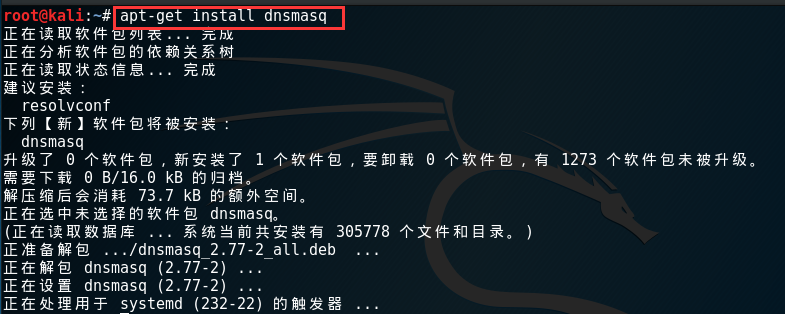
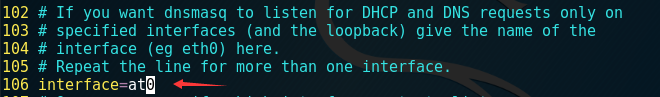
下载dhcp 和 dns服务器：就一个工具dnsmasq



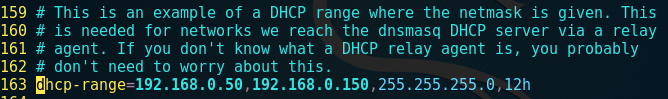
修改配置文件：

vim /etc/dnsmasq.conf

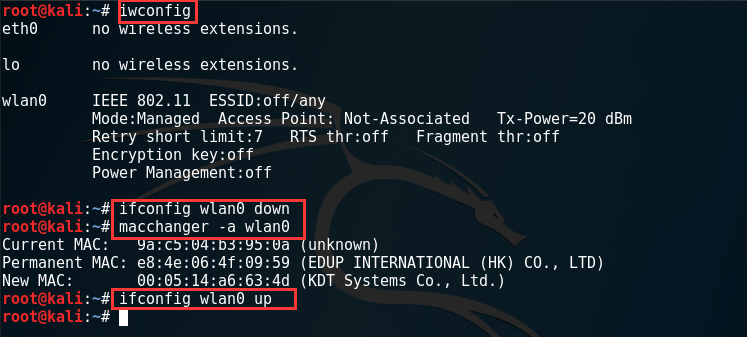
配置dns 和 dhcp 服务的监听物理端口



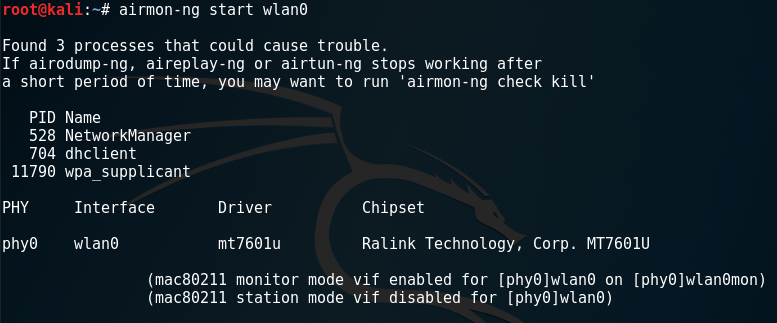
配置分配的IP地址池



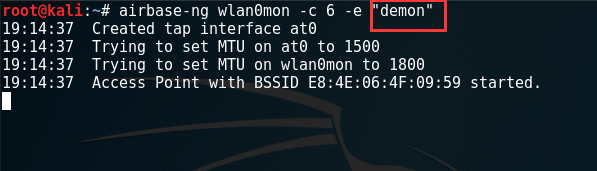
不管搞不搞事情，都修改一下mac地址



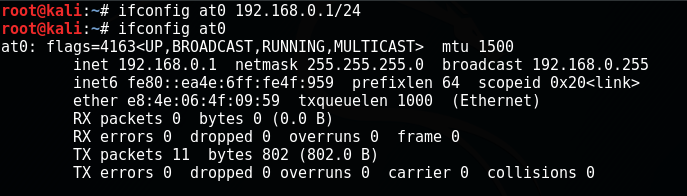
开启混杂模式



开启伪造热点，demon是热点名字，此时at0就会被创造，代表热点网卡



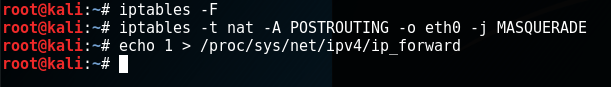
开启一个新的shell，给at0设置临时IP地址，注意：这个IP地址是充当地址池的网关



