|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 院系 | 计算机学院 | 班 级 | 19级软件工程 | | 组长 | 冼子婷 |
| 学号 | 18338072 | 18346019 | | 18322043 |  |  |
| 学生 | 冼子婷 | 胡文浩 | | 廖雨轩 |  |  |

1. **实验报告如有雷同，雷同各方当次实验成绩均以0分计。**

**警示**

1. **当次小组成员成绩只计学号、姓名登录在下表中的。**
2. **在规定时间内未上交实验报告的，不得以其他方式补交，当次成绩按0分计。**
3. **实验报告文件以PDF格式提交。**

Ftp协议分析实验

一、打开“FTP数据包”的“ftp例1.cap”文件，进行观察分析，回答以下问题(见附件)

|  |  |
| --- | --- |
| 题号 |  |
| 1 | FTP客户端的mac地址是多少？ |
| 答案 | 00:14:2a:20:12:96 |
| 截图 |  |
| 分析 | TCP的连接和建立都是采用客户/服务器的方式。主动发起建立连接的应用进程称为客户，被动等待连接建立的应用进程称为服务器。发送建立TCP连接请求的是172.16.39.73地址的机器，因此该机器是客户端，其mac地址为00:14:2a:20:12:96 |
| 2 | 第1、2、3号报文的作用是什么？ |
| 答案 | 客户端172.16.39.73和服务端172.16.28.58用三次握手建立TCP连接。具体来看：1号报文是客户端首先在服务器21号端口与服务器端发起一个用于控制的TCP连接，并且把自己的MSS（Maximum Segment Size）告诉对方。2号报文是服务端收到连接请求报文端后，同意并发回确认。3号报文是客户端收到服务端的确认后，建立TCP连接。 |
| 截图 |  |
| 分析 | TCP连接建立的过程：  客户端的TCP向服务器发送连接请求报文段，一个建立连接的同步（SYN）请求。  服务器的TCP收到连接请求报文段后，如同意则发回确认（SYN/ACK）应答。  客户端收到此报文段后，向服务器给出确认（ACK）。  也就是俗称的TCP连接“三次握手”过程。 |
| 3 | 该数据包中共有多少个TCP流？ |
| 答案 | 5个 |
| 截图 |  |
| 分析 | 第一种方法：SYN置为1时表示一个TCP连接请求，通过筛选SYN为1的字段，可以筛选出客户端向服务器发出连接请求报文段和服务器的TCP收到连接请求报文段后同意的报文段。  可以看出有5次TCP连接请求和连接同意，即共有5个TCP流。  第二种方法，也可以通过Wireshark通过两端的IP加port过滤出一个TCP/UDP流，即通过Wireshark的Statistics->Conversations，点击TCP标签即可看到所有的TCP流。 |
| 4 | 用什么用户和密码登录成功？ |
| 答案 | USER: wlx2008  PASS: wlx2008 |
| 截图 |  |
| 分析 | 由于ftp协议是以明文方式发送用户名和口令，只需要筛选出ftp的数据包即可捕获到用户名和用户密码 |
| 5 | 该FTP的命令连接和数据连接分别是什么样的连接？ |
| 答案 | 第一次连接属于命令连接，后四次连接都是数据连接 |
| 截图 |  |
| 分析 | FTP是一个客户/服务端系统，客户端和服务器通过两个连接进行通信，其一是控制连接，客户端发出FTP命令，服务器给出应答。在命令连接中，FTP服务器使用的端口号是21。其二是数据连接，真正的文件传输是在这个连接上进行的。服务器端的数据连接端口号是20。 |
| 6 | 该FTP的连接模式是那种？为什么？ |
| 答案 | 主动模式，因为数据连接是由服务器端主动发起的，客户端利用控制连接将客户端端口号通告给服务器，客户端发送PORT命令。 |
| 截图 |  |
| 分析 | FTP的数据连接支持两种模式：主动模式和被动模式，区别在于数据连接是由谁发起的。  主动模式即Port方式，收到数据传送请求后，服务器主动与客户端建立连接。服务器必须获得客户端的端口号，在此模式下，客户端利用控制连接，将客户端号通告给服务器。客户端发送的命令是PORT n1,n2,n3,n4,n5,n6，其中前四位表示客户端的IP地址，后两位确定端口号为n5\*256+n6。  被动模式是发送Pasv命令到FTP服务器，服务端随机打开一个高端端口，并通知客户端在该端口上传数据的请求。 |
| 7 | 最后四个报文的作用是什么？ |
| 答案 | 最后四个包是四次挥手过程，表示数据传输结束，TCP连接释放。 |
| 截图 |  |
| 分析 | 最后四个数据包前两个数据包中可以看出，客户端向服务端发送quit请求。  TCP连接的释放需要双方都发送释放连接的报文，等待对方确认。  即客户端释放连接，置FIN位，服务端发送ACK确认。  服务器释放连接置FIN位，客户端发送ACK确认。 |
| 8 | 该数据包中有多少个ftp的命令及应答，其含义分别是什么？ |
| 答案 | 共十次命令和响应，其中分别为  命令（Request）：  USER: 指定登陆的用户名，以便服务器进行身份验证  PASS: 指定用户口令，该命令必须跟在登陆用户命令之后  PORT: 该命令告诉FTP服务器，客户端监听的端口号是address，让FTP服务器采用主动模式连接客户端  XMKD: 新建目录  RNFR: 重新命令文件，该命令的下一条命令应该用RNTO指定新的文件名  RNTO: 该命令和RNFR命令共同完成对文件的重命名，紧跟在RNFR命令后  STOR: 上传一个指定的文件，并将其存储在指定的位置  NLST: 返回指定路径下的目录列表，省略<路径>时，返回当前目录  RETR: 请求服务器将指定路径内的文件复制到客户端，也即下载指定的文件  QUIT: 关闭与服务器的连接  应答（Response）：  220: 客户端与服务端完成连接的建立  331: 用户名正确，需要用户密码  230: 用户登入成功  200: 命令执行成功  150: 文件状态正常，开始数据连接  226: 结束数据连接，数据传输完成  257: 路径创建成功  350: 请求文件成功，需要下一步的操作命令  250: 请求文件操作完成  221: 服务端断开控制连接 |
| 截图 |  |
| 分析 | 筛选出通过ftp协议传送的数据包，查看通过ftp发起的命令请求和对应的响应 |

