**实 验 报 告**

实验名称： arp攻击

课程名称： 网络信息安全

学院： 信息学院

学号：202030504193

姓名： 张碧洪

实验日期：2021.5.7

浙江理工大学

目录

[一. 实验目的 3](#_Toc71398740)

[二. 实验工具 3](#_Toc71398741)

[三. 实验内容 3](#_Toc71398742)

[1. arp数据包格式 3](#_Toc71398743)

[2. 三种arp数据包攻击 4](#_Toc71398744)

[1) Arp请求包攻击 4](#_Toc71398745)

[2）Arp免费包攻击 4](#_Toc71398746)

[3）Arp响应包 4](#_Toc71398747)

[3. Wireshark抓包分析 4](#_Toc71398748)

[4. arp攻击的防范 4](#_Toc71398749)

[5. 参考文献 4](#_Toc71398750)

# 实验目的

学习虚拟机的安装，版本控制软件Git，收发包以及抓包软件的使用。并且了解arp协议，以及arp三种数据包的内容。

# 实验工具

Ubuntu系统，window10系统，GitHub，科来数据包生成器，Wireshark抓包软件。

# 实验内容

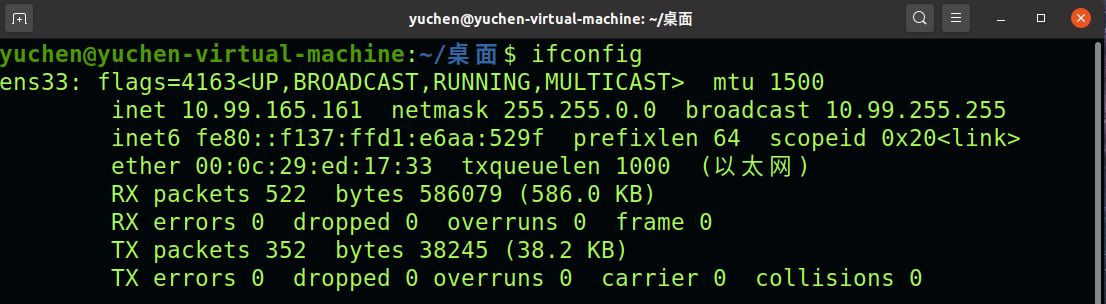
## arp数据包格式



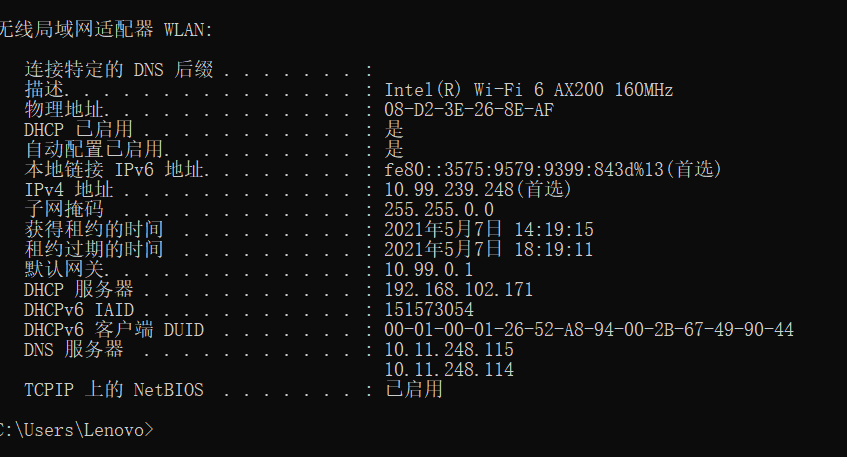
我们主要通过操作码来控制arp数据包的类型，1代表arp请求包，2代表arp应答包。Arp请求包一般不知道目的主机的Mac地址时我们一般都填写FF:FF:FF:FF:FF:FF.而对于免费arp包来说目的地址和源地址都填写自己的本机的即可。详细的数据包文件已经上传GitHub。

