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

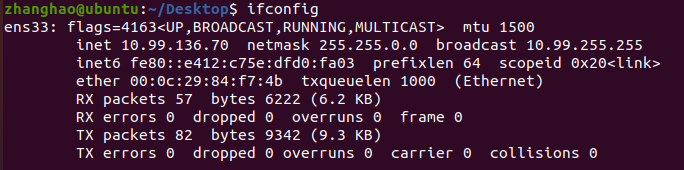
1. **实验内容**
2. 采用科来数据包生成器生成三种ARP协议数据包（请求、应答、免费(Gratuitous ARP)三种形式的ARP包；
3. 采用科来数据包播放器软件将三种伪造数据包向攻击目标机发送，检验三种形式的ARP包是否具备断网攻击能力（采用arp命令查看攻击前后的目标机ARP缓存表是否发生变化并截图说明）

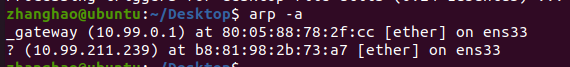
攻击主机的初始化网络设置：



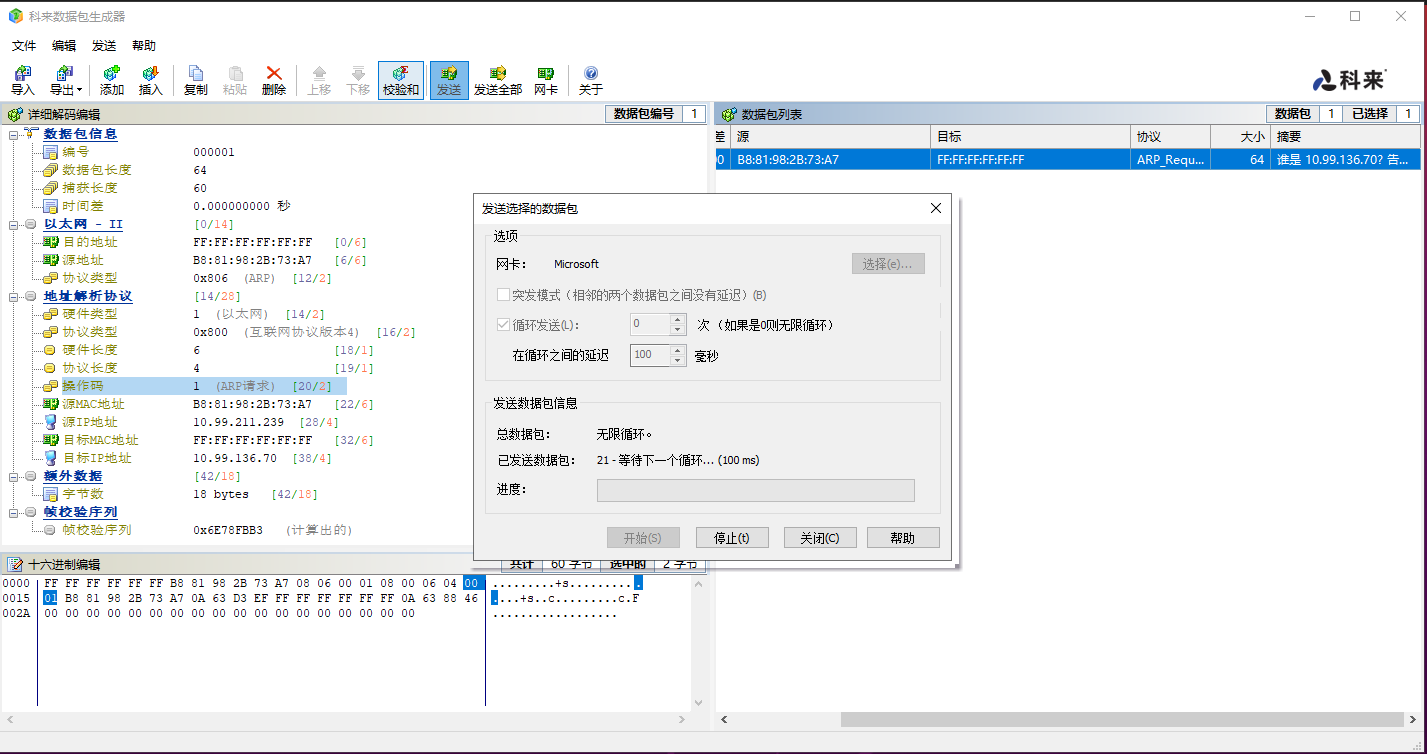


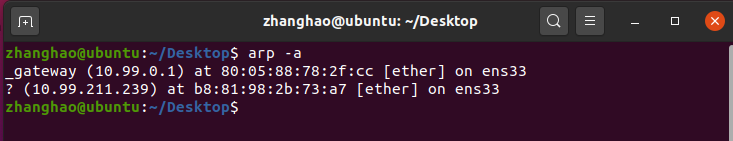
被攻击主机的初始化网络设置：





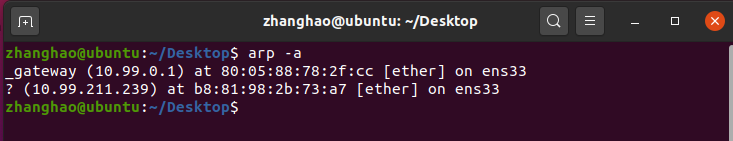
ARP请求包攻击：

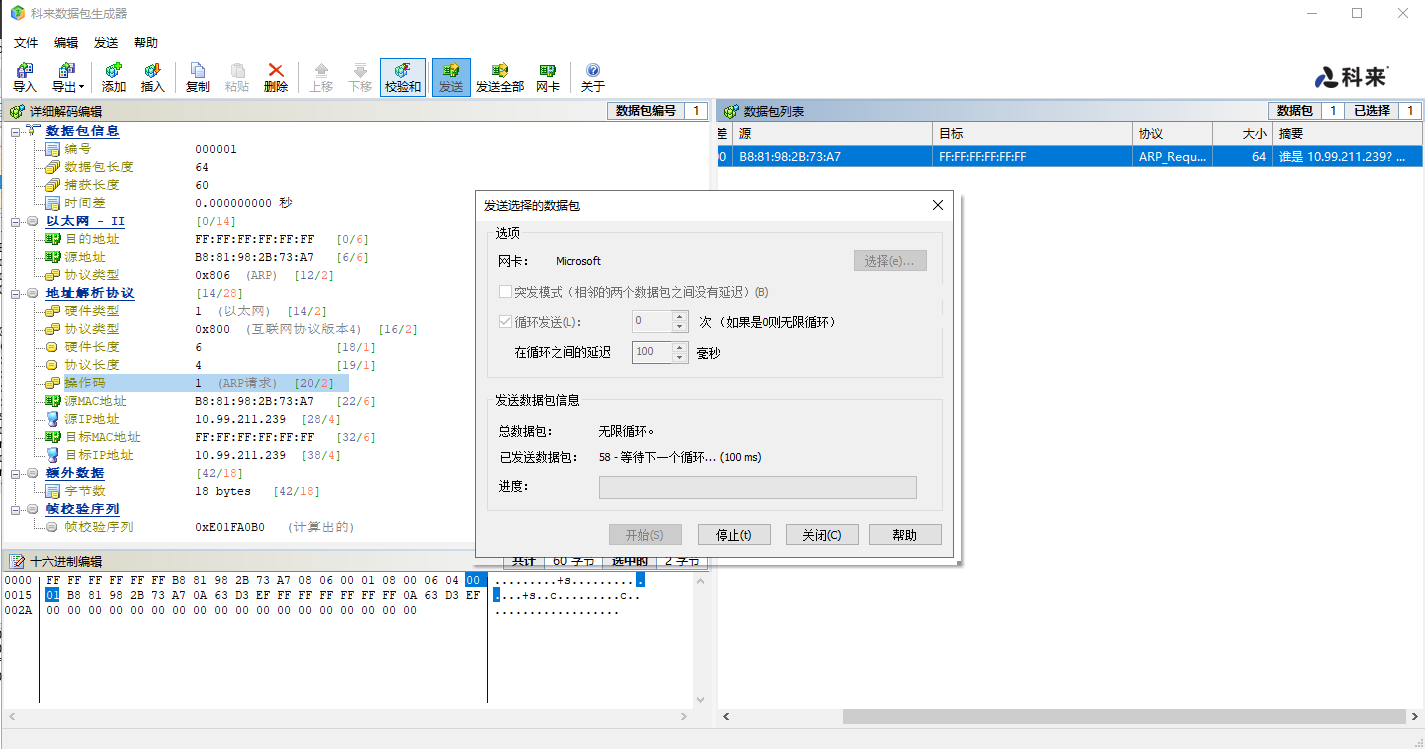




使用科来数据包生成器发送ARP请求包时间间隔为100ms，观察被攻击主机，被攻击的主机ARP缓存表中的MAC地址未发生改变，因此攻击无效。被攻击主机可以正常上网。

