**信息安全技术实验报告**

|  |  |  |
| --- | --- | --- |
| **实验名称** | **计算机网络基础及常用工具** | |
| **组长** | **姓名** | **学号** |
| 李骏豪 | 21307259 |
| **组员** | 李骏豪 | 21307259 |
| 梁铭恩 | 21307360 |
| 叶梓聪 | 21307417 |
| **实验分工** | | |
| **姓名** | **任务** | |
| 李骏豪 | 完成了实验2及报告 | |
| 梁铭恩 | 完成了实验3及报告 | |
| 叶梓聪 | 完成了实验1及报告 | |

表1-1 实验中的节点名称、用户名及密码



【**交报告**】使用FTP方式提交，推荐使用Filezilla客户端

地址为ftp://ftp.network-security.asia；账号与密码为：student/5ecur1ty

文件以组号（组长学号）+实验名称命名

# 实验目的

1. 通过分析网络流量理解交换机、路由器等工作原理，理解子网划分和子网掩码，进一步理解网络原理，为学习以后的章节准备基础知识；
2. 熟练使用tcpdump、wireshark等流量分析工具进行网络流量分析，掌握Scapy的用法，能够使用scapy构造常见的协议数据包，为进行后面章节的实验准备基本的操作技能。

# 实验任务

## 实验1：使用tcpdump分析ICMP流量

1. 登录Client，查看当前的网络接口、可监听的网卡、查看ARP缓存列表
2. 用tcpdump 监听端口eth0，观察所有流量
3. 在client上打开另一个终端窗口，对Internal Server执行ping操作。分析tcpdump 观察到的相关流量，分析涉及到的ARP请求、ARP响应、ICMP ECHO请求、ICMP ECHO响应，记录每个包的源MAC地址、目标MAC地址、源IP地址、目标IP地址，填写表1-2子网内。
4. 同上述步骤（2），用tcpdump 监听网络；
5. 在Client上对External Server执行ping操作。 观察tcpdump 监听到的网络流量，分析涉及到的ARP请求、ARP响应、ICMP ECHO请求、ICMP ECHO响应，记录每个包的源MAC地址、目标MAC地址、源IP地址、目标IP地址。填写表1-2跨子网。
6. 清空 Client上的ARP缓存
7. 将Client的子网掩码修改为28
8. 在把Client网卡eth0的子网掩码故意配错的情况下，分析ICMP的流量， 重复上面步骤（2）、（3），填写表1-2掩码错。
9. 对应记录的表格信息，分析三次操作的结果有什么不同？为什么这样？

表1-2  流量分析记录表

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 操作 | ARP请求 | | ARP响应 | | ICMP ECHO请求 | | ICMP ECHO 响应 | |
| 源MAC | 目标MAC | 源MAC | 目标MAC | 源IP | 目标IP | 源IP | 目标 |
| 子网内 |  |  |  |  |  |  |  |  |
| 跨子网 |  |  |  |  |  |  |  |  |
| 掩码错 |  |  |  |  |  |  |  |  |

## 实验2：使用wireshark分析Web访问过程流量

1. 在Client上先运行wireshark，选择监听以太网网卡eth0的所有流量；
2. 在Client 上通过浏览器访问 www.imool.com.cn网站，然后关闭浏览器；
3. 根据wireshark中捕获到的流量，解释从访问www.imool.com.cn到关闭浏览器整个过程中Client主机都发生了哪些网络活动，回答以下问题：
4. 域名解析过程涉及哪些IP包，请求和响应分别是什么？
5. ARP解析过程中，网关的MAC地址是什么？
6. Client和www.imool.com.cn的连接建立过程、连接拆除过程；
7. 使用Wireshark的协议流追踪功能，提取Web访问的Cookie信息。

## 实验3：使用Scapy构造ICMP Echo Request数据包

Attacker机器提供Scapy工具，可通过Scapy交互式界面或在python脚本中导入Scapy库的方式进行操作。

1. 在Attacker命令行终端中启动Scapy交互式界面;
2. 创建IP层，将源ip（src）设置为Client ip，将目的ip（dst）设置成External Server ip；
3. 创建ICMP层；
4. 创建负载数据；
5. 将IP层、ICMP层、负载三者进行组合生成数据包；
6. 通过.show()方法来查看已构造好的数据包内容
7. 将构造好的数据包发送出去
8. 在Client上捕获从External Server发送来的ICMP Echo reply包，证明Attacker伪造ICMP Echo request数据包成功