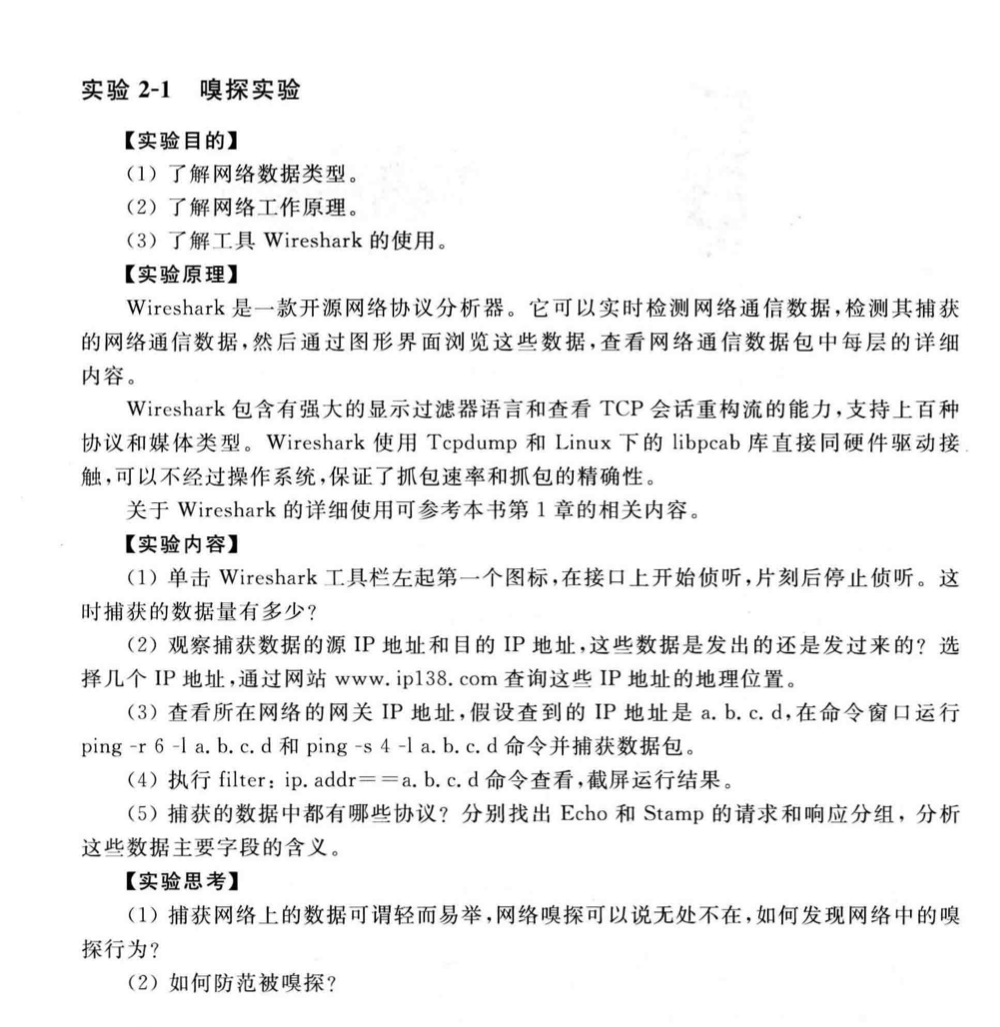
二、打开“FTP数据包”的“ftp例2.cap”文件，进行观察分析，回答以下问题

