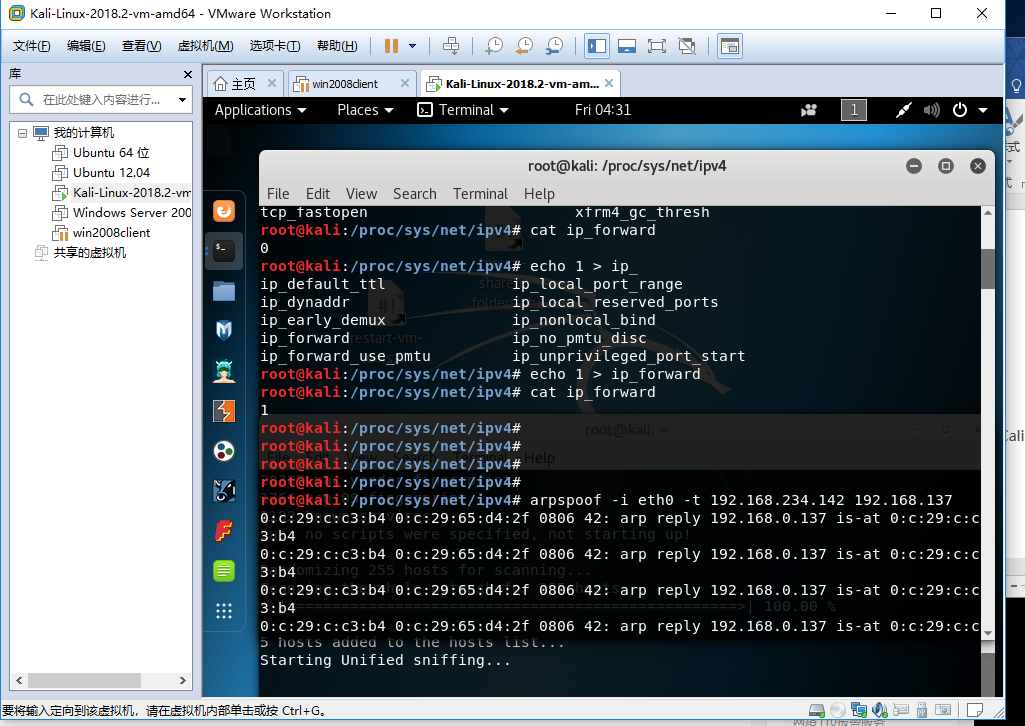
**Mac泛洪攻击与ARP攻击模拟项目**

环境搭建：

WMware workstation 12 PRO安装，Windows Server虚拟机、Cali虚拟机、Ubuntu虚拟机



Windows server 2008搭建FTP服务器：

<https://wenku.baidu.com/view/590c321110a6f524ccbf85ea.html?qq-pf-to=pcqq.c2c>

其中遇到的问题及解决方法：

