信息安全课程实验二

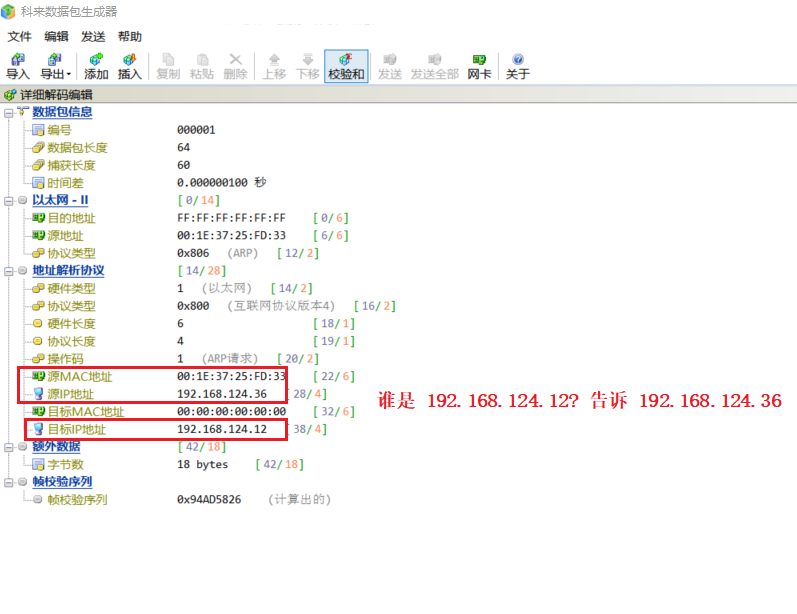
1. **实验目的**

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；

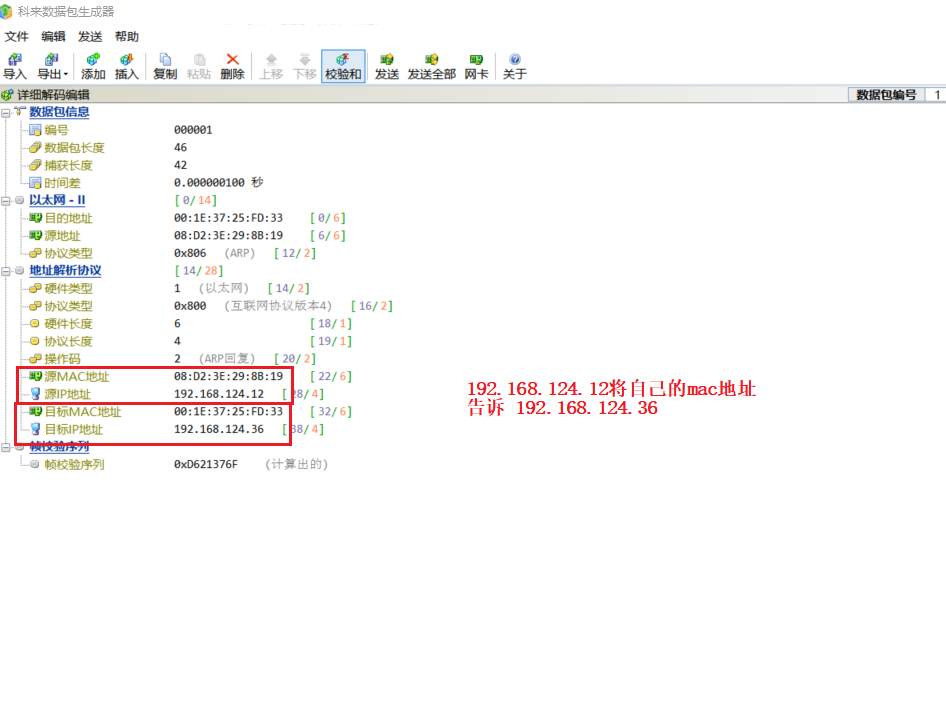
1. **实验工具**

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

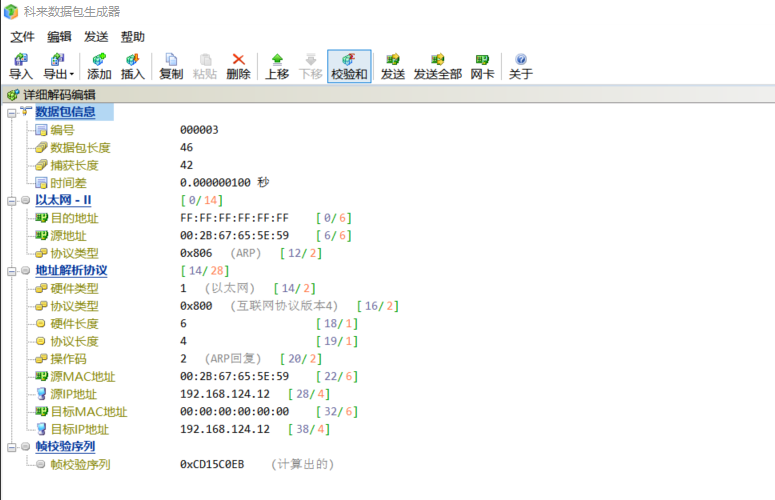
1. **实验内容**
2. 使用科来数据包生成器生成ARP协议数据包
3. 请求包



1. 响应包



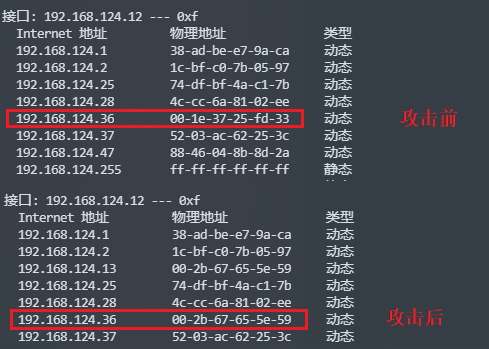
1. 免费包



1. 使用科来数据包生成器伪造数据包并攻击
2. 伪造请求包

192.168.124.36 发送ARP请求包查询192.168.124.12的mac地址，伪造这个请求包，并将请求方的mac地址改为其他，并发送。则需要响应方(192.168.124.12)的ARP缓存会不正确，不能将ARP响应包发送到192.168.124.36，以至于双方不能正常通信，从而达到断网攻击。