|  |  |
| --- | --- |
| 题号 |  |
| 1 | FTP服务器的ip是多少？FTP客户端的mac地址是多少？ |
| 答案 | 服务器IP地址：172.16.3.240  客户端mac地址：00:14:2a:20:12:96 |
| 截图 |  |
| 分析 | 通过SYN置位的标志，找到建立TPC连接的三次握手过程，其中source是发起连接的客户端，destination是服务器。 |
| 2 | 该数据包中共有多少个TCP流？ |
| 答案 | 9个 |
| 截图 |  |
| 分析 | SYN置为1时表示一个TCP连接请求，通过筛选SYN为1的字段，可以筛选出客户端向服务器发出连接请求报文段和服务器的TCP收到连接请求报文段后同意的报文段。  可以看出有9次TCP连接请求和连接同意，即共有9个TCP流。  或者在Wireshark的Statistics->Conversations，点击TCP标签即可看到所有的TCP流 |
| 3 | 最后用什么用户和密码登录成功？ |
| 答案 | USER: kjdown  PASS: kjdown |
| 截图 |  |
| 分析 | 通过过滤出ftp客户端的请求（USER和PASS）和服务器的响应码（230登陆成功，331用户名正确需要密码，530登陆失败），可以过滤出登录的操作，最终使用用户名kjdown和密码kjdown登录成功。 |
| 4 | 该FTP的命令连接和数据连接分别是什么？ |
| 答案 | 命令连接：图中数据包序号小于等于172的包  数据连接：图中数据包序号大于等于228的包 |
| 截图 |  |
| 分析 | 通过筛选同步位SYN置为1的数据包，可以得到连接请求或连接接受的报文。由于控制连接中FTP服务器使用的端口号是21，连接由客户端发起。图中序号小于等于172号的数据包都访问到了服务器的21端口，即命令连接。  由于本次FTP连接模式是被动模式，客户端的数据连接端口是随机的，FTP服务器收到Pasv命令后随机打开一个高端端口并且通知客户端在该端口上传送数据的请求。并且在205-209数据包之后，用户登陆成功后才能进行数据连接，所以图中序列号大于等于228的数据包进行的4次连接是数据连接。 |
| 5 | 哪几个报文是FTP数据连接的三次握手报文？ |
| 答案 | 1. 228 229 230 2. 256 257 258 3. 286 287 288 4. 324 325 326 |
| 截图 |  |
| 分析 | FTP的控制连接不论是主动模式还是被动模式都会涉及到服务端的21端口。因此找出同步位SYN置位且不涉及21端口的数据包，并且由于本次FTP连接模式是被动模式，客户端的数据连接端口是随机的，按照三次握手的规则即可找出。 |
| 6 | 哪几个报文是FTP数据连接的挥手报文（结束报文）？ |
| 答案 | 1. 237 238 239 240 2. 270 271 272 273 3. 293 294 296 297 4. 620 621 622 623 |
| 截图 |  |
| 分析 | 控制连接不论是主动模式还是被动模式都会涉及到服务端的21端口。因此找出终止位FIN置位且不涉及21端口的数据包，并且由于本次FTP连接模式是被动模式，客户端的数据连接端口是随机的，按照四次挥手的规则即可找出。 |
| 7 | 该FTP的连接模式是那种？为什么？ |
| 答案 | 被动模式 |
| 截图 |  |
| 分析 | 被动模式即Pasv方式，FTP的客户端发送Pasv命令到FTP服务器，FTP服务器收到Pasv命令后，随机打开一个高端端口，并且通知客户端在该端口上传送数据的请求。 |

