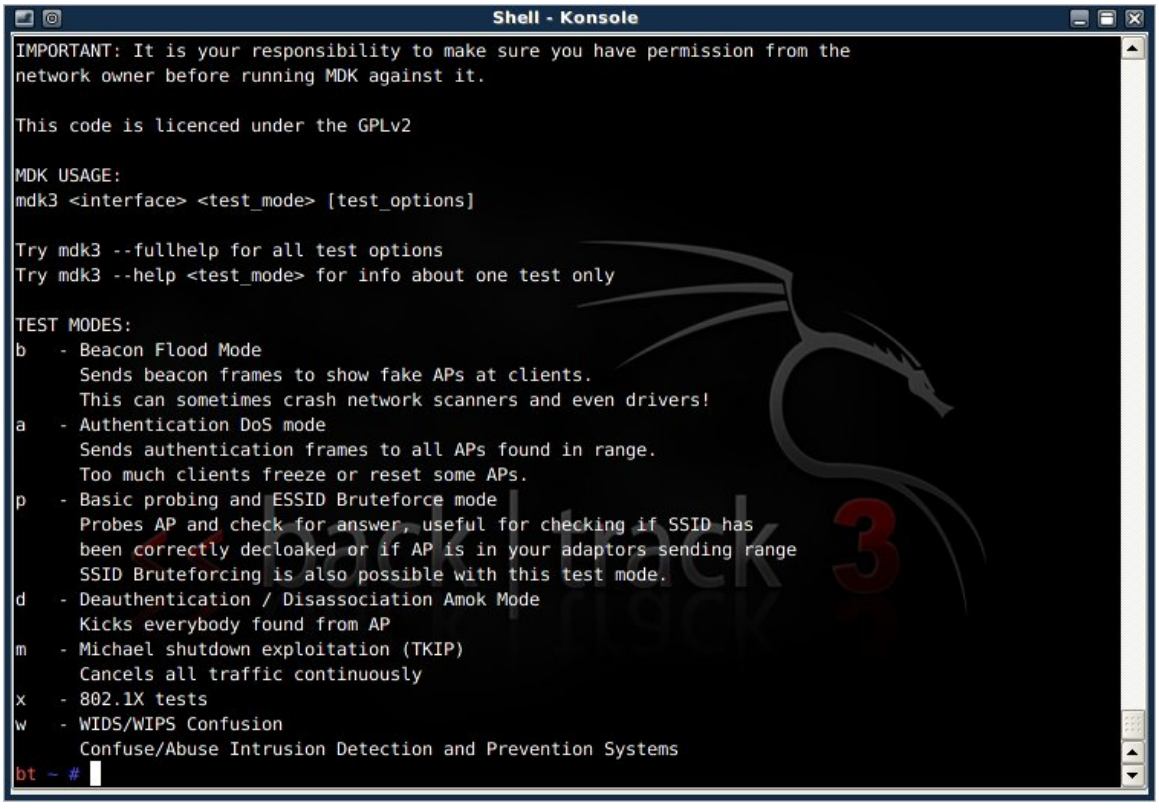

图 1 MDK3 的几种攻击模式

Beacon Flood Mode

这种攻击模式类似于 Fackap，就是向无线信道中发送大量虚假的 SSID，来充斥客户端的无线信号列表，使客户端找不到真实的 AP，以下是 Beacon Flood 模式的参数，可以为将要生成出的 SSID 设定各种参数，如 WEP/WPA 加密信号、Ad-Hoc 对等信号、自定义 ESSID 与 BSSID 等。