## 三种arp数据包攻击

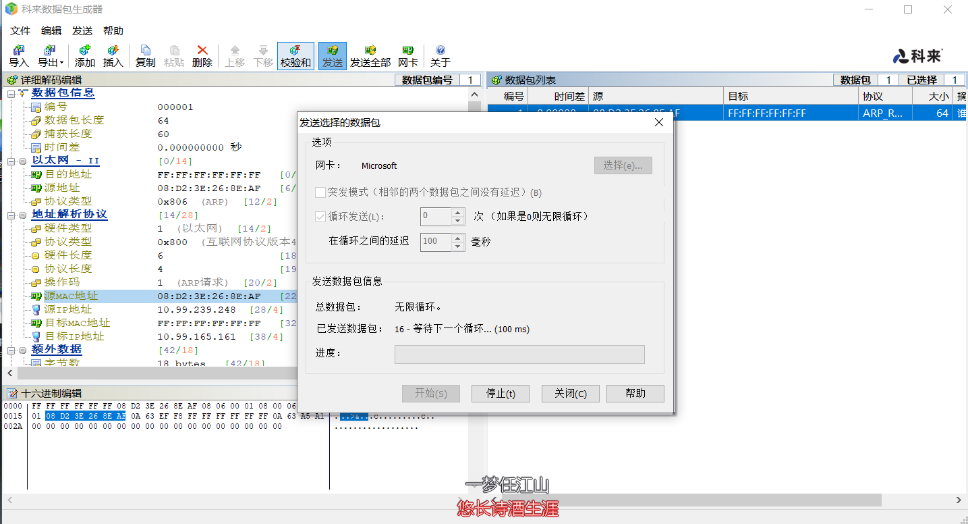
**被攻击主机：**

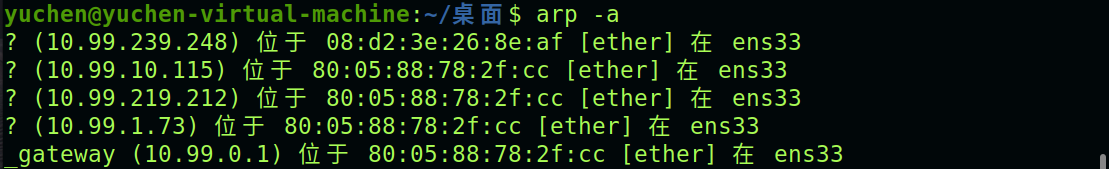


**攻击主机：**



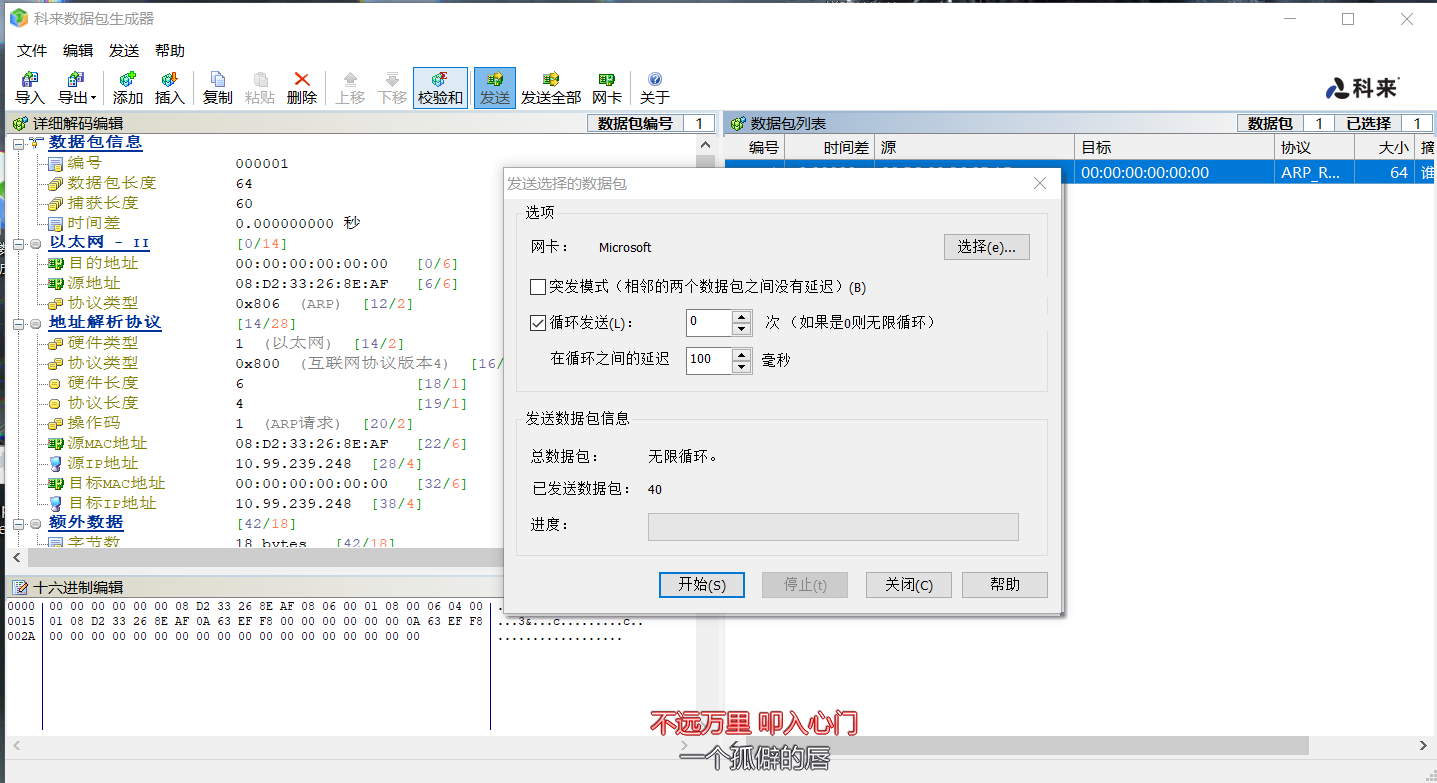
