信息安全课程实验二

1. **实验目的**

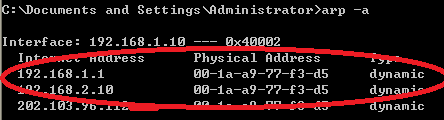
学习虚拟机安装，版本控制Git软件、收发包、抓包软件使用及初步具备协议分析能力；

1. **实验工具**

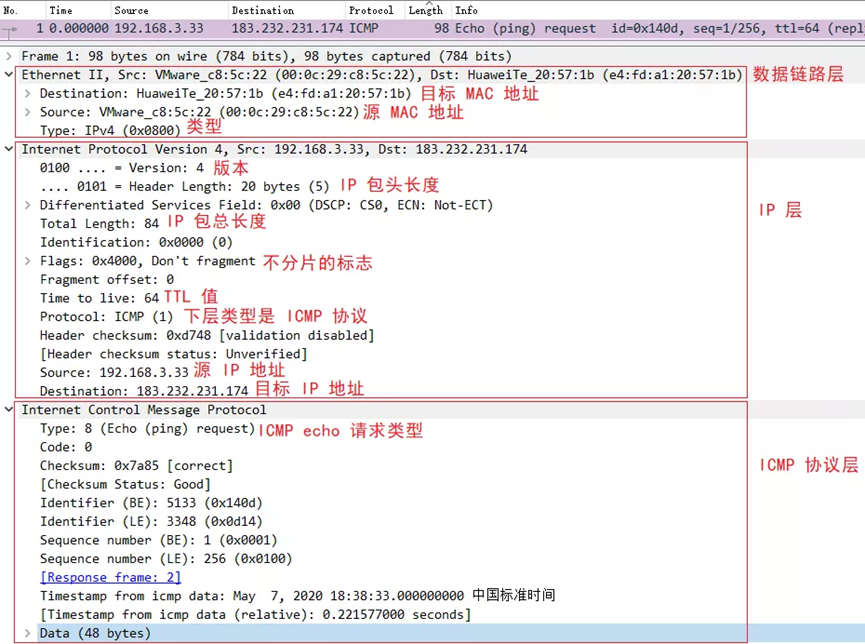
Centos6以上系统，GitHub，科来数据包生成器/科来数据包播放器软件（pktbuilder\_x64/pktplayer\_x64），Wireshark

1. **实验内容**
2. 采用科来数据包生成器生成三种ARP协议数据包（请求、应答、免费(Gratuitous ARP)三种形式的ARP包；

B、采用科来数据包播放器软件将三种伪造数据包向攻击目标机发送，检验三种形式的ARP包是否具备断网攻击能力（采用arp命令查看攻击前后的目标机ARP缓存表是否发生变化并截图说明）



C、整个攻击过程采用Wireshark进行抓包并参考如下图对三种ARP协议进行协议分析和标注，同时对应攻击数据包导出以pcap包格式保存；



D、针对ARP攻击，如何进行防护，请提出自己的意见和建议。

1. **实验报告要求**
2. 对实验过程进行截图，并配合文字详述以上实验内容；
3. 对实验报告中引用的互联网资料，需要以参考文献形式加以引用标注
4. **实验报告上交截止时间**

作业内容包括：三种ARP协议的PCAP数据包文件（共三个文件），实验报告一份，将这些内容上传github进行版本控制。[2020年5月11日18点前将作业的github下载链接发zhxhz@163.com](mailto:2020年5月11日18点前将作业的github下载链接发zhxhz@163.com)邮箱。