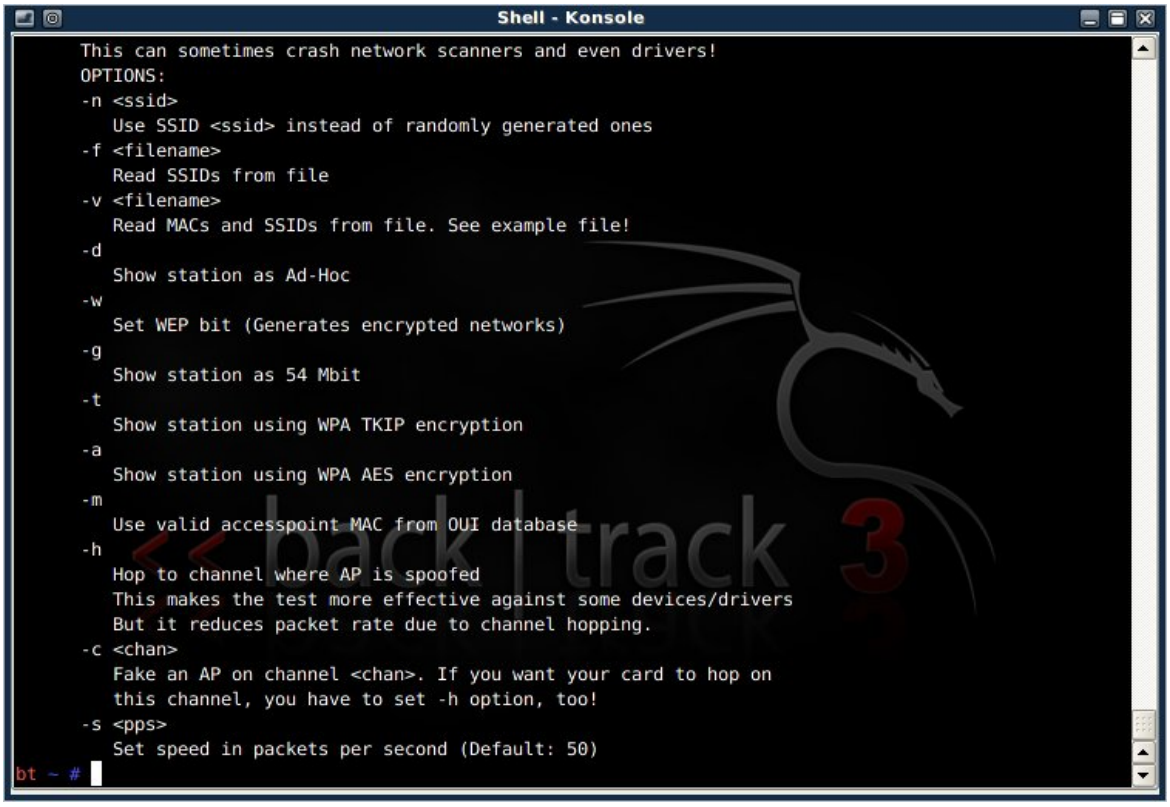

图 2 Beacon Flood Mode 的参数

发送 mdk3 wlan0 b 即可向无线网络 1-13 信道广播随机产生的 SSID，wlan0 作为无线网卡的接口，可以使用-c 参数指定对单一信道发送广播

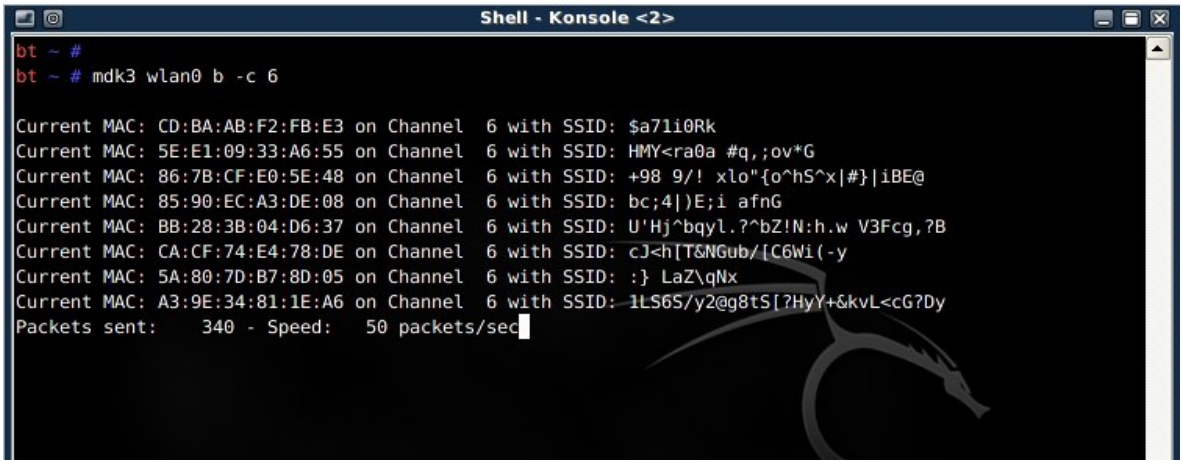

图 3

上图可以看到在默认情况下，发包的速率为 50pps，因此可以使用-s 参数来指定它每

