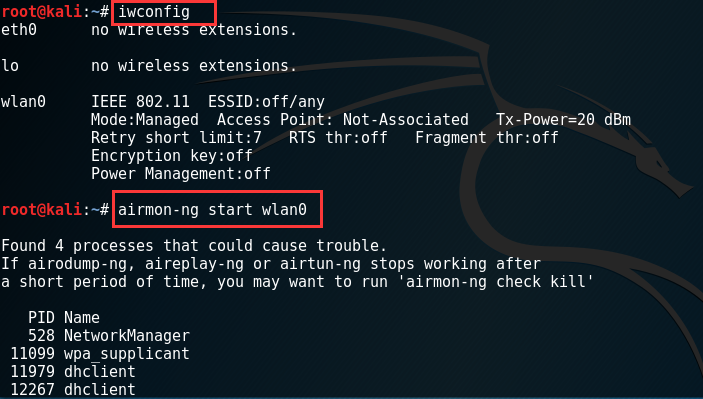
本篇实验参考老外Deepanshu Kapoor 安全专家的文档

MITM（中间人攻击）：原理就是伪造一个热点，攻击真实的热点，客户端连上伪造的热点后就可以对他进行抓包等。

将无线网卡开启混杂模式



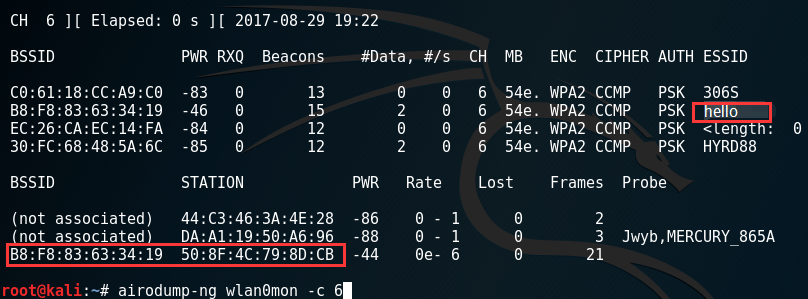
安装网桥配置命令



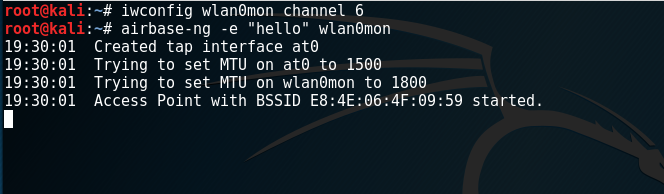
开启侦听，获取目标

airodump-ng wlan0mon –c 6

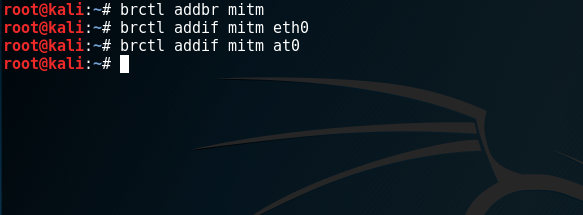
可以获取到客户端和ap的mac地址，然后ap名为hello



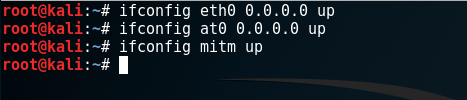
让网卡工作在频道6上，并伪造热点hello，此时虽然能连，但不能上网也不能分IP地址