**三、**在线捕获数据包实验

1. 阅读教材P64-69内容，熟悉FTP协议。

2. 完成P51的实例2-1。



【解答】

(1)



在监听过程中使用搜索引擎搜索，6.36秒捕获了592个数据包

(2)













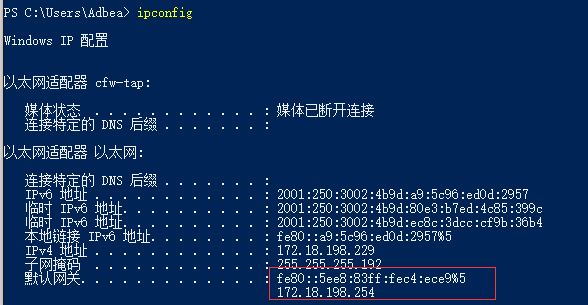




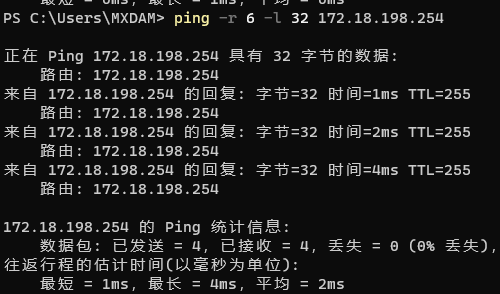
这些数据都是发过来的

(3)