秒的发包速率，使用 mdk3 wlan0 –c 6 –s 1000

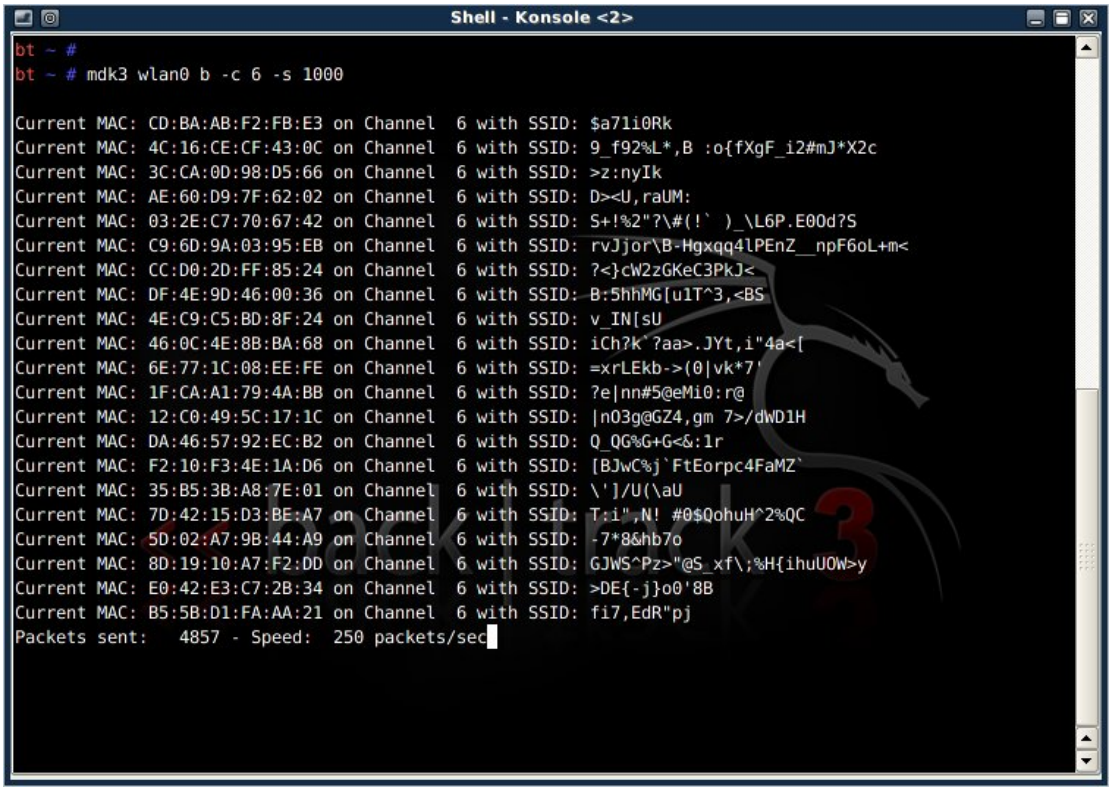

图 4

可以看到此网卡的最高发包率为 250pps，产生的效果如下图：

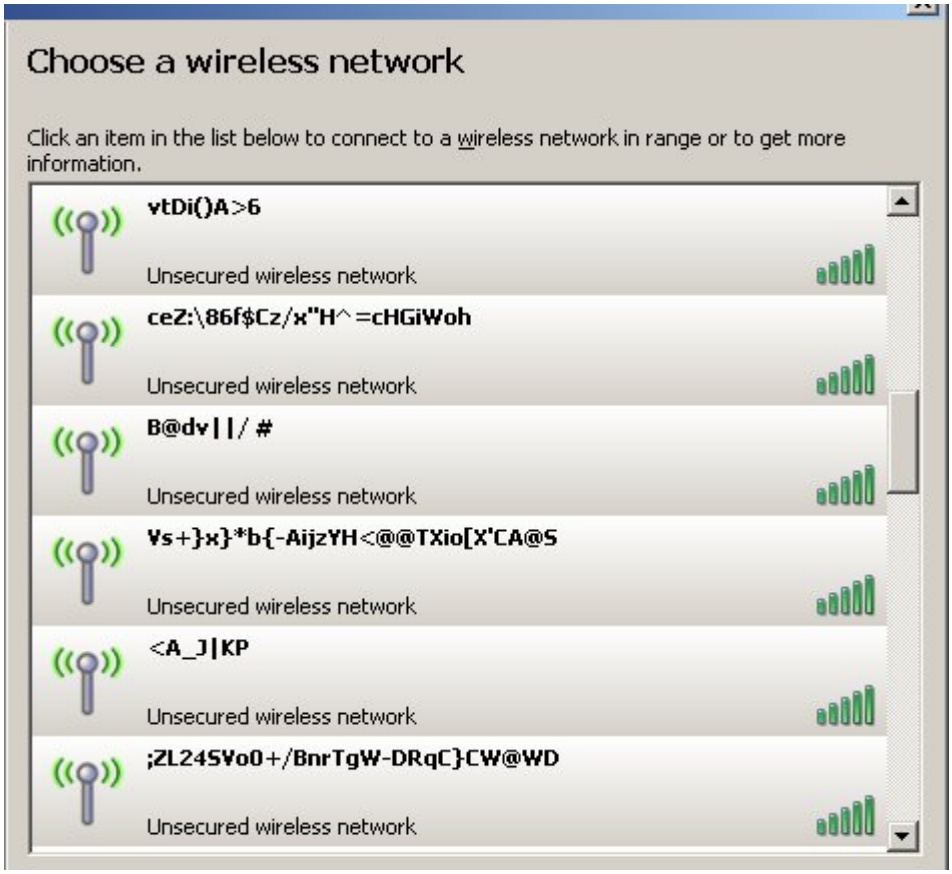

图 5 Fackap

若要使用自定义的 SSID 对信道进行广播，可以使用-f 参数读取目标文本中设定的 SSID，可以将设定好 SSID 的文本直接放在/Root 目录下：