作业情况如下所示：

1.首先是利用科来软件生成ARP请求包，然后发送攻击对象

具体操作如下所示：

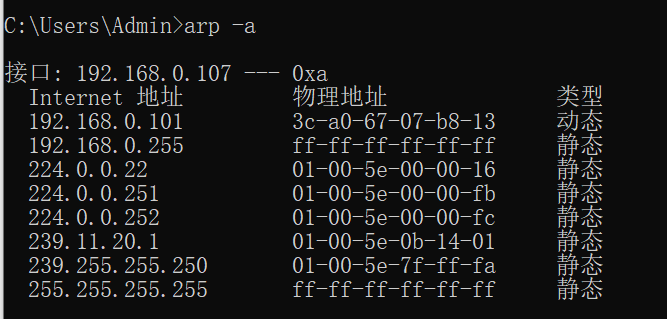
1. ARP请求包的生成图



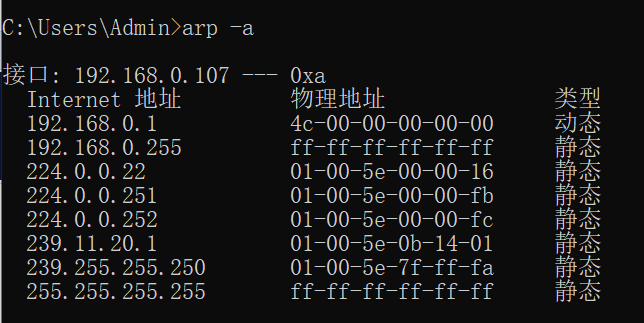
（2）开始发送ARP请求包，设置发送1000次。



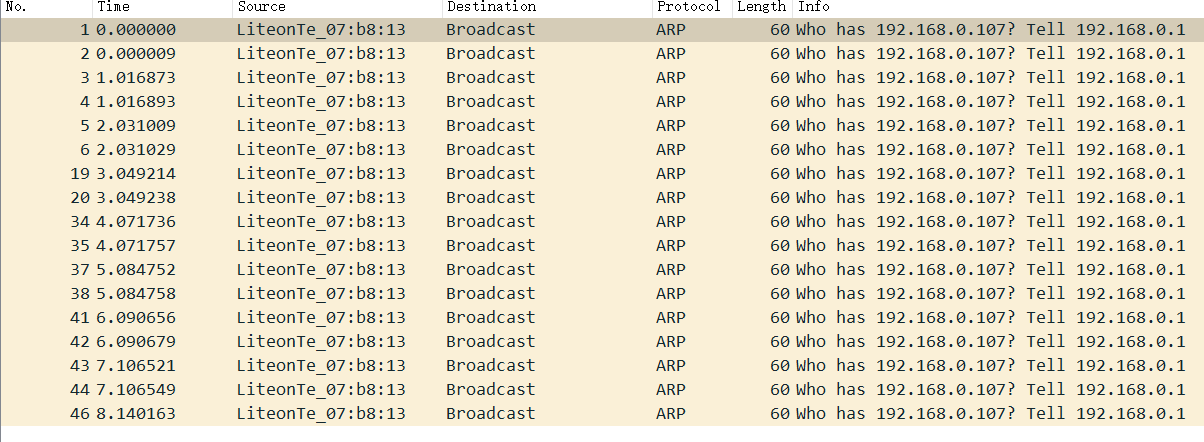
发送ARP请求包之前的ARP缓存表