默认网关为：172.18.198.254

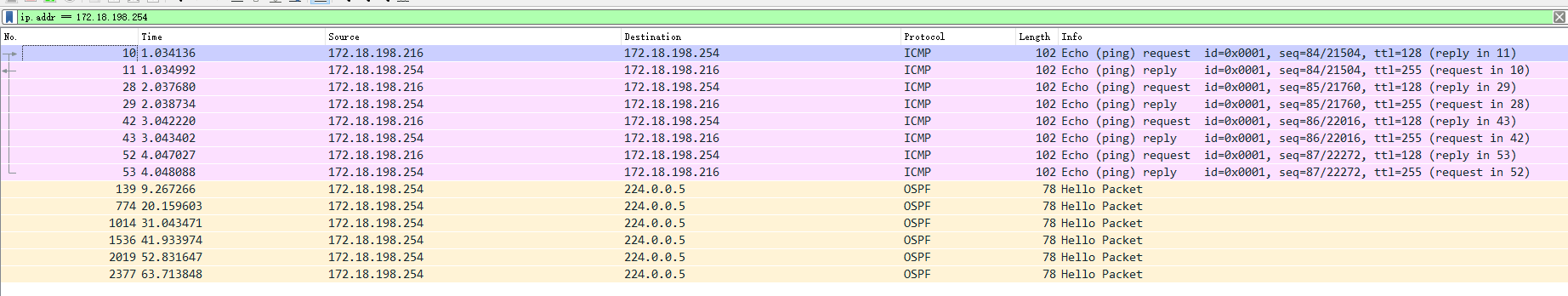


Ping的命令出现错误-l需要后面添加一个字节大小的参数，因为-l默认为32字节大小，此处添加了32作为参数。

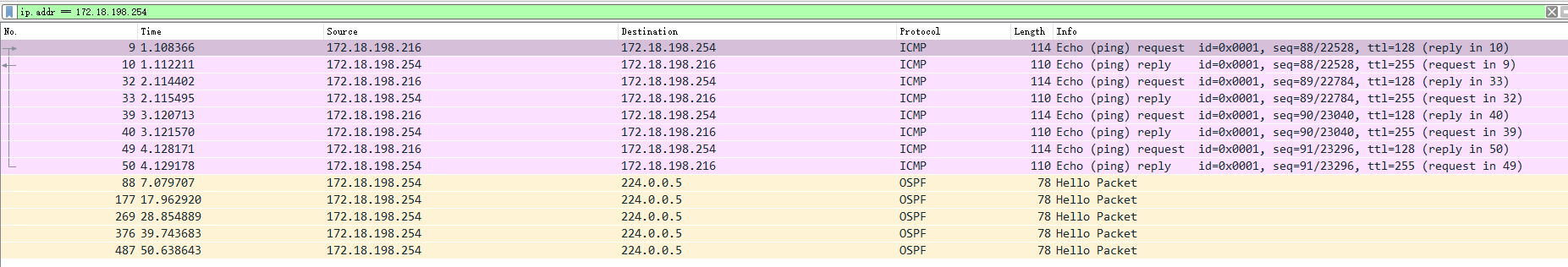


(4)

ping -r 6 -l 32 172.18.198.254



ping -s 4 -l 32 172.18.198.254



(5)

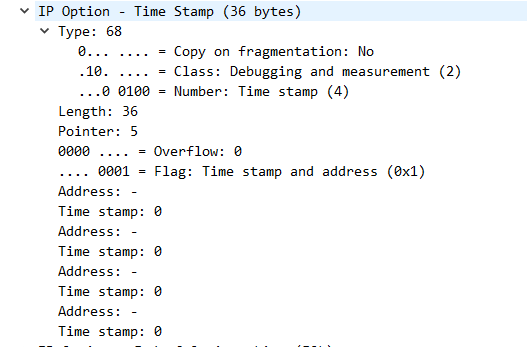
协议类型：ICMP与OSPF

ICMP：在IP通信中，经常有数据包到达不了对方的情况。原因是，在通信途中的某处的一个路由器由于不能处理所有的数据包，就将数据包一个一个**丢弃**了。或者，虽然到达了对方，但是由于搞错了端口号，服务器软件可能**不能接受**它。这时，可以使用**ICMP 报文**来进行故障定位，将故障信息传递给源端。