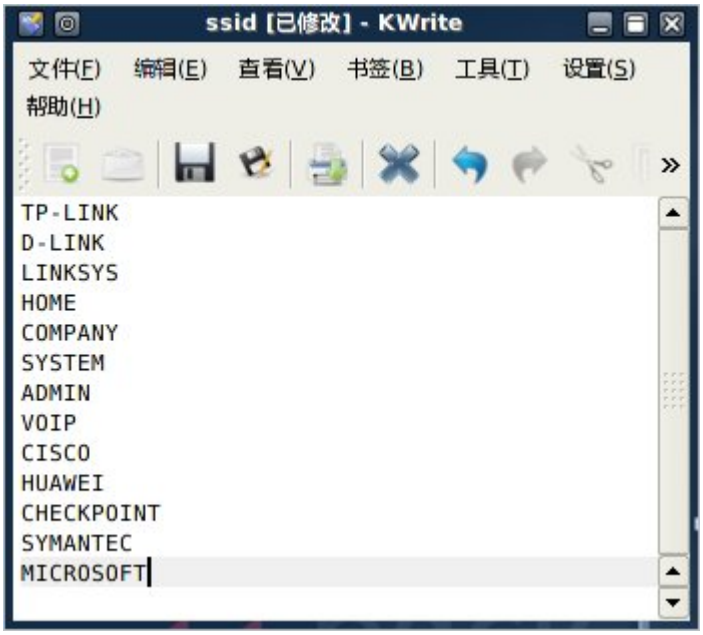

图 6 ESSID 列表

使用 mdk3 wlan0 –c 6 –f ssid，ssid 为自定义保存的文件名，存放在/root 目录下可以不指定路径，发包的效果如下：

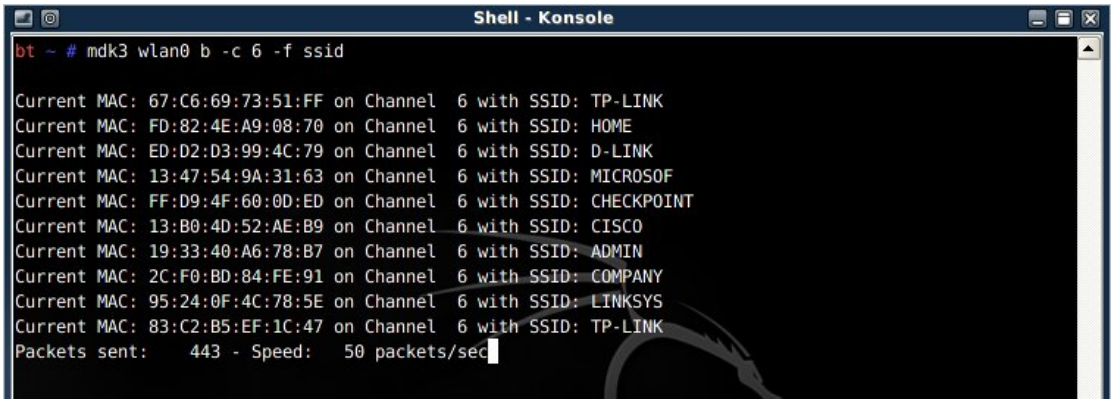

图 7

再来看一下在 WINDOWS 无线管理器下产生的效果。mdk3 在发包时除非手动进行停止，否则它会一直循环的发包。而在 WINDOWS 无线管理器下，这些 SSID 显示不会重复，重复的 