### Arp请求包攻击

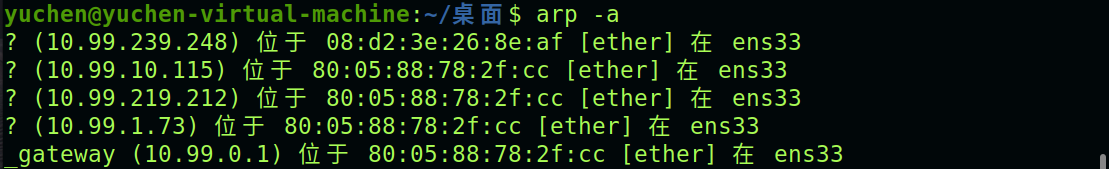


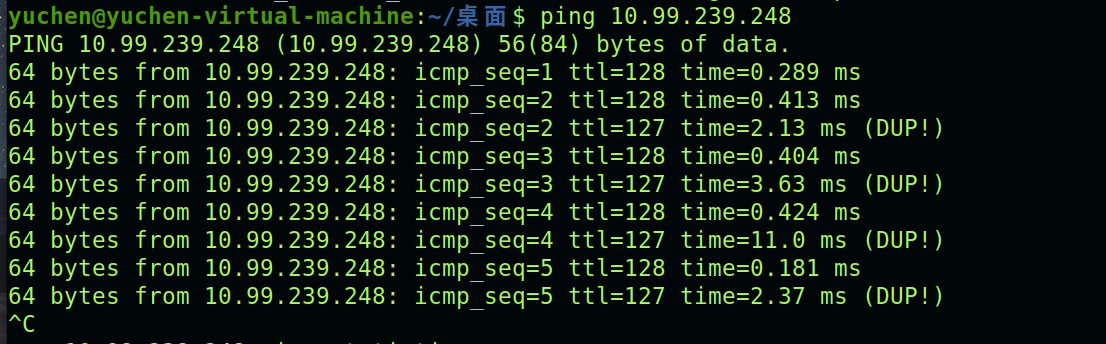


我们讲数据包调整成无线循环，并将时间间隔调整为100毫秒，进行发送。我们将源IP地址设置为被攻击者的IP，源Mac地址设置为一个错误的mac地址。观察被攻击者的arp缓存表并未发生变化。因此攻击无效。

