信息安全课程实验二

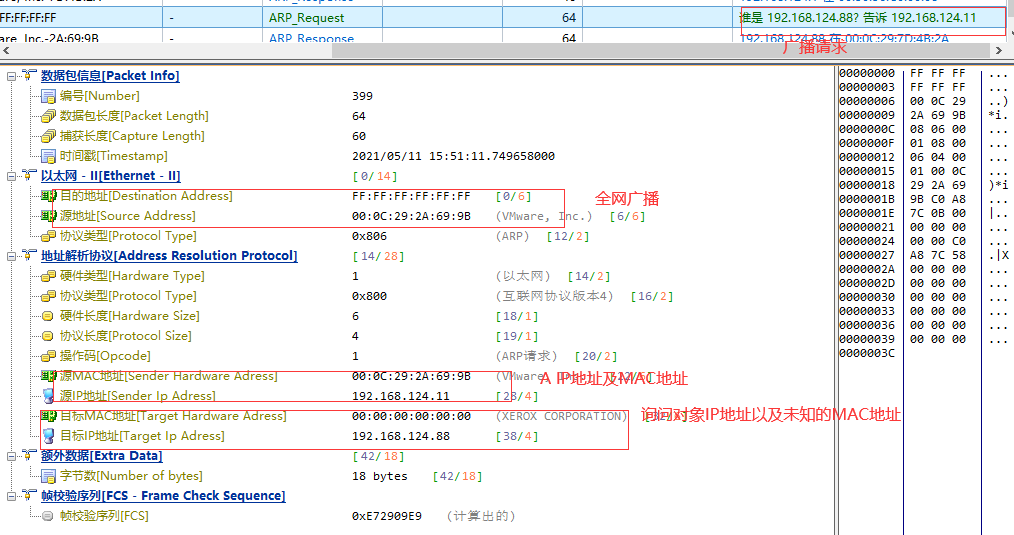
1. **实验目的**

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；

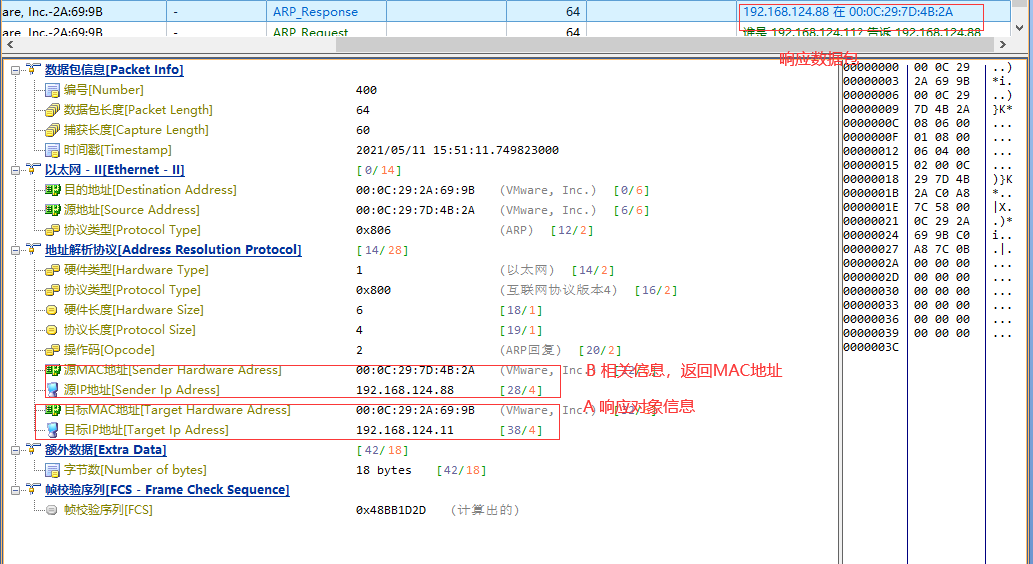
1. **实验工具**

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

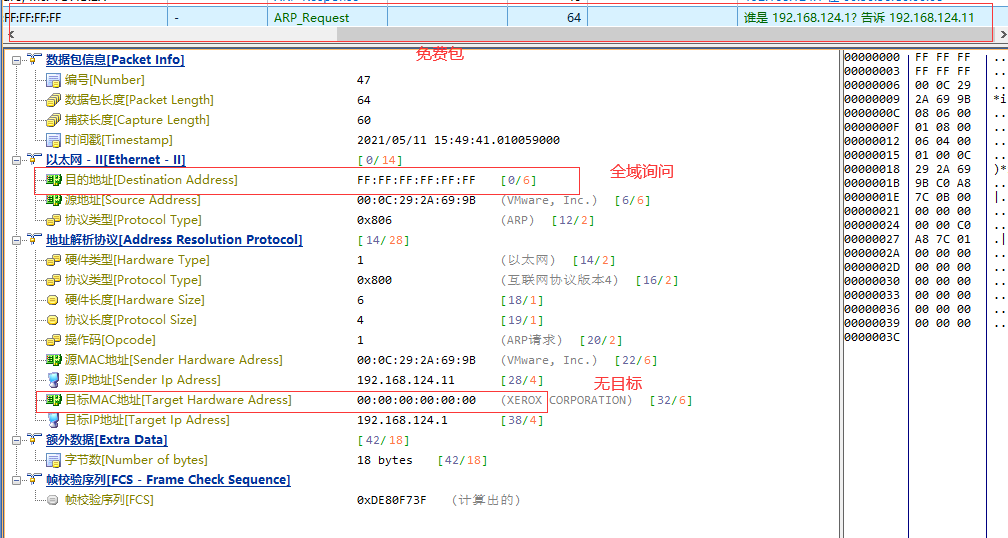
1. **实验内容**
2. 采用科来数据包生成器生成三种ARP协议数据包（请求、应答、免费(Gratuitous ARP)三种形式的ARP包：
3. 请求包



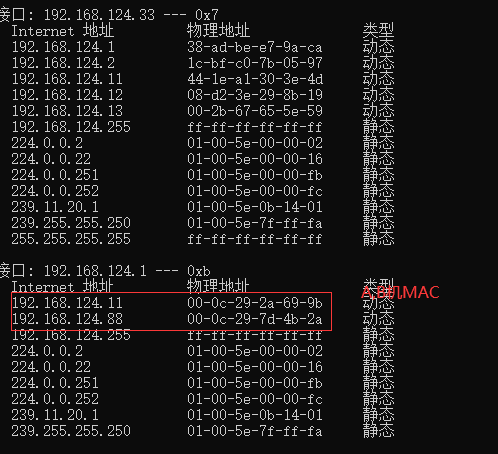