SSID 标记只会显示信号最强的一个，而使用第三方的无线管理器或者在 LINUX 下以 BSSID 作为排列依据的工具会将所有重复的 SSID 全部显示出来。

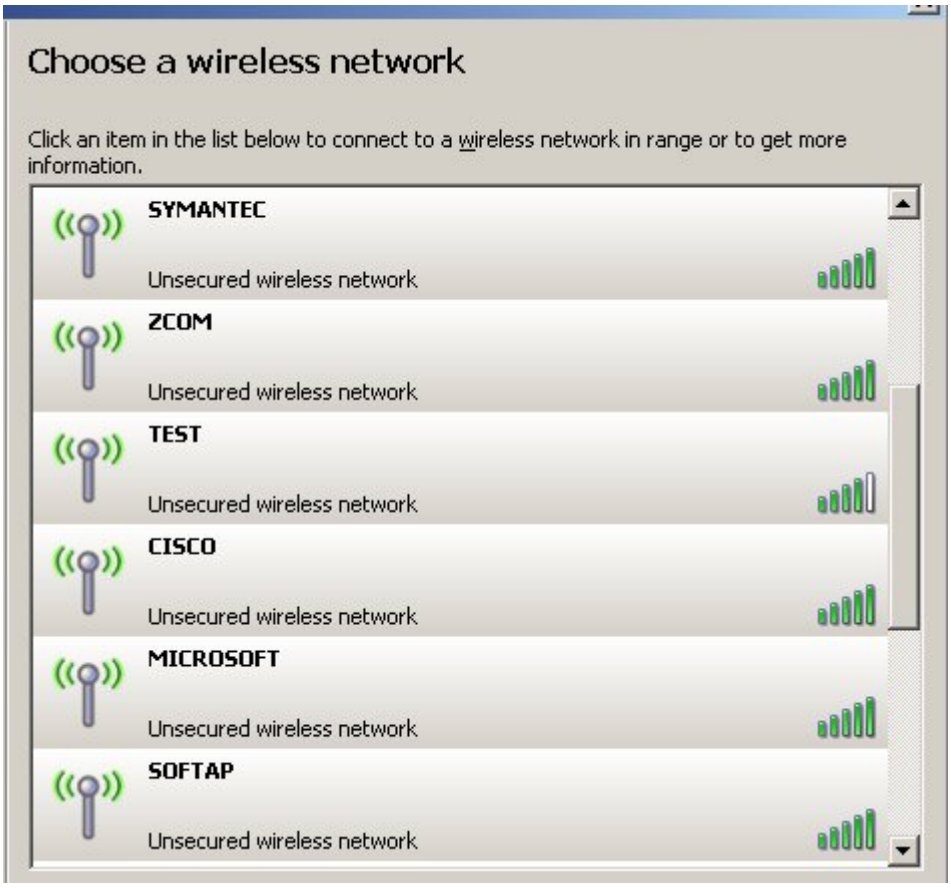

图 8 Fackap

Authentication DoS mode

这是一种验证模式的攻击，攻击的效果是自动模拟出随机产生的 MAC 地址向目标 AP 不断发送验证请求，导致 AP 忙于处理过多的验证请求而停止正常用户的登录请求，甚至影响已在线的客户端。