开启一个shell桥接所用网卡，使得之间在同一广播域下 at0为伪造的ap，eth0是真实可以上网的网卡

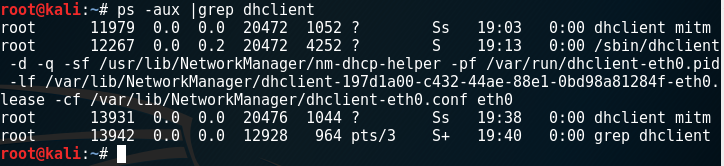


网桥的每个物理网卡作为一个端口，运行于混杂模式，是在链路层工作，所以不需要IP

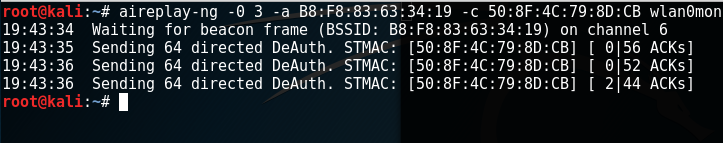


mitm端口需要上网，因此需要给它开启dhclient客户端（68）来获取IP地址。

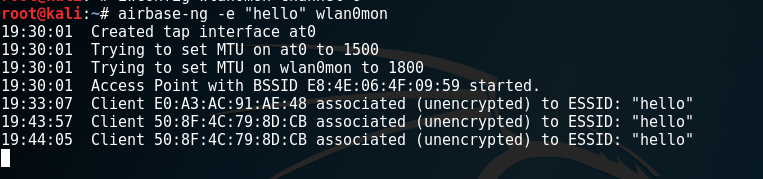
dhclient mitm&



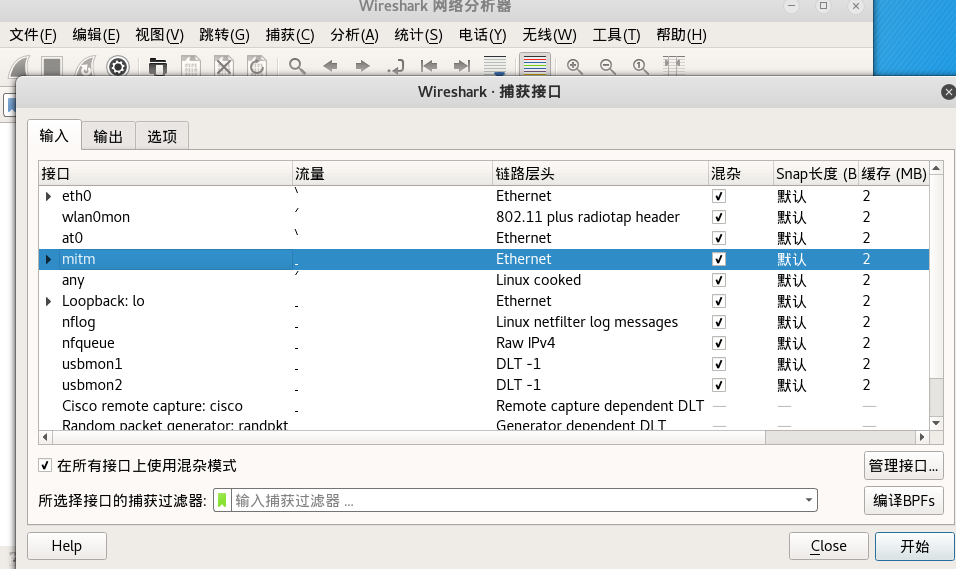
攻击客户端，让其掉线。

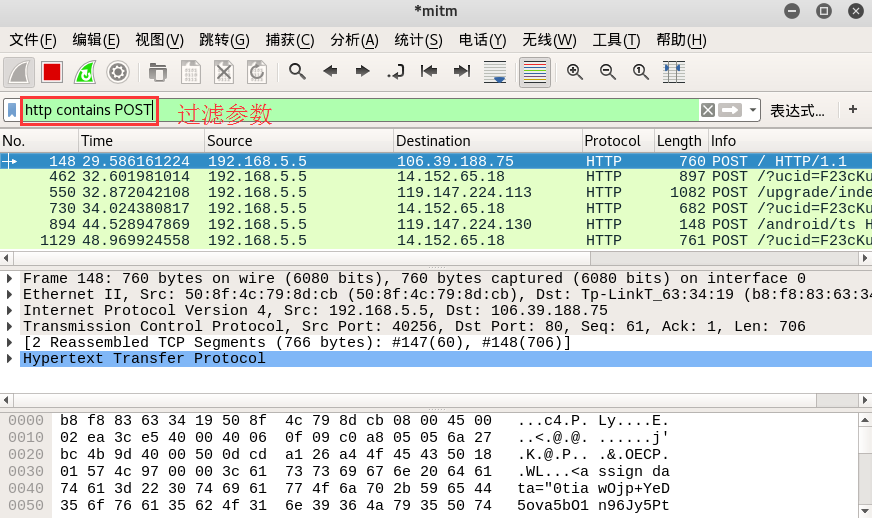


然后再刚刚启动伪造热点的窗口上可以看到有客户端连接（上钩了）



打开wireshark 监听mitm网卡





后面就可以安安静静的抓包了

------------write by demon