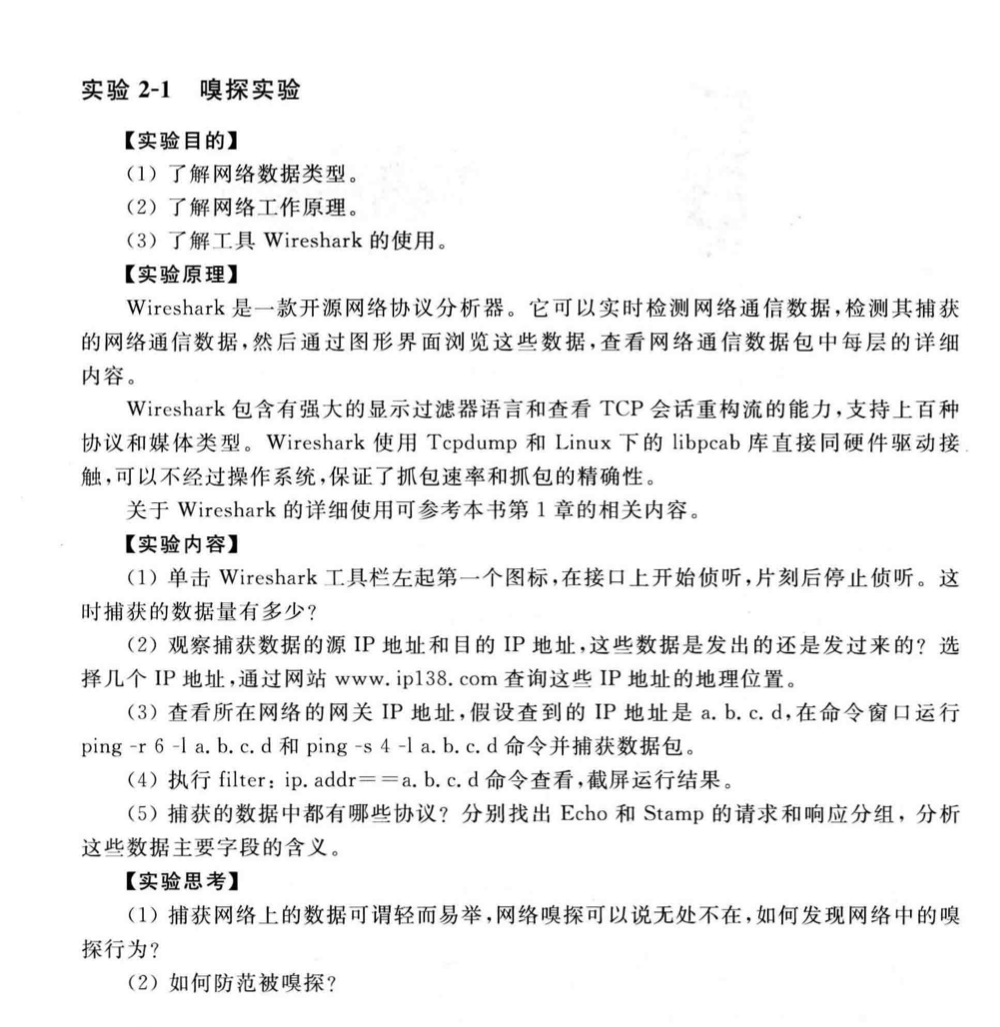
OSPF：开放式最短路径优先（Open Shortest Path First，OSPF）是广泛使用的一种动态路由协议，它属于链路状态路由协议，具有路由变化收敛速度快、无路由环路、支持变长子网掩码（VLSM）和汇总、层次区域划分等优点。

Echo字段：回送选项，协商终端是否将接收的内容返回给发送者

Stamp字段：并没有找到，但是有一个类似的字段，只有ICMP协议才有。



ICMP 时间戳请求允许系统向另一个系统查询当前的时间，但不包含日期，返回的建议值是自午夜零点开始计算的时间（UTC）。



（1）发现网络中嗅探行为的方法：

1. 检查网络接口卡是否为混杂模式（PROMISC）。

2. 监视DNS Reverse Lookups。一些嗅探器在收到一个网络请求时，就会执行DNS反向查询，试着将IP地址解释为主机名。因此，在网络中执行一个Ping扫描或者Pinging一个不存在的IP地址，就会触发这种活动。如果得到了回应，就说明网络中安装有网络嗅探器，如果没有收到任何回应，表明没有嗅探器在运行。