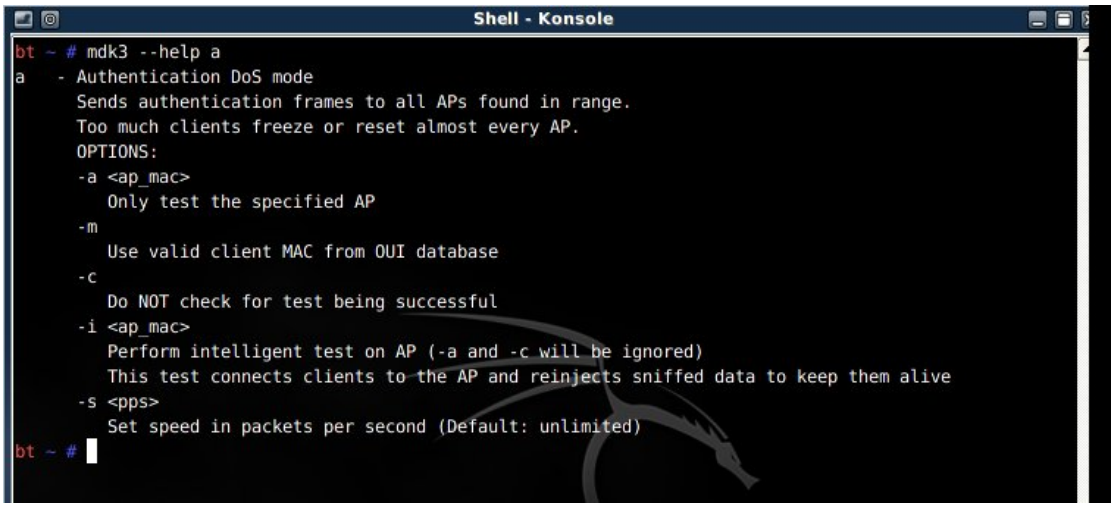

图 9 Authentication DoS mode 的攻击参数

在默认情况下，若不指定参数，使用 mdk3 wlan0 a 它会向所有可发现距离范围内的 AP 进行循环攻击，导致周围的 AP 均无法正常工作。这里测试时使用-a 参数指定目标 AP 的 BSSID，也就是我自己的 AP，mdk3 wlan0 –a 02:40:77:BB:55:13 效果如下：