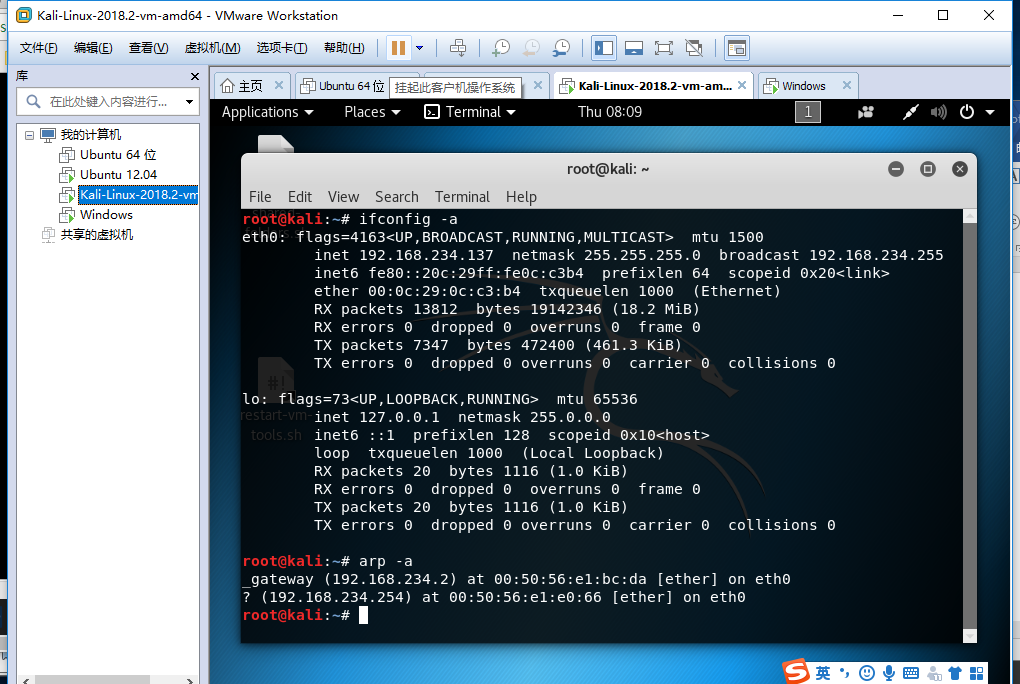
win server 2008 创建用户时密码不满足策略要求：

<https://blog.csdn.net/qq_37533911/article/details/78780515>

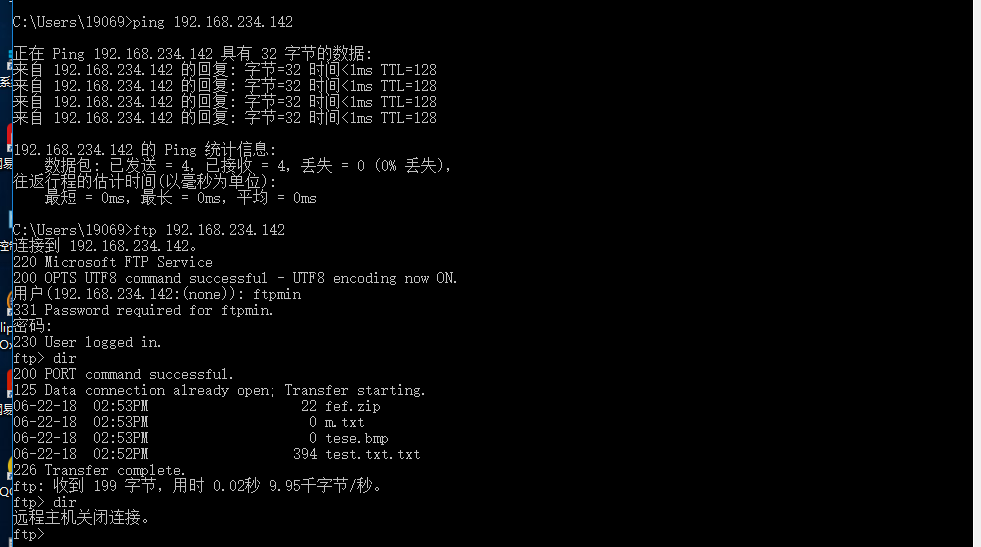
**实验一 MAC泛洪攻击实现**

<https://blog.csdn.net/chengxuya/article/details/7884852>

