|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 姓名： | | 学号： | 专业年级：软件工程2020 | 班级： 卓越班 |
| 分组： | | 实验室： | 指导教师：郭念 | 实验日期：2022.04.21 |
| **实验的准备阶段**  **(指导教师填写)** | **课程名称** | **计算机网络与安全** | | |
| **实验名称** | **Wireshark 软件使用与 ARP 协议分析** | | |
| **实验目的** | 学习 Wireshark 的基本操作，抓取和分析有线局域网的数据包；掌握以太网 MAC 帧的基本结构，掌握 ARP 协议的特点ࣿ工作过程。 | | |
| **实验内容** | 使用 Wireshark 抓取局域网的数据包并进行分析：  1. 学习 Wireshark 基本操作：重点掌握捕获过滤器和显示过滤器。  2. 观察 MAC 地址：了解 MAC 地址的组成，辨识 MAC 地址类型。  3. 分析以太网帧结构：观察以太网帧的首部和尾部，了解数据封装成帧的原理。  4. 分析 ARP 协议：抓取 ARP 请求和应答报文，分析其工作过程。 | | |
| **实验类型**  （打☑） | ☑验证性 □演示性 □设计性 □综合性 | | |
| **实验的重点、难点** | 1. 分析以太网帧结构； 2. 分析 ARP 协议 | | |
| **实验环境** | 1. PC 机一台，连入局域网； 2. Wireshark 软件，建议 3.0 以上版本。 | | |
| **实验的实施阶段** | **实验步骤及实验结果** | 1.1 WireShark 基本使用  1. 通过 Wireshark 官网下载最新版软件，按默认选项安装。  2. 运行 Wireshark 软件，程序界面会显示当前的网络接口列表，单击要观察的网络接口，开始捕捉数据包，Wireshark 软件选择网络接口的界面截图如下：。    3. 点击工具栏上的红色方块按钮停止捕捉。  4. 菜单、工具栏、状态栏和主窗口界面截图如下：    5. 可以根据需要通过菜单“视图” 以，”编辑/首选项/外观”的相关选项对基本设置进行更改，界面截图如下：    5. 使用“显示过滤器”可以方便地从捕获的数据包中筛选出要观察的数据包。显示过滤器支持若干的过滤选项：源 MAC、目的 MAC、源 IP、目的 IP、TCP/UDP 传输协议、应用层协议（HTTP, DHCP）、源端口 Port、目的端口 Port 等。在显示过滤器栏中输入下面的命令：  •arp //显示 arp 协议报文，界面截图如下：    在显示过滤器栏中输入：ip.scr == a.b.c.d && icmp //显示源地址为&&的icmp报文, 界面截图如下：    6. 通过主菜单“文件”/“导出特定分组”, 界面截图如下：，可以保存捕获的网络数据 （也可以先选中某些包，只保存部分数据）。    7. 如果只想捕捉特定的数据包，可以使用菜单“捕获”/“捕获过滤器”选定想要的类型。例如，选择“IPv4 only”，Wireshark 只抓取 ipv4 类型的数据包。界面截图如下：    8. Wireshark 还提供了丰富的统计功能供用户选用，界面截图如下：。    更多文档可以查询 Wireshark 使用帮助 3。  1.2 观察 MAC 地址  启动 Wireshark 捕捉数据包，在命令行窗口分别 ping 网关，分析本机发出的数据包。界面截图如下：      请回答：该帧的Destination MAC 地址和Source 的 MAC 地址，MAC 地址类型、OUI 信息、I/G位和G/L 位。  Destination MAC 地址 IPv4mcast\_fb (01:00:5e:00:00:fb)  Source 的 MAC 地址 de:bf:c8:3e:85:ae (de:bf:c8:3e:85:ae)  MAC 地址类型 多播  OUI 信息 de:bf:c8  I/G位 1  G/L 位 1    1.3 分析以太网的帧结构  选择其中一个数据包，点击 Ethernet II 展开，界面截图如下，    查看 MAC 帧的各个字段。请回答该帧有哪些字段，字段值分别为什么？  该帧有目的地址字段、源地址字段和 2字节的类型字段。字段值分别为：debf, c83e, 85ae  1.4 ARP 协议分析  1. 打开本机的CMD窗口，先使用arp -a查看arp缓存，再使用 arp -d 命令（其语法见图1.1–10)，清空本机的 ARP 缓存。界面截图如下，      2. 开启 Wireshark， 在CMD窗口ping 本机的同网段地址，在显示过滤器条框中输入“arp”，界面截图如下：    使用 arp -d 命令，清空本机的 ARP 缓存。开启 Wireshark，ping 与本机网段不同的 IP 地址或域名，界面截图如下：    请回答： ARP 报文的各个字段是什么？分析请求/响应的过程。  1.ARP报文中各个字段的含义如下：  硬件类型：表明ARP协议实现在何种类型的网络上。  协议类型：代表解析协议（上层协议）。这里，一般是0800，即IP。  硬件地址长度：MAC地址长度，此处为6个字节。  协议地址长度：IP地址长度，此处为4个字节。  操作类型：代表ARP协议数据包类型。0表示ARP协议请求数据包，1表示ARP协议应答数据包。  源MAC地址：发送端MAC地址。  源IP地址：代表发送端协议地址（IP地址）。  目标MAC地址：目的端MAC地址（待填充）。  目标IP地址：代表目的端协议地址（IP地址）。  2.请求/响应的过程。  1）主机A向主机B发送数据时，应用层数据经过传输层和网络层的封装变成IP数据报到达链路层后，需要封装成帧。 2）帧头需要目的MAC地址，发送主机会首先在其ARP缓存表中查找对应IP或第一跳路由器IP的MAC地址，如果有的话，进行步骤4，否则进行步骤3. 3）主机A会进行一个ARP广播请求，然后会收到一个单播应答，得到IP地址对应的MAC地址 注意：如果主机A和主机B不在同一个局域网内，那么ARP就要找到位于本局域网中的某一个路由器的MAC地址，然后把分组发给这个路由器，让这个路由器把分组发送给下一个网络，剩下的工作就交给下一个网络来做了 4）得到目的MAC地址后，就能封装成帧，送到网卡的输出队列进行发送了。另外顺便会在主机A的ARP缓存表中新增一条记录，以便下次快速查找。 | | |
| **实验结果的处理阶段** | **实验结果的分析与总结** | 1. 使用了显示过滤器后，Wireshark 的抓包工作量会减少吗？  不会减少，过滤只是查找只显示的信息，不会减少任何抓包工作量。但捕抓过滤会减少，对确定的捕抓类型抓包。  2. MAC 帧的长度和 IP 数据报的长度有怎样的关系？请用你的数据记录进行验证。  MAC帧 = 6字节源mac地址 + 6字节目标mac地址 + 2字节类型（ipv4或ipv6） + ip数据报（46~1500字节）+ 4字节帧检验序列FCS MAC帧长度是需要在64~1518字节之间的，太长或者太短都是无效的帧。  3. 假设本机