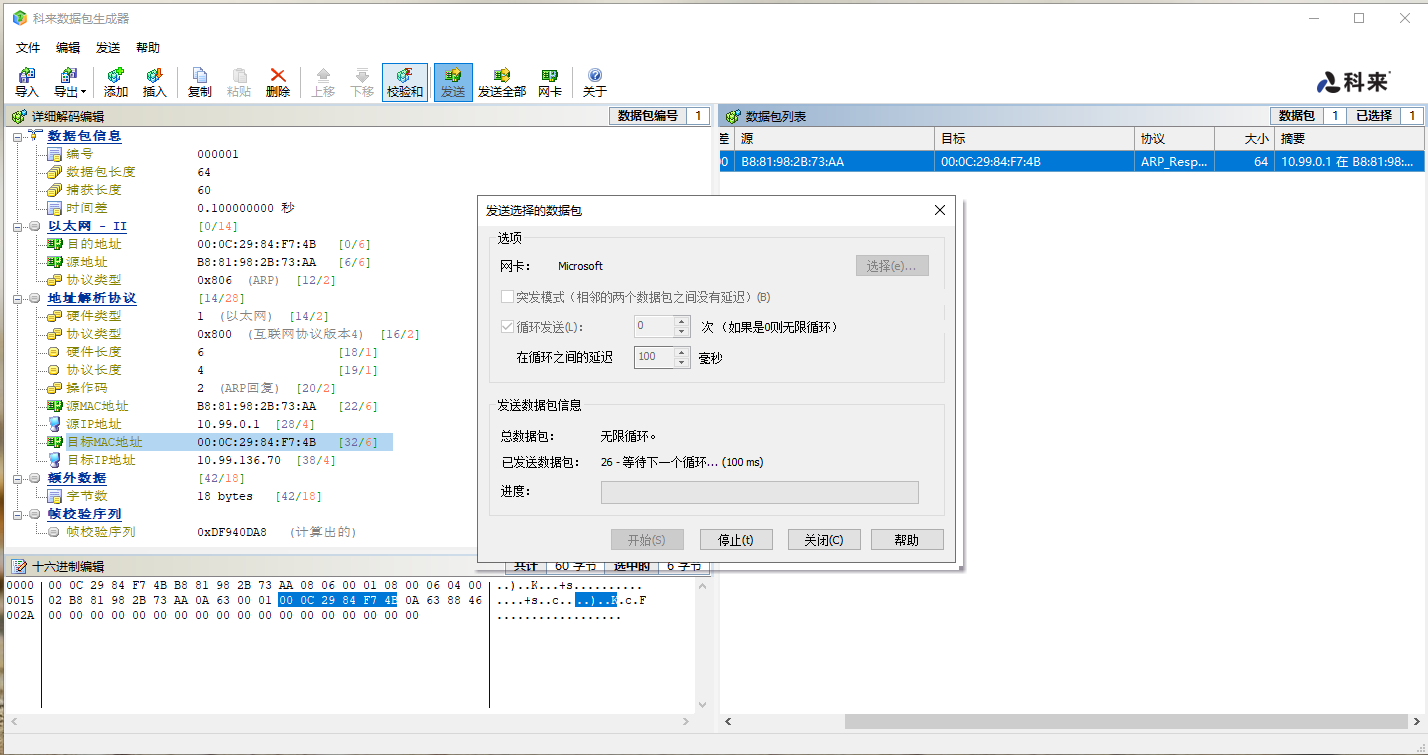
免费ARP包：

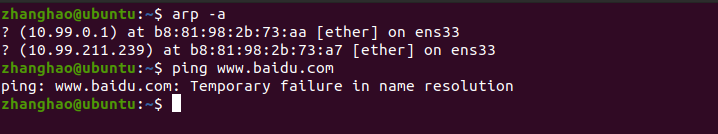




免费ARP数据包的源地址和目的地址相同，同样使用科来数据包发送，时间间隔为100ms，观察被攻击主机的ARP缓存表依然保持不变，故攻击无效。

ARP回复包：