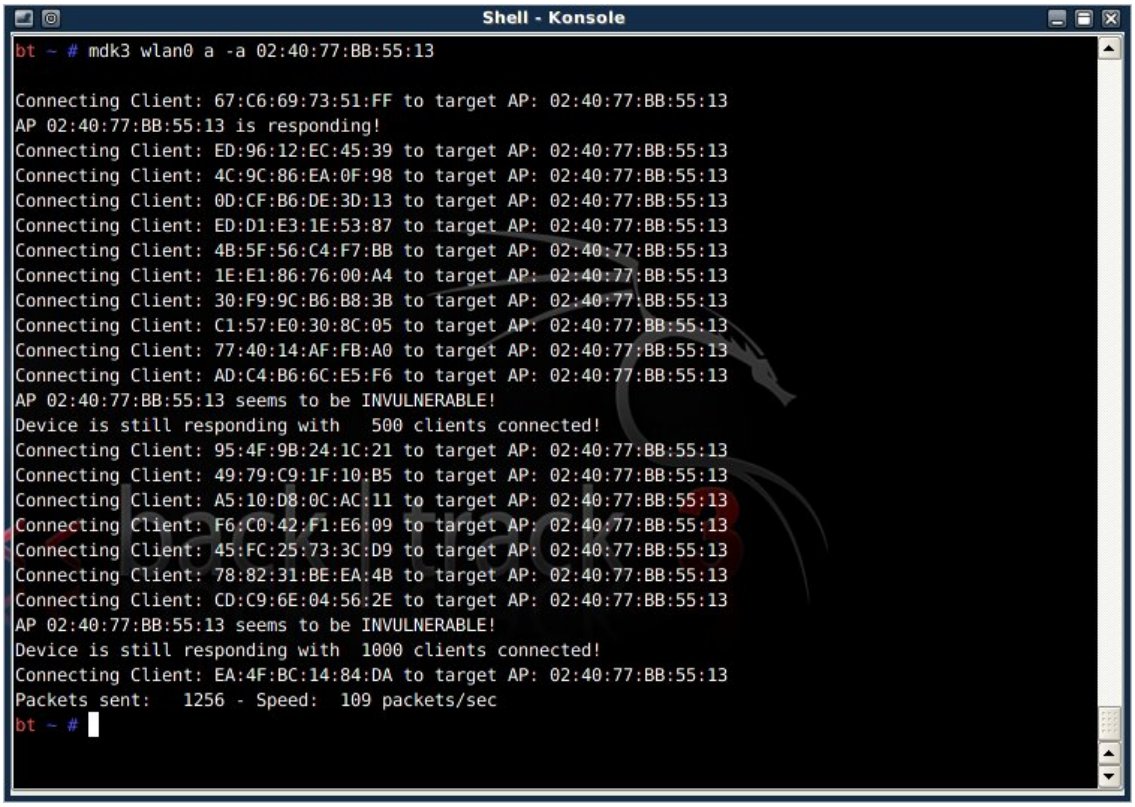

图 10 Authentication DoS 模式攻击

程序会在攻击过程中自动检测 AP 的状态，但是实际测试过程中发现并不一定准确，图上虽然显示 AP seems to be Invulnerable，还能接受更多的验证请求，但仅攻击了十几秒之后，用新的客户端去连接 AP，已经无法建立正常连接，此时连接在此 AP 的客户端也发现不能正常上网了，攻击停止后客户端依旧无法连接上 AP，最后只好将 AP 断电重启才恢复正常。

Deauthentication/Disassociation Amok Mode

这是危害力极大的一种攻击模式，可以将所有可见距离范围内AP的客户端均踢下线，包括AP与AP之间的连接（有时候AP与AP之间会进行桥接模式或中继方式的连接），作者对此攻击模式的一段标语：Allowing a single attacker to get down a huge network ....，只需一个攻击者就可能造成大范围的无线网络瘫痪。

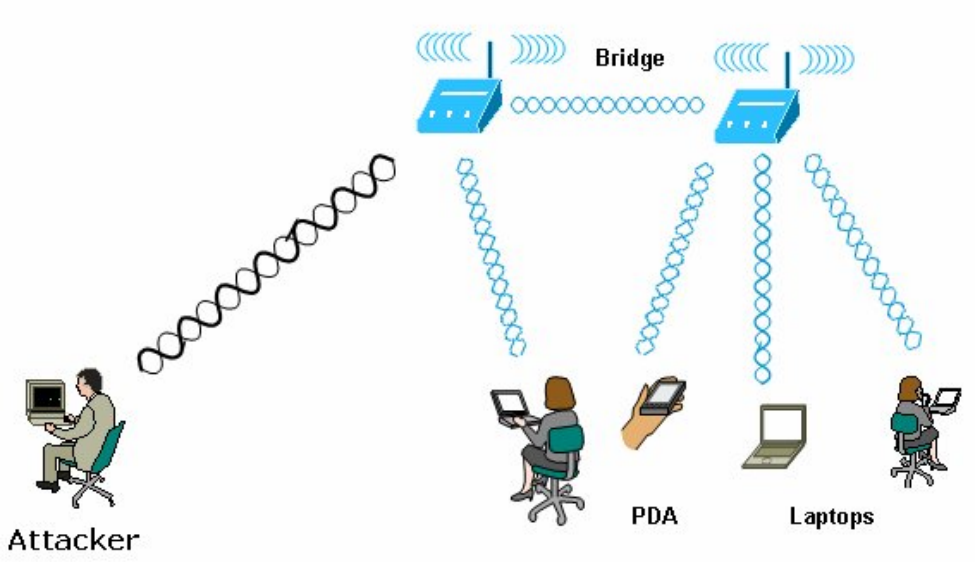

图11

与Aireplay-ng -0攻击模式的效果类似，但是与之不同的是此攻击模式会对周围所有的AP发动循环式的攻击，直到手动停止。可以指定参数加入BSSID的黑名单与白名单列表。