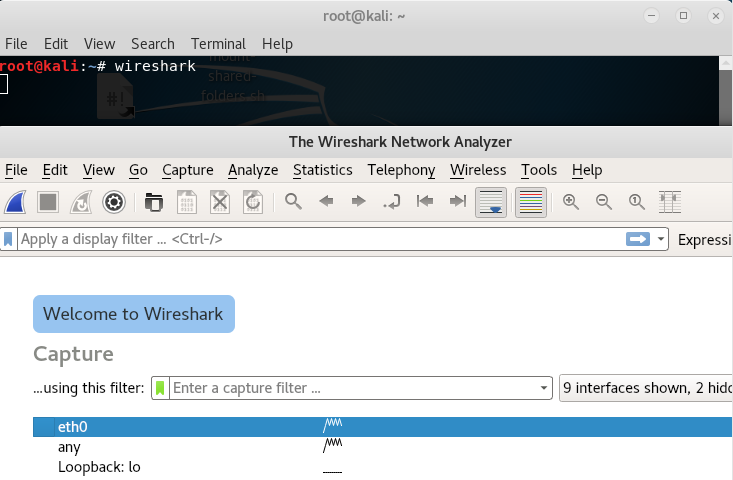
1、主机C（攻击机）的IP查询和ARP表查询：



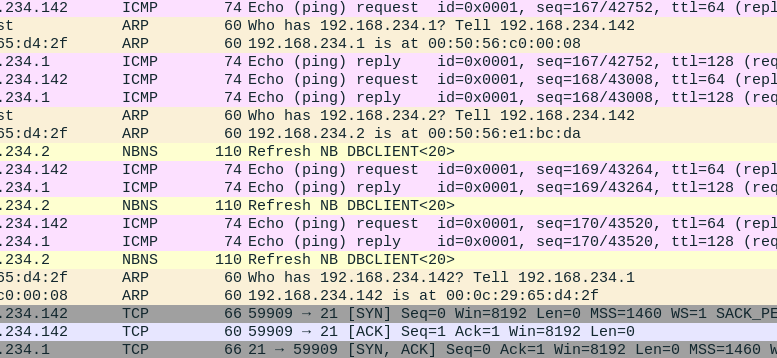
登录与通信：



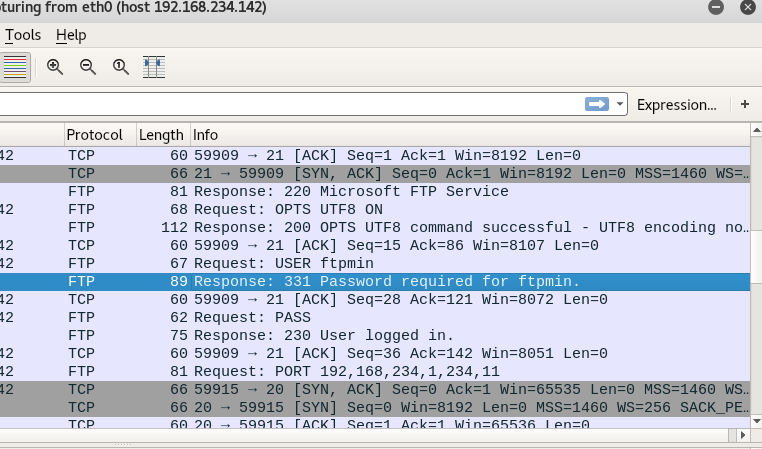
Cali中安装Wireshark



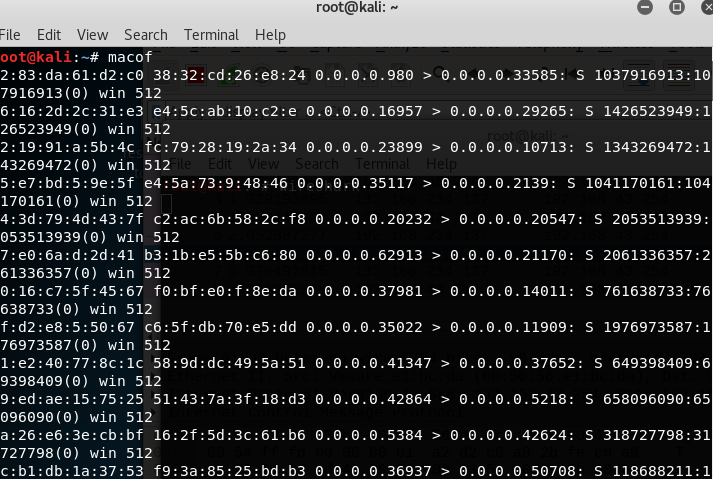
用Wireshark监听客户机，设置过滤器“host 192.168.43.254”