**【实验要求】**

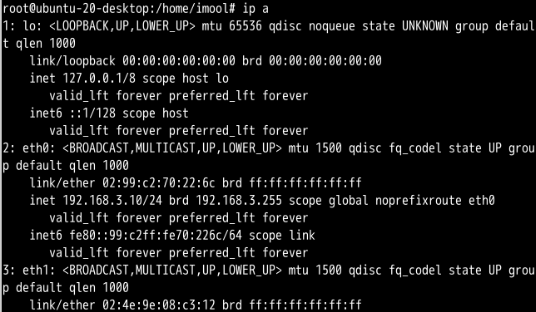
重要信息信息请给出截图。

# 实验步骤与实验结果记录

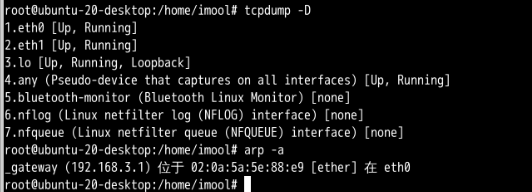
实验1：使用tcpdump分析ICMP流量

（1）

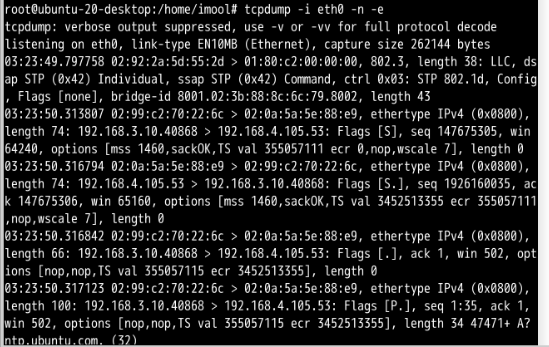
查看当前的网络接口



查看可监听的网卡和ARP缓存列表

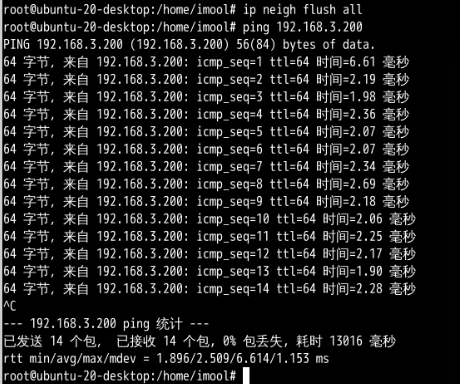


（2）用tcpdump监听端口th0，观察所有流量

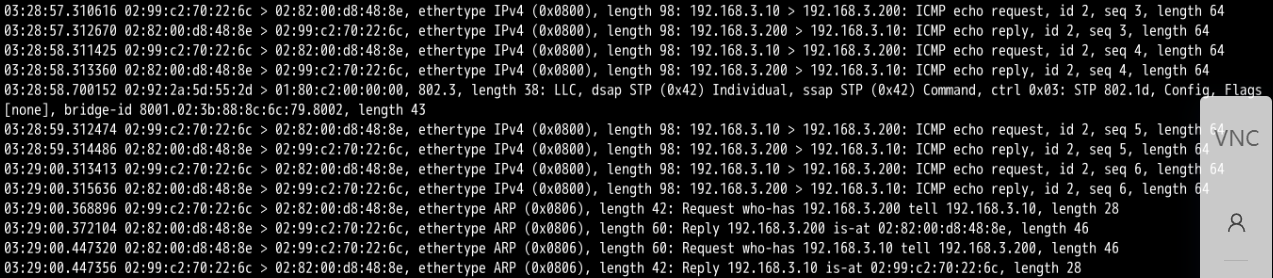


（3）

Client端ping Internet Server

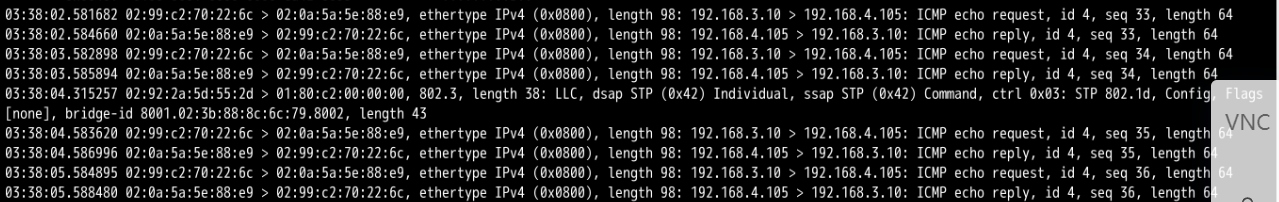


Tcpdump观察相关流量



1. 、（5）tcpdump监听网络，client端对external server执行ping 操作

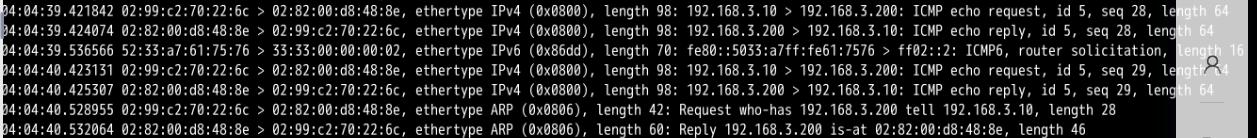




（8）

Client修改子网掩码后重复（2）、（3）

Tcpdump监控流量截图



（9）分析

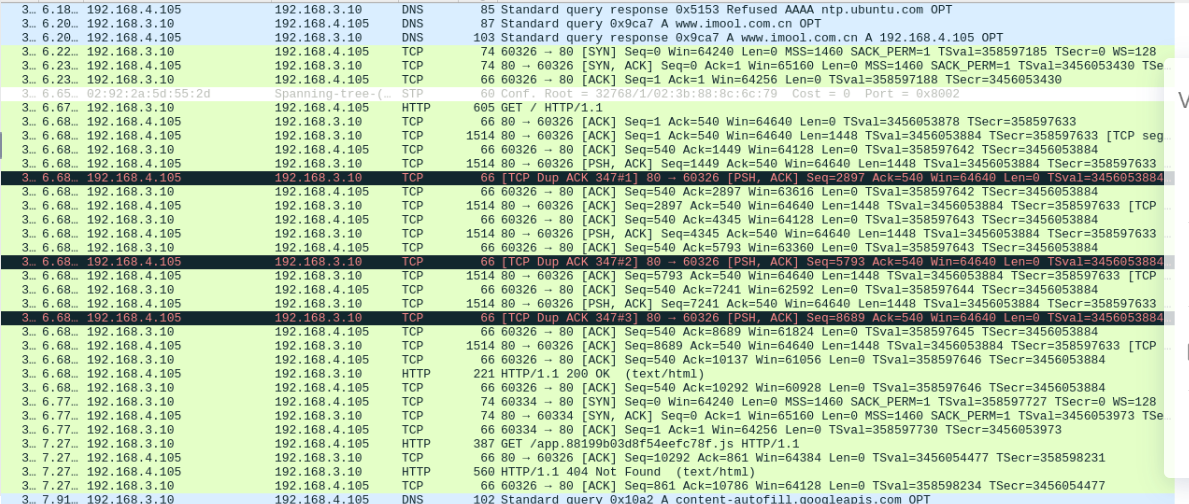
表1-2 流量分析记录表

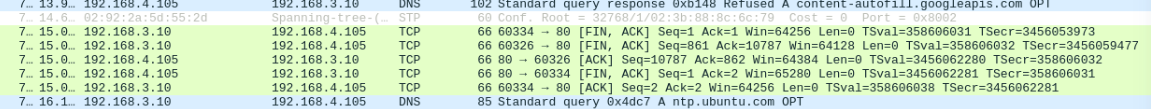
|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 操作 | ARP请求 | | ARP响应 | | ICMP ECHO请求 | | ICMP ECHO 响应 | |
| 源MAC | 目标MAC | 源MAC | 目标MAC | 源IP | 目标IP | 源IP | 目标 |
| 子网内 | 02:99:c2:70:22:6c | 02:82:00:d8:48:8e | 02:82:00:d8:48:8e | 02:99:c2:70:22:6c | 192.168.3.10 | 192.168.3.200 | 192.168.3.200 | 192.168.3.10 |
| 跨子网 | 02:99:c2:70:22:6c | 02:0a:5a:5e:88:e9 | 02:0a:5a:5e:88:e9 | 02:99:c2:70:22:6c | 192.168.3.10 | 192.168.4.105 | 192.168.4.105 | 192.168.3.10 |
| 掩码错 | 02:99:c2:70:22:6c | 02:82:00:d8:48:8e | 02:82:00:d8:48:8e | 02:99:c2:70:22:6c | 192.168.3.10 | 192.168.3.200 | 192.168.3.200 | 192.168.3.10 |

实验2：使用wireshark分析web访问过程流量

（3）

（a）请求：192.168.3.10 响应：192.168.4.105





（b）ARP解析过程中，网关的MAC地址是

（c）