使用mdk3 wlan0 d进行测试，效果如下：

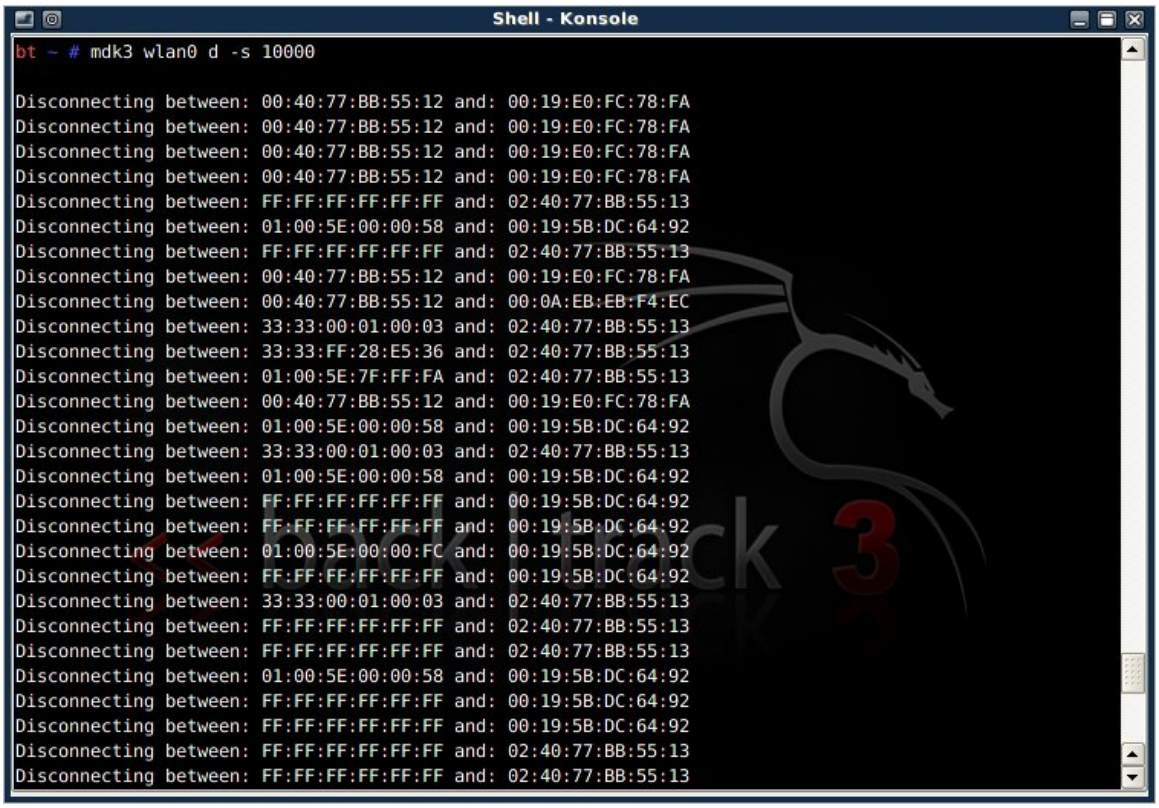

图 11 Deauthentication/Disassociation Amok 模式攻击

左列的MAC地址为客户端的BSSID，右列的MAC为AP的BSSID，可以看到攻击会循环的断开AP与客户端之间的连接，所造成的结果可想而知...

最后我们试想一下这样的场景：攻击者驾着车来到某一写字楼下面，将一个高增益的定向天线对准某一层办公楼，锁定完目标后，首先使用分离模式将所有的客户端与AP断开连接，同时对所有的AP进行虚假验证模式的攻击，让AP忙于处理大量的登录验证请求而失去响应，此时正常的客户端发现无线连接中断并且无法自动重登录之后，肯定会打开无线连接管理器采取手动连接的方式试图连接原先的信号，而正巧攻击者正使用Fackap模式不断的将自定义的SSID充斥满无线信道中，当正常客户端打开他们的无线连接管理器之后，却发现有成百上千个信号出现在列表当中，却不知道应该连接哪个...那一定是相当糟糕的事情☺

2009-2-8
ZOOBOA
zooboa@gmail.com