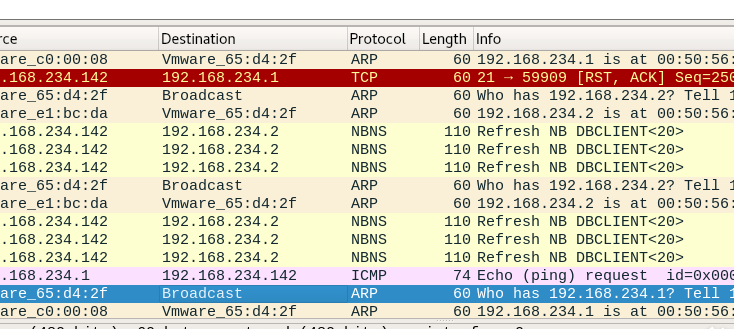
读取到登录名“ftpmin”以及登录密码“ ”（空格）。



用攻击机采取mac泛洪攻击



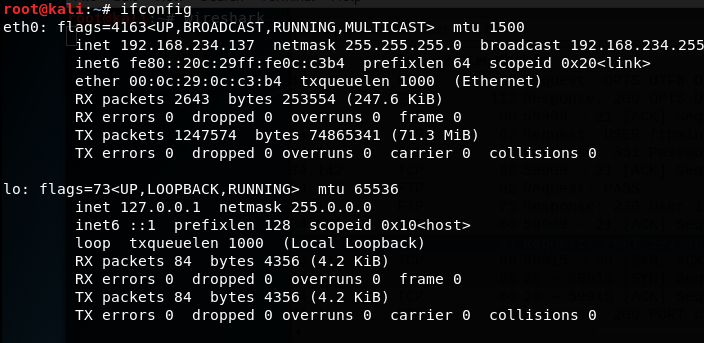
Mac泛洪攻击使得被攻击机只能广播信息，攻击机从而获取信息



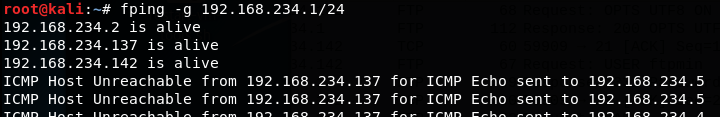
**第二部分 kali 实现arp攻击和arp欺骗**

参考：<https://blog.csdn.net/niekai01/article/details/52214942>

攻击机IP：

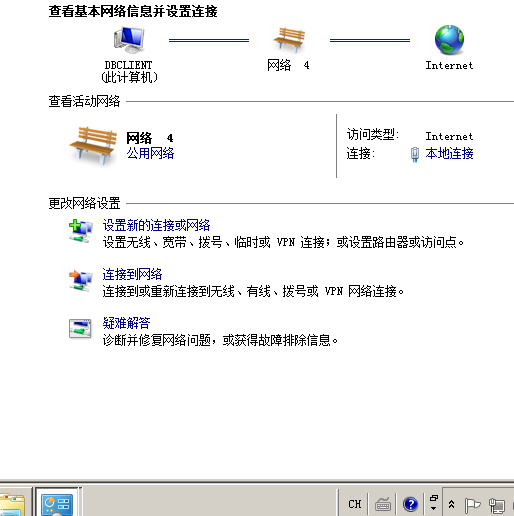


Fping找寻局域网中其它主机

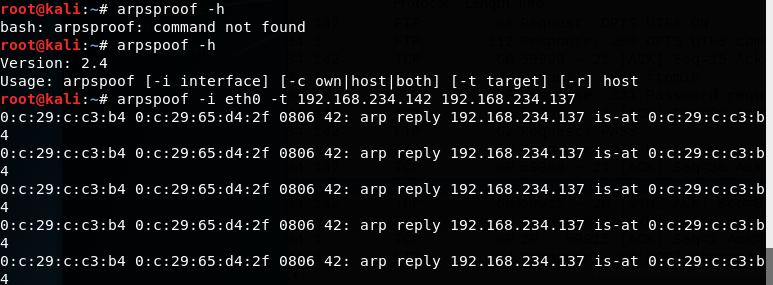


所以确定攻击机IP：192.168.234.137，攻击目标IP：192.168.234.142

攻击前攻击目标可以联网



此时，在Kali中使用arpspoof工具实现ARP攻击

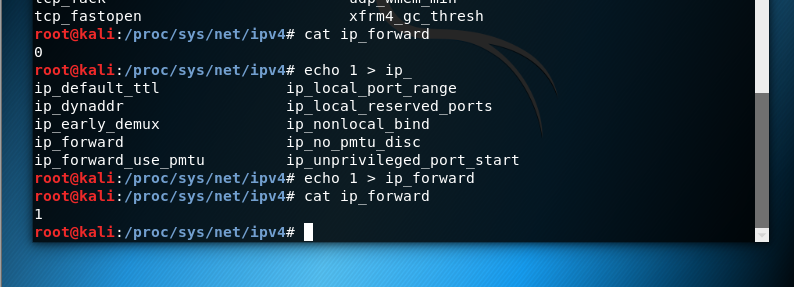