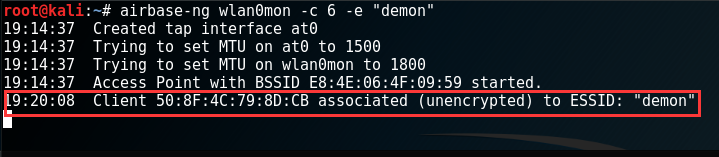
开启刚刚配置好的dhcp服务：



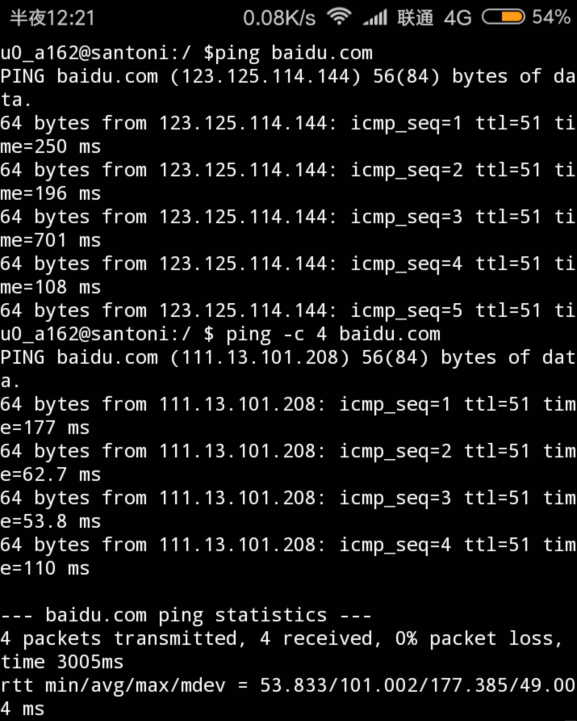
此时kali上有两个网段，一个(at0)不能上网，一个(eth0)可以上网，需要将两个网段关联起来，这里可以通过nat转发来实现

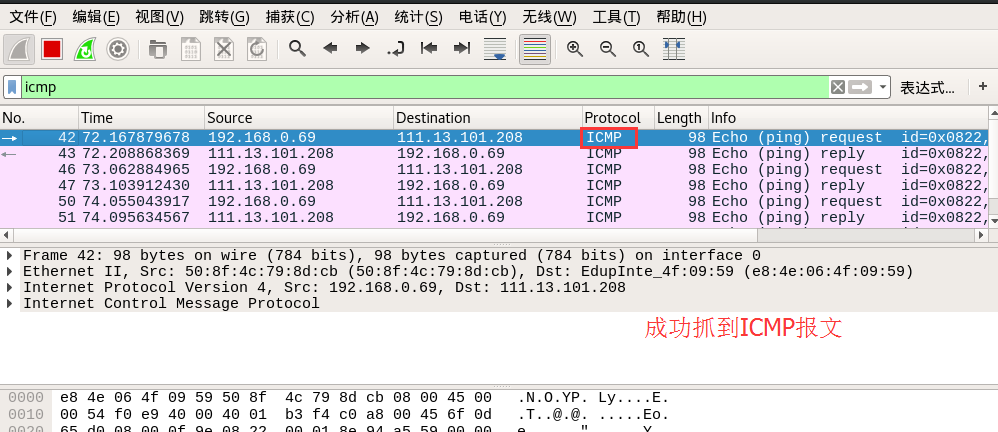


此时，回到刚刚开启伪造热点的窗口，可以用手机模拟受害者连上伪热点。



开启wireshark进行抓包，这里就抓icmp好了，然后用手机ping百度模拟通信





然后就可以默默当中间人，抓包改包社工了

--writen by demon