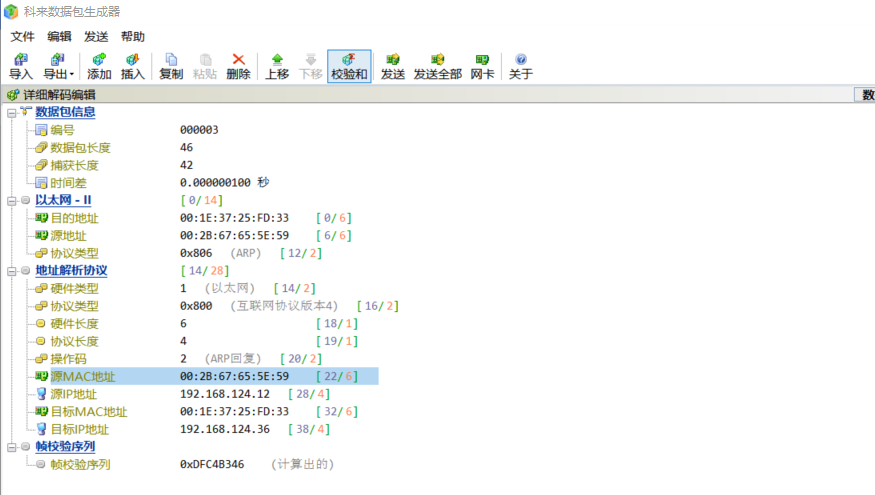


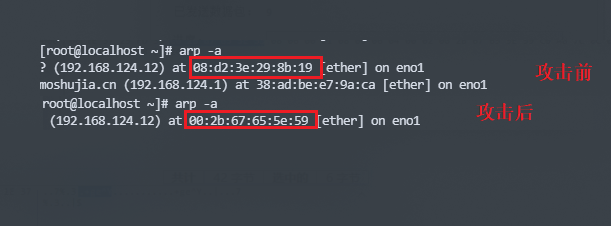


可以看到需要响应方的ARP缓存发生了变化。

1. 伪造响应包

192.168.124.36 发送ARP请求包查询192.168.124.12的mac地址。192.168.124.12需要发送一个响应包告诉自己的mac地址。伪造这个响应包，并将响应包中192.168.124.12的mac地址改为攻击者的mac地址，并发送。则需要192.168.124.36会收到一个错误的mac地址，从而达到窃听或者断网攻击。

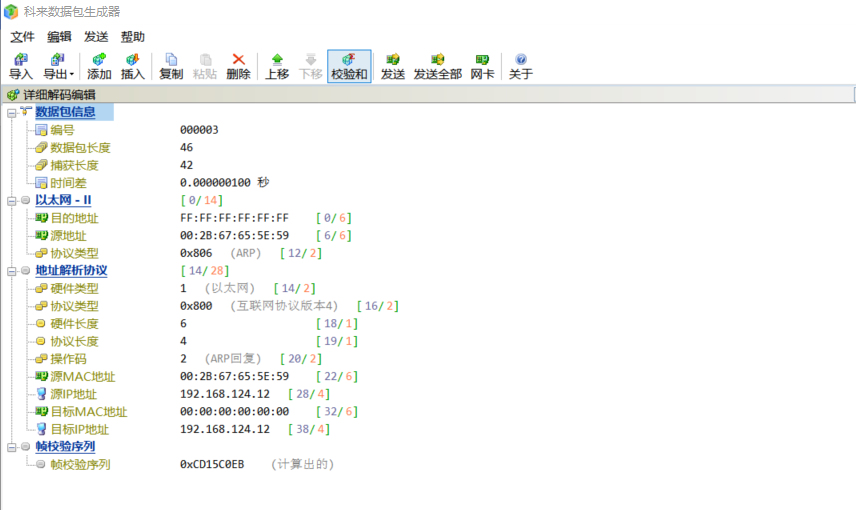


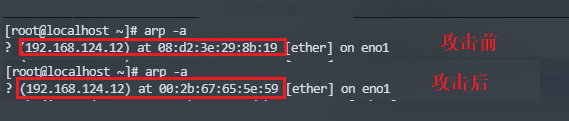


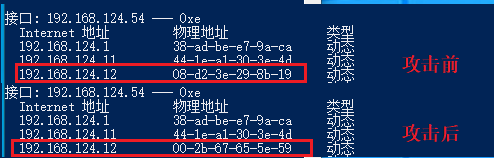
可以看到变成了攻击者的mac地址。

1. 伪造免费包

攻击者发送ARP免费包，数据包中的地址192.168.124.12但是mac地址是攻击者的mac地址，并不断发送，就可以使其他主机的ARP缓存发生变化，可以使攻击者伪装成被攻击者，可以接收到被攻击者收到的数据，从而达到窃听或者断网攻击，与响应包不同的是全局发送，影响更广。