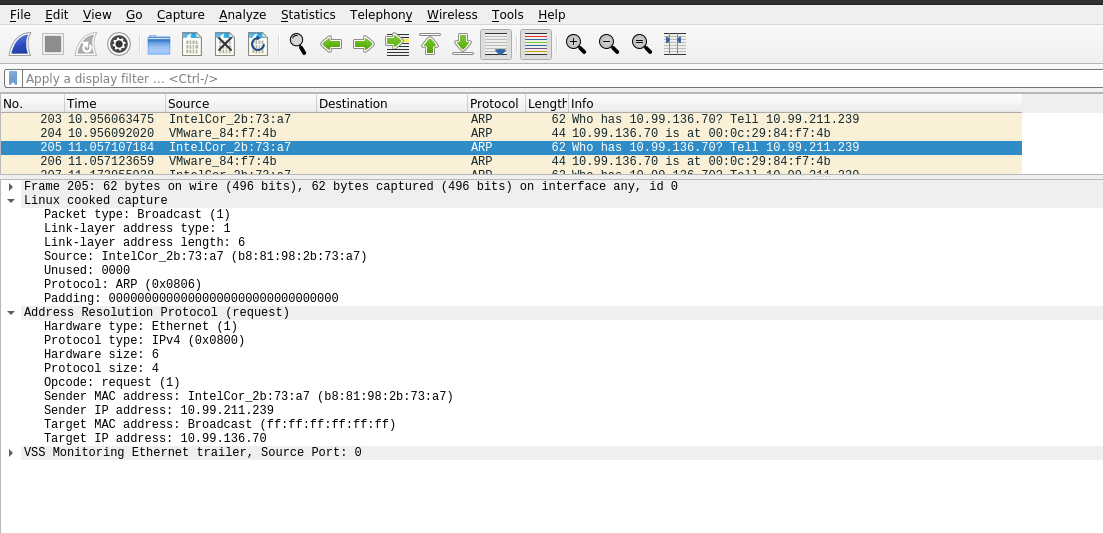




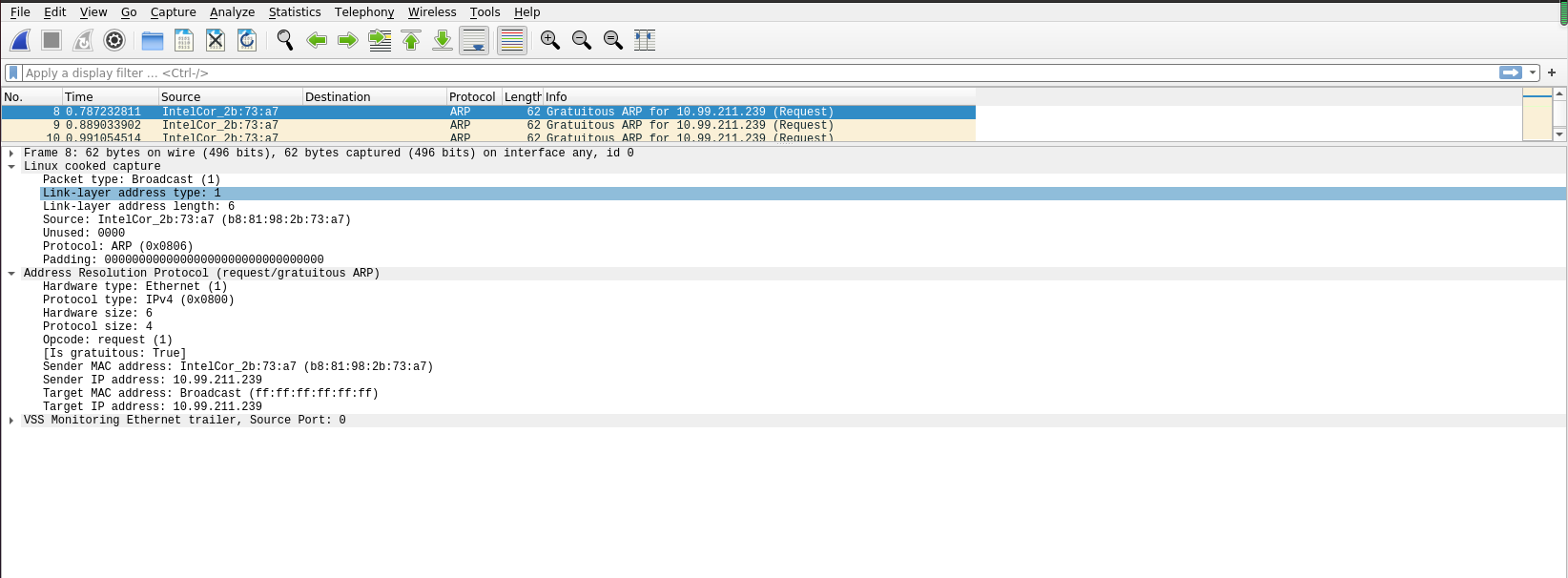
将源地址更改为网关地址，源MAC地址填写一个错误的地址，使用科来数据包进行发送，观察被攻击主机的ARP缓存表，发现网关的MAC地址变为填写的错误地址。尝试PING百度，则出现域名解析失败，攻击成功。