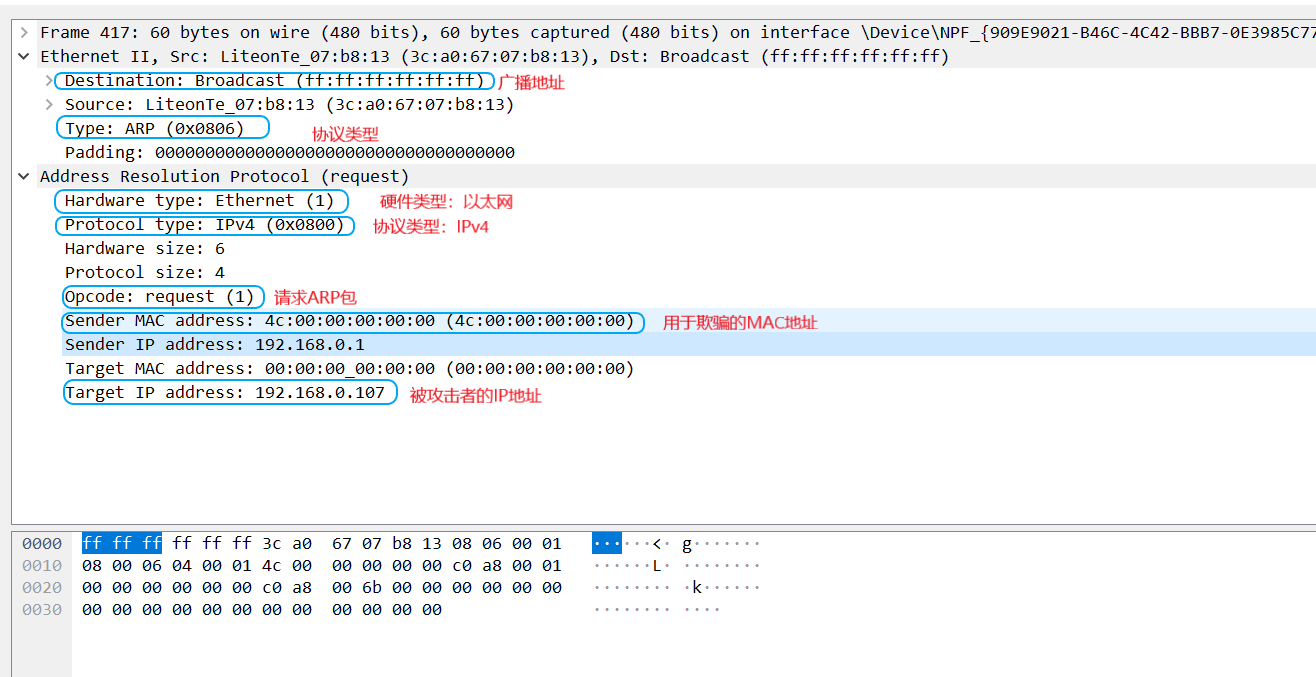
发送ARP请求包之后的ARP缓存表



此时被攻击者的电脑已经断网，通过抓包软件抓包，得到数据如下所示

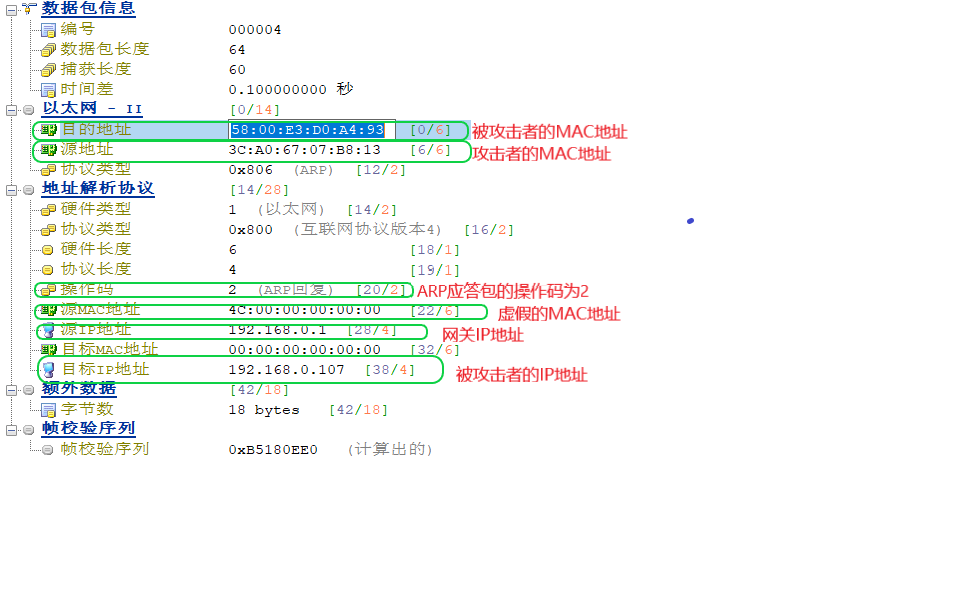


随便点一个展开如下所示：

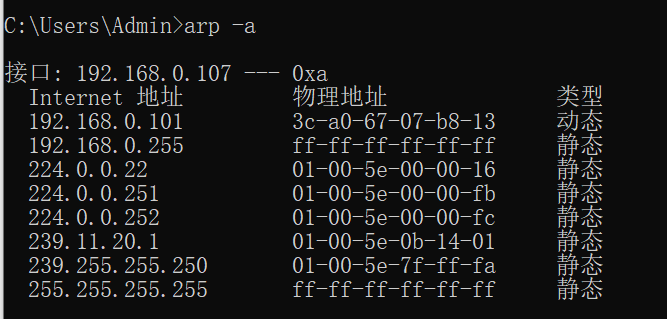


2.其次是利用科来软件生成ARP应答包，然后发送攻击对象