3. 发送一个带有网络中不存在的MAC地址的广播包到网络中的所有主机。正常情况下，网络中的主机接口卡在收到带有不存在的MAC地址的数据包时，会将它丢弃，而当某台主机中的网络接口卡处于混杂模式时，它就会回应一个带有RST标志的包。这样，就可以认为网络中已经有嗅探器在运行。

4. 小心监控网络中各种交换机和路由器的运行情况，来及时发现这些网络设备出现的某种不正常的现象。

5. 使用Honeypot（蜜罐）技术来设计一个陷阱，以此来诱骗嗅探者对它进行嗅探，并通过它来找到嗅探的源头。

6. 小心监视你网络中的主机，经常查看主机中的硬盘空间是否增长过快，CPU资源是否消耗过多，系统响应速度是否变慢，以及系统是否经常莫名其妙地断网等等。

7. 在Linux发行版本中运行ARPWatch来监控网络中是否有新的MAC地址加入。

（2）防范被嗅探的方法：

一、在以太网中防御网络嗅探的方法

在以太网中，你可以使用下列的方法来防御网络嗅探：

1. 尽量在网络中使用交换机和路由器。

2. 对在网络中传输的数据进行加密。不管是局域网内部还是互联网传输都应该对传输的数据进行加密。

3.对于E-mail的内容进行加密后再传输。应用于E-Mail加密的方法主要有数字认证与数字签名。

4. 划分VLAN（虚拟局域网）。应用VLAN技术，将连接到交换机上的所有主机逻辑分开。将它们之间的通信变为点到点通信方式，可以防止大部分网络嗅探器的嗅探。

5. 在网络中布置入侵检测系统（IDS）或入侵防御系统(IPS)，以网络防火墙等安全设备。它们对于许多针对交换机和路由器的攻击方法，很容易就识别出来。

6. 强化安全策略，加强安全培训和管理工作。

7. 在内部关键位置布置防火墙和IDS，防止来自内部的嗅探。

8. 如果要在的网络中布置网络分析器，应当保证网络分析器本身的安全，最好事先制定一个网络分析策略来规范使用。

二、在无线局域网中防御无线网络嗅探的方法

1. 禁止SSID广播；

2. 对数据进行加密。你可以在无线访问点（AP）后再连接一个×××网关，通过×××强大的数据加密功能来保护无线数据传输；

3. 使用MAC地址过滤，强制访问控制；

4. 使用定向天线；

5. 采取屏蔽无线信号方法，将超出使用范围的无线信号屏蔽得；

6. 使用无线嗅探软件实时监控无线局域网中无线访问点（AP）和无线客户连入情况。

本次实验完成后，请根据组员在实验中的贡献，请实事求是，自评在实验中应得的分数。（按百分制）

【交实验报告】

上传实验报告：[ftp://172.18.178.1/](ftp://222.200.180.109/) 用户名/口令：netjob/d502 截止日期（不迟于）：1周之内

上传包括两个文件：

（1）小组实验报告。上传文件名格式：小组号\_ Ftp协议分析实验.pdf （由组长负责上传）

例如: 文件名“10\_ Ftp协议分析实验.pdf”表示第10组的Ftp协议分析实验报告

（2）小组成员实验体会。每个同学单独交一份只填写了实验体会的实验报告。只需填写自己的学号和姓名。

文件名格式：小组号\_学号\_姓名\_ Ftp协议分析实验.pdf （由组员自行上传）

例如: 文件名“10\_05373092\_张三\_ Ftp协议分析实验.pdf”表示第10组的Ftp协议分析实验报告。

|  |  |  |
| --- | --- | --- |
| 学号 | 学生 | 自评分 |
| 18338072 | 冼子婷 | 98 |
| 18322043 | 廖雨轩 | 98 |
| 18346019 | 胡文浩 | 98 |
|  |  |  |
|  |  |  |

**注意：不要打包上传！**