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；

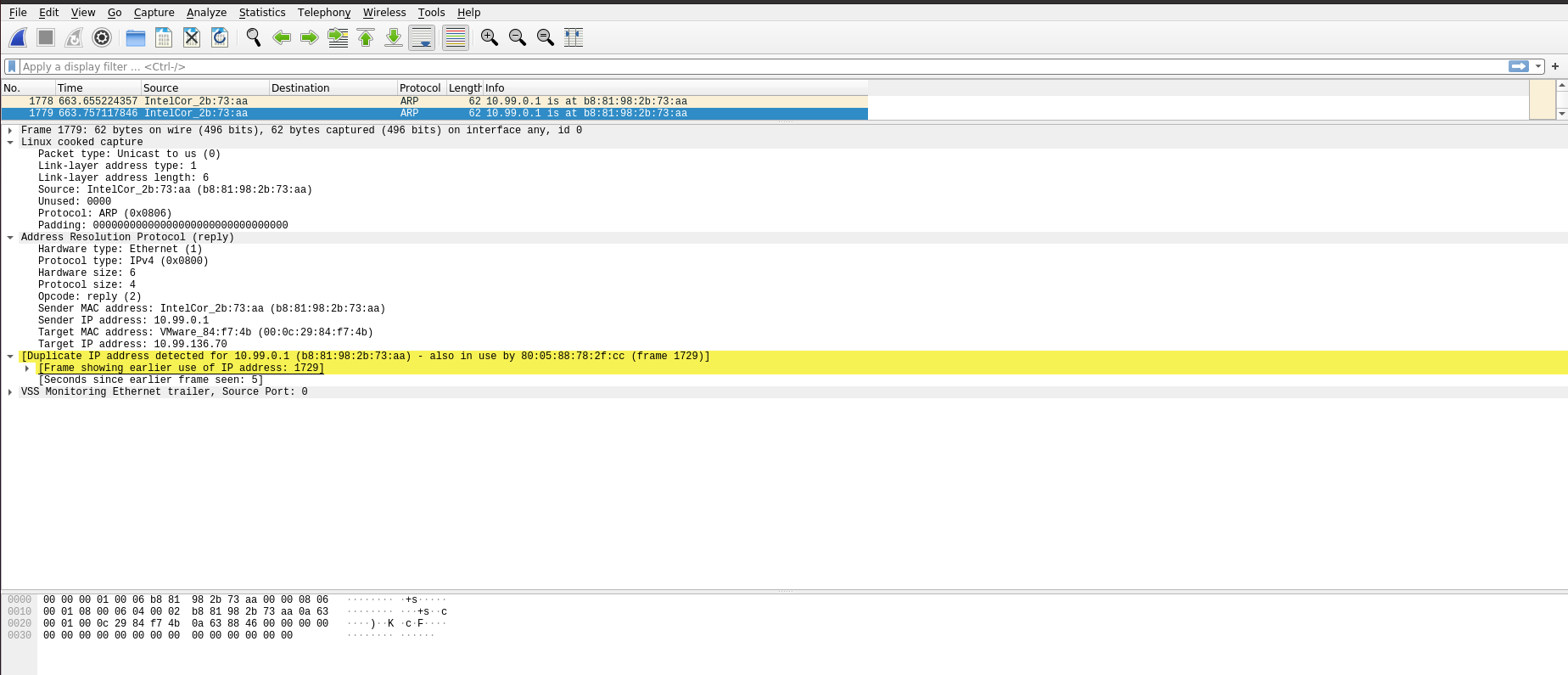
ARP请求：



免费ARP包：



ARP回复包：



D、针对ARP攻击，如何进行防护，请提出自己的意见和建议。

参考文献：

# ARP 断网攻击的原理是什么？如何完全防护？https://www.zhihu.com/question/20338649