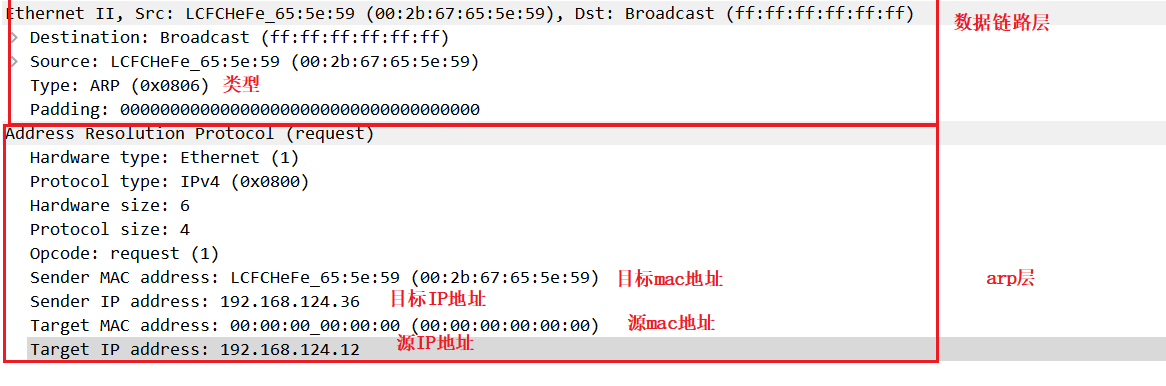




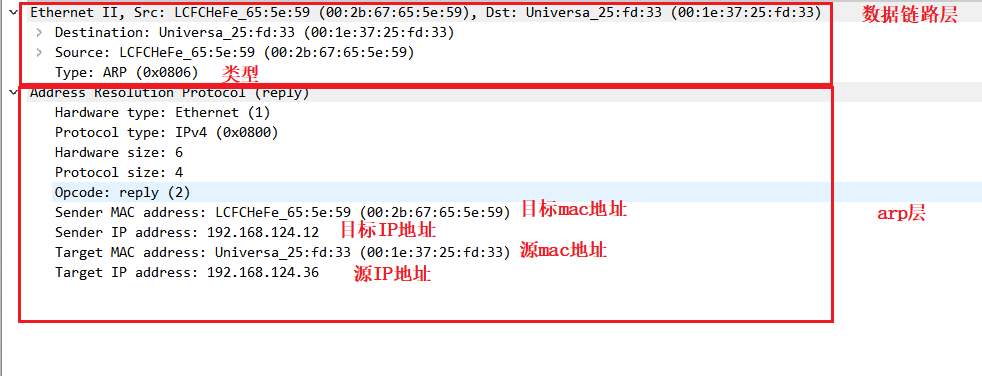


可以看到多台主机的ARP缓存都收到了影响。

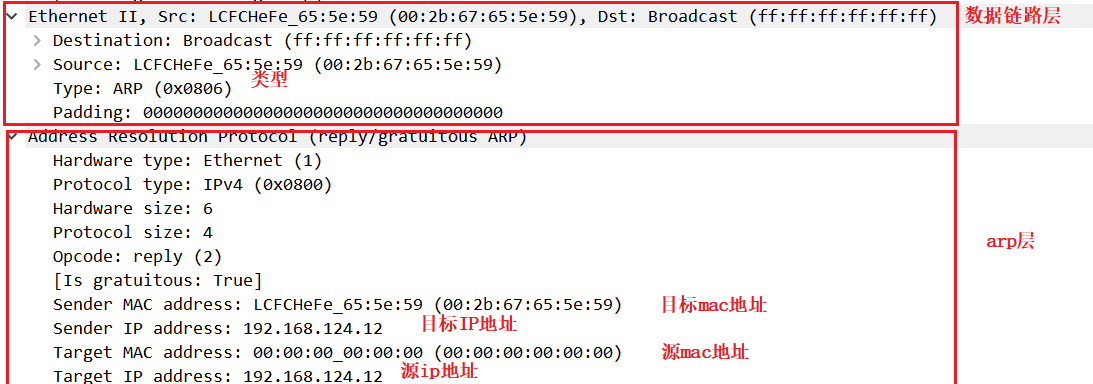
1. 协议分析和标注
2. 请求包



1. 响应包



1. 免费包



1. 针对ARP攻击的防护

可以运用静态的ARP来绑定正确的MAC地址。可以提前录入MAC地址或者使用一些ARP防御的安全软件。

1. **实验总结**

通过此次ARP协议分析和ARP攻击实验，学习了ARP协议的原理和wireshark抓包、数据包生成器、数据包广播器等工具的使用。也了解到了ARP攻击的危害。