### 2）Arp免费包攻击

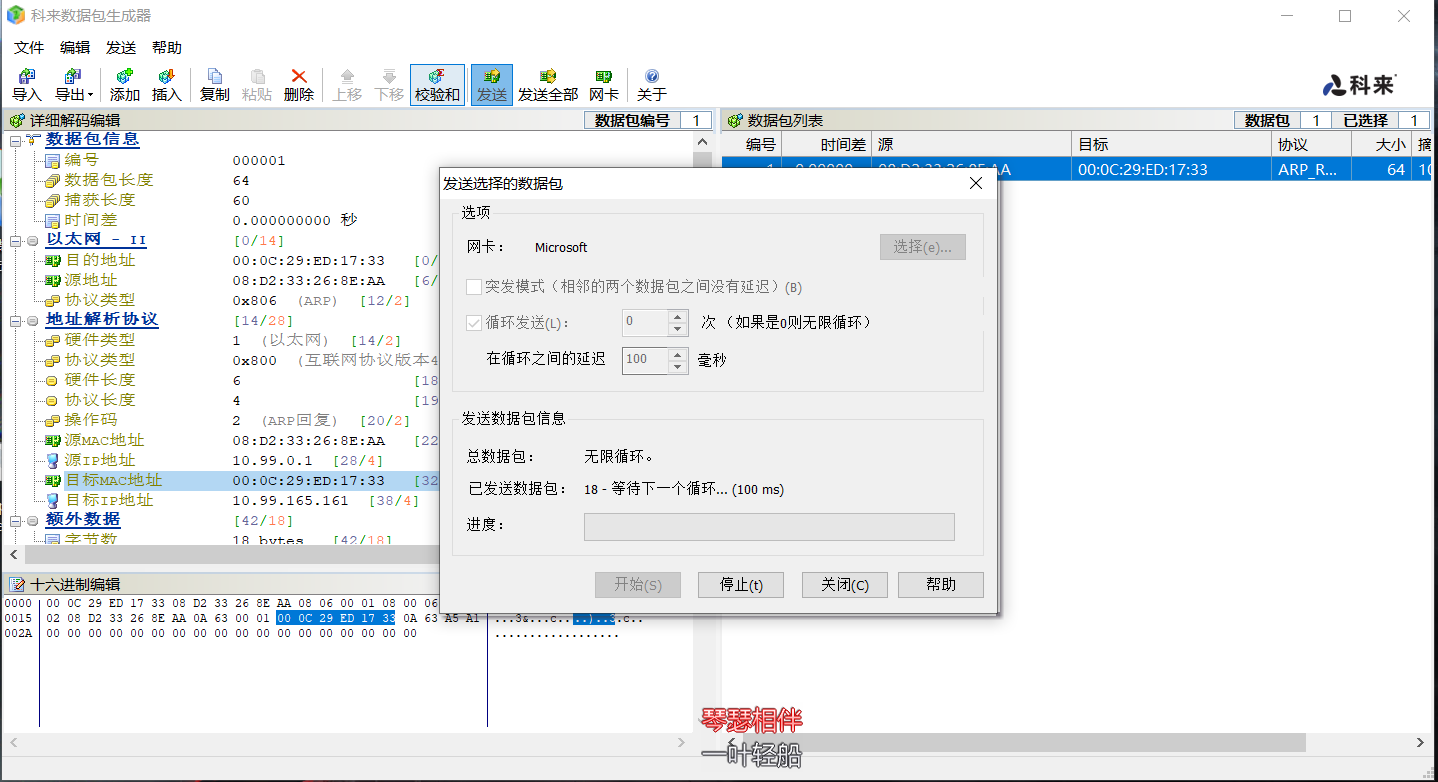


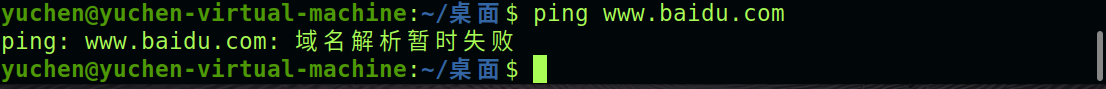


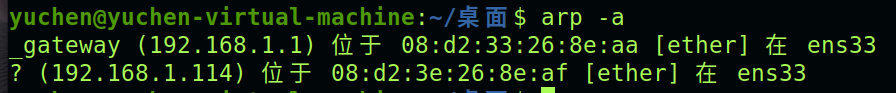


我在攻击主机上构建并发送免费arp包，其中源IP以及目的IP都设置为攻击主机的IP地址。当时源mac地址设置为错误的mac的地址，并在局域网中发送。然后观察被攻击主机的arp缓存表，发现并没有改变。并且被攻击主机依旧能和攻击主机保持通信。