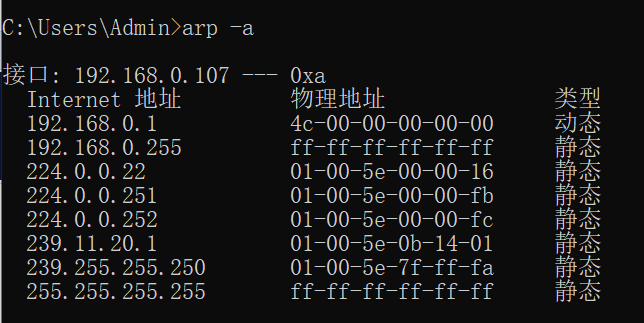
（1）ARP应答包的生成图



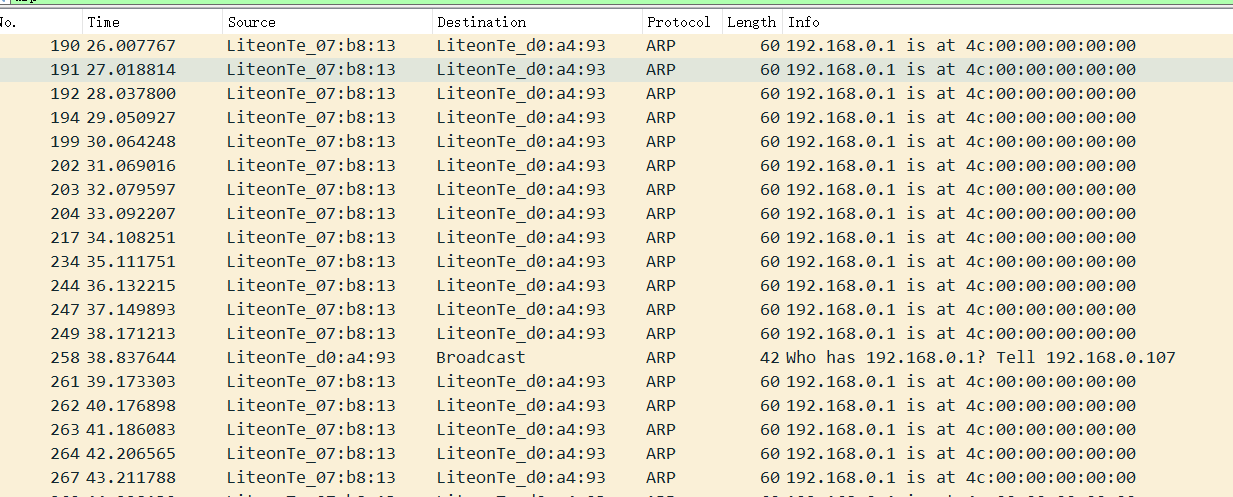
发送ARP应答包之前的ARP缓存表



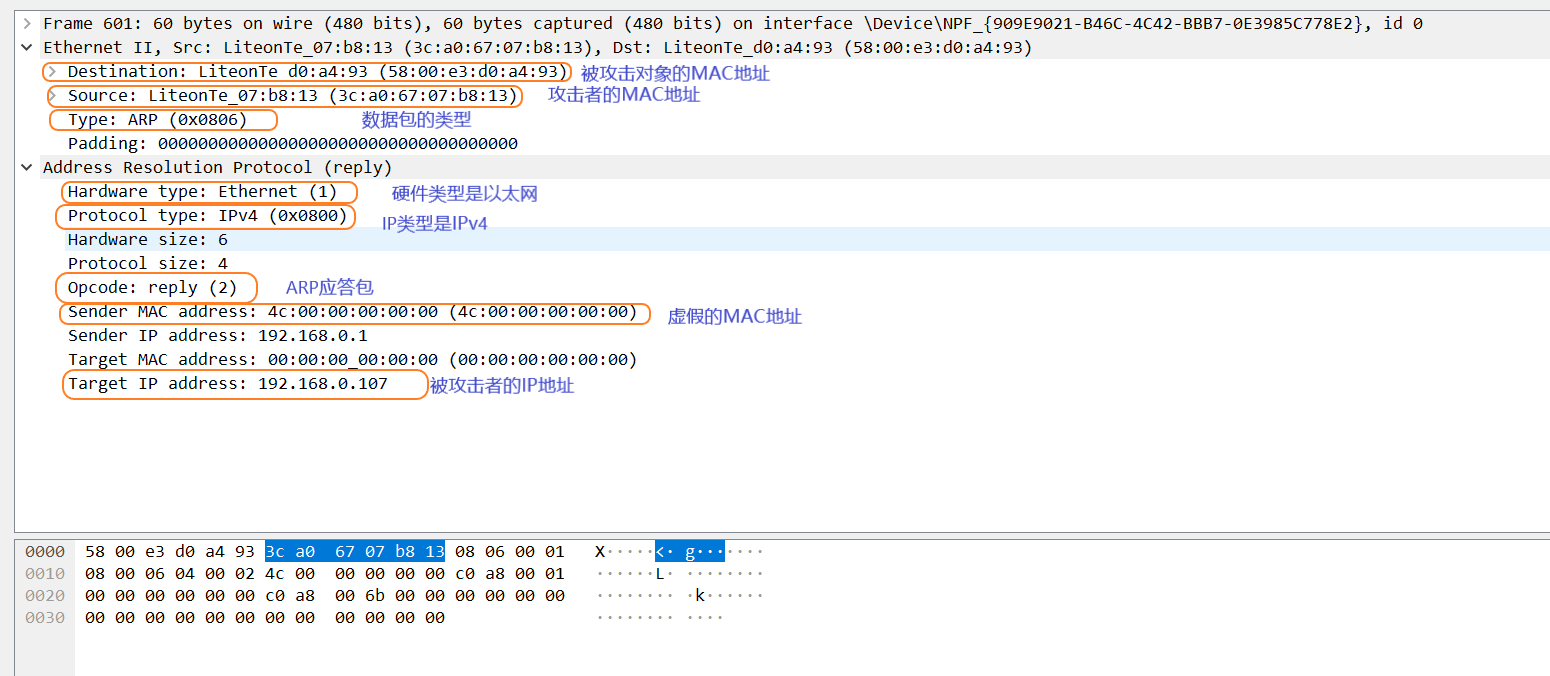
发送ARP应答包之后的ARP缓存表



此时被攻击者的电脑已经断网，用抓包软件进行抓包，得到如下所示的图：