1. 应答包



1. 免费包



1. 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）
2. 攻击前ARP缓存表信息



1. 请求包伪造数据



修改后A机对应MAC地址在B ARP缓存中已更改



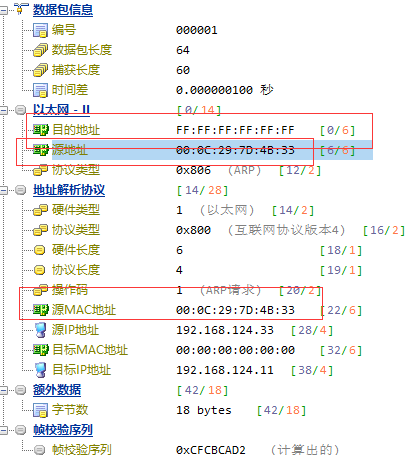
1. 响应包伪造数据



修改后B机对应MAC地址在A ARP缓存中已更改



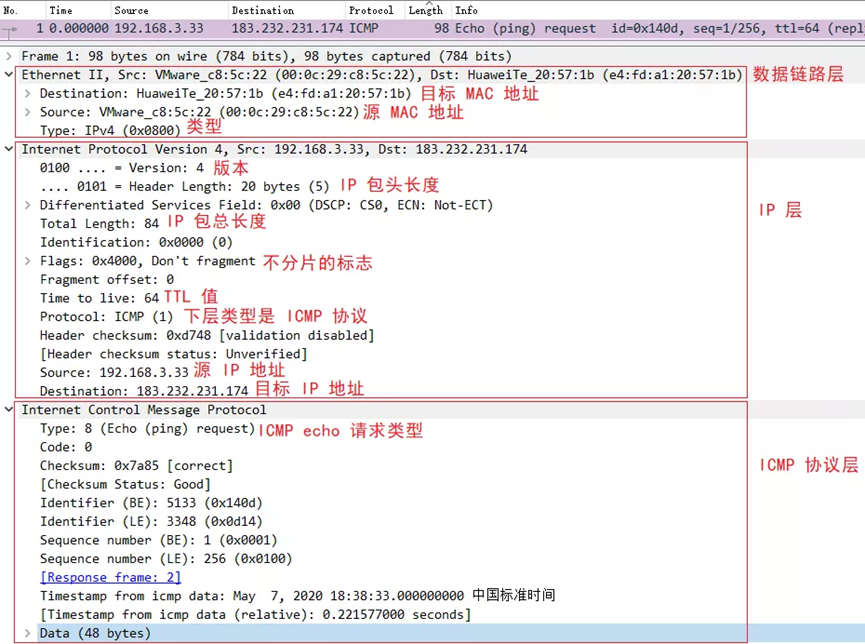
1. 免费包伪造数据



缓存修改：



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；



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。