**会话截取-登录别人的百度贴吧**

**可以实现在同一个局域网内，抓到别人浏览的网页，可以随时搞破坏，不对的！！！但是成功几率也不是很大**

Wireshark 抓包

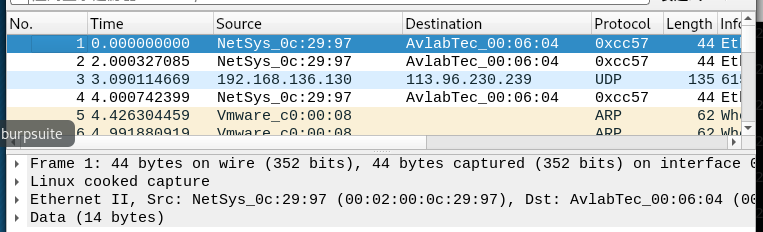
Ferret 重新生成抓包后的文件

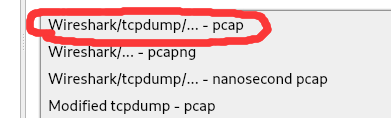
Hamster 重放流量

1. 流量转发：echo 1 >/proc/sys/net/ipv4/ip\_forward

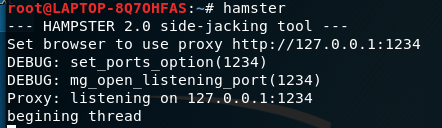
**一：**

1. arpspoof -i eth0 -t 192.168.136.130 192.168.136.2
2. 输入Wireshark，出现如图：



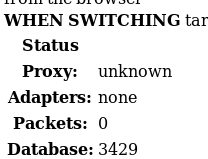
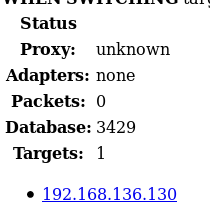
目标电脑登录网站（灯火互联网），关掉，本来是红颜色的，点击“文件”，选择“另存为”，保存格式为保存到桌面，关掉所有窗口，停掉欺骗

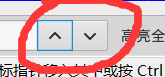
1. 在桌面打开终端，输入ferret -r 文件名(cookie.pcap)，生成了一个 文件，这时桌面上有两个文件，（cookie.pcap和hamster.txt）打开 hamster.txt也是看不懂的。
2. 用到工具Hamster 重放流量



要求把http的端口改为1234，并且访问1234

1. 打开火狐，右键页面上方打开菜单栏，选择“编辑——首选项—— 网络代理（页面最下方）”，改成这个样子，

，然后访问，会出现，即没有抓到。再次在桌面打开终端，执行以下操作，（cp hamster.txt /root —— cd .. —— hamster）,打开浏览器，输入127.0.0.1，发现

1. 点击IP地址，出现很多的链接，Ctrl+F，在搜索框输入 www/atcpu.com，点击链接，不能出现目标电脑浏览的网页，就按 ，直到找到对应网站的页面为止，

1. 先删掉第一种方法保存的hamster.txt

**二：**

ls —— rm hamster.txt

1. ferret -i eth0
2. 在另一个终端hamster
3. 在火狐中修改代理，同一，在目标电脑（即window7系统里面浏 览网页，127.0.0.1:1234里面的网址也在实时更新）