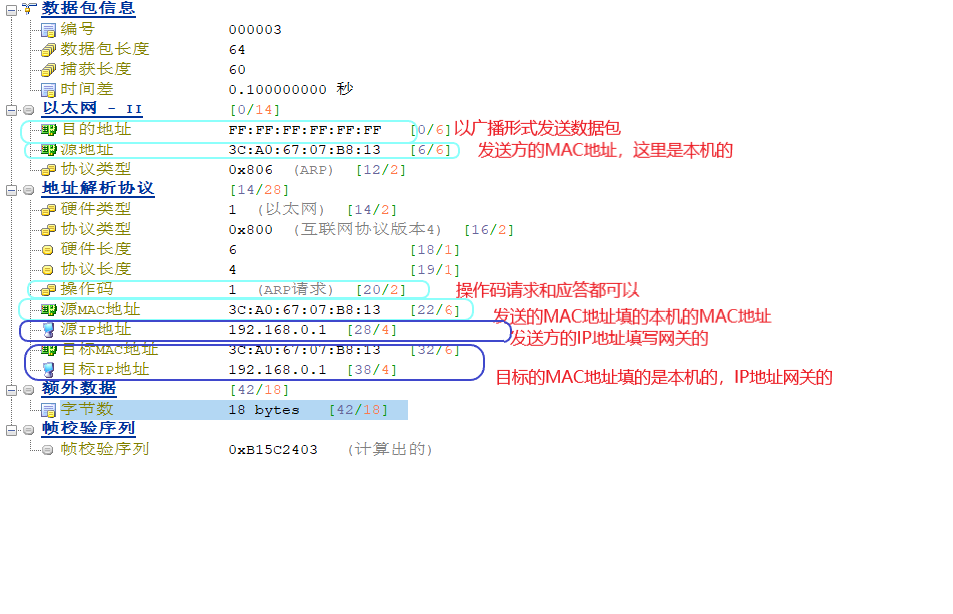


点开其中一个得到如下所示的图：

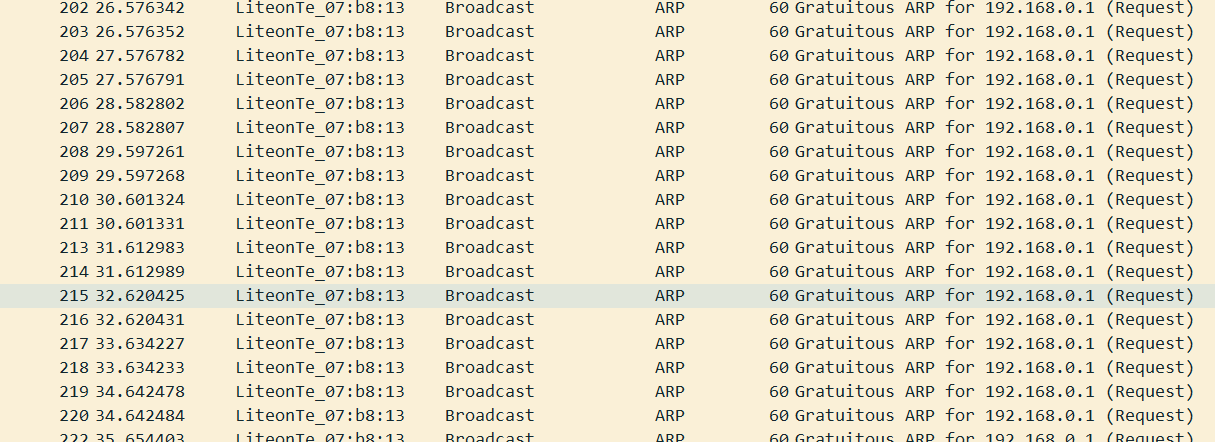


3.最后是利用科来软件生成ARP应答包，然后发送攻击对象

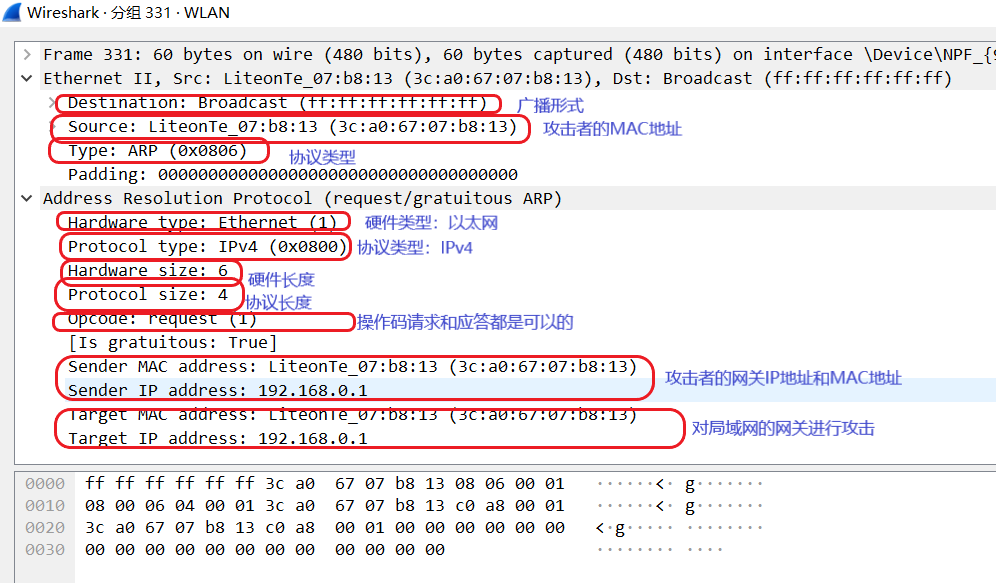
（1）ARP免费包的生成图[1][2]



源IP地址和目标IP地址之所以都是网关的，是想对整个局域网进行攻击，然后对ARP免费包进行数据抓取，得到以下数据分析



点开其中一个得到如下所示的图：



# 实验总结

1.选择的局域网最好选择实验室的网，不使用校园网。

2.再发送数据包之前提前把杀毒软件关闭掉。

3.要提前知道攻击者和被攻击者的MA地址和IP地址

# 参考文献

[1]https://www.zhihu.com/question/64514922/answer/221264172

[2]https://blog.csdn.net/ethan0ly/article/details/53793078