### 3）Arp响应包

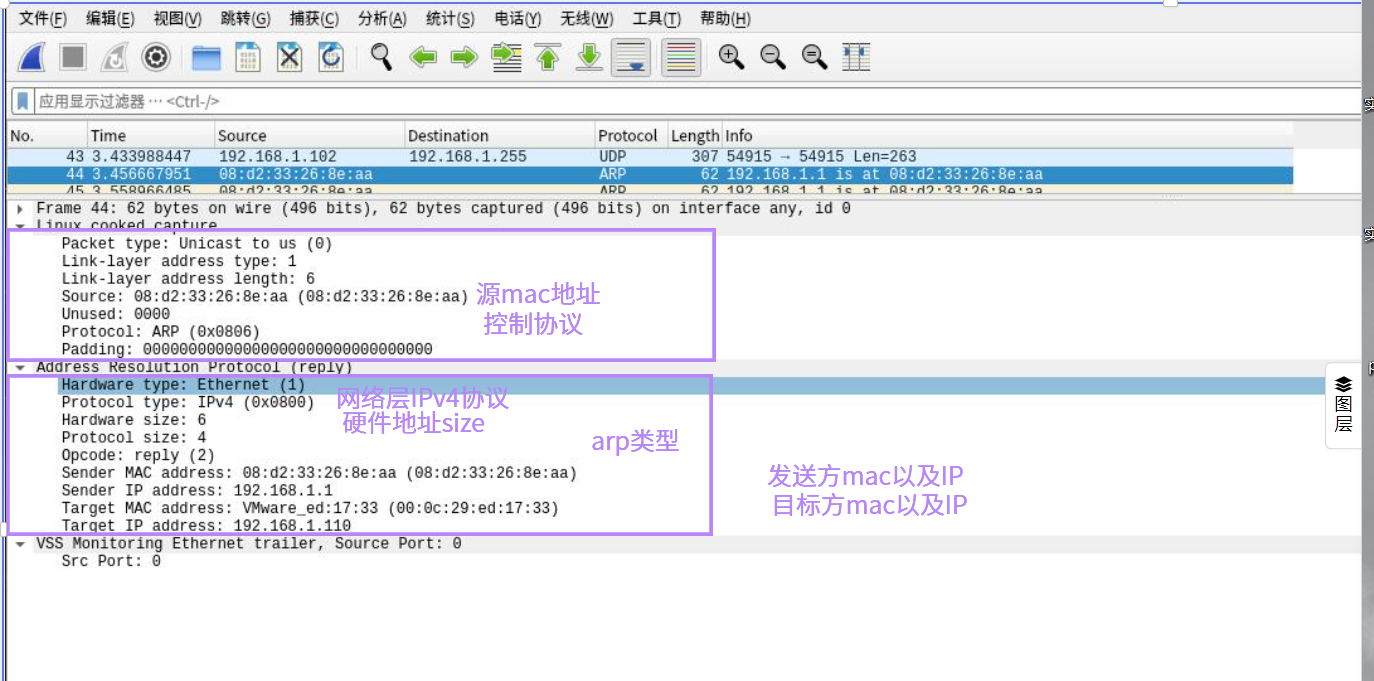






我们在进行构建arp响应包的时候源IP地址填成网关地址，源mac地址随便填一个错误的。目标IP地址以及目标mac地址填被攻击主机的IP地址以及mac地址。可以看到域名解析失败。并且查看arp缓存表发现，网关的mac地址变成我们填写的错误mac地址。

## Wireshark抓包分析



## arp攻击的防范

可以在客户端设置静态的ARP映射表，这样就不会受到ARP的欺骗；也可以在交换机上设置访问控制，对于所有流经交换机但IP地址和MAC地址与网关不匹配的情况进行过滤，从而避免了ARP的攻击。

## 参考文献

1. arp数据包 https://blog.csdn.net/zzsfqiuyigui/article/details/8965154.