之后无法上网（是Windows Server），没有浏览器，无法展示

（2）现在尝试ARP欺骗，获取被攻击者的用户名和密码。

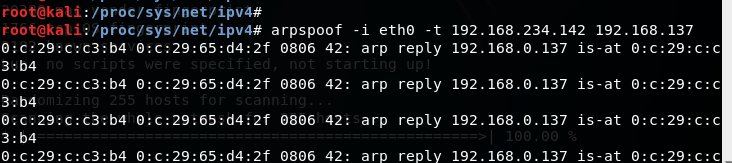
首先，我们要使用的工具还是ARPSpoof，因为我们此次攻击方式是欺骗，同时，我们还是用Eteercap去嗅探目标靶子的流量，来获取目标的重要信息。

但是，首先要开始IP转发功能，linux因为系统安全考虑，是不支持IP转发的，其配置文件写在/proc/sys/net/ipv4的ip\_forward中。默认为0，接下来修改为1 。

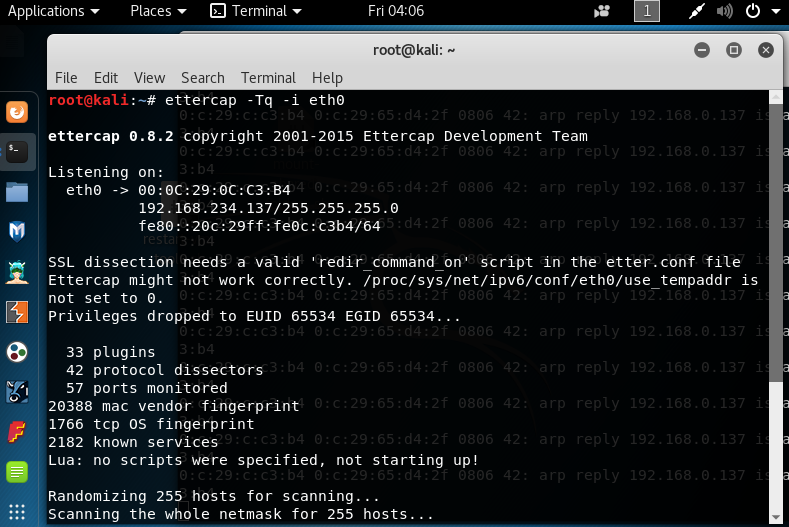


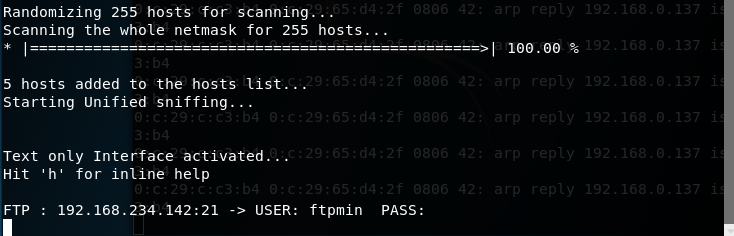
从图中我们可以看出，系统的配置文件以备我们修改，接下来我们开始arp欺骗。

依然使用arpspoof，具体参数如图



此时欺骗成功，接下来我们使用ettercap嗅探。





用实验一的机子登录server，相当于两者发生数据交换，被ettercap嗅探出来，得到用户名：ftpmin，密码为空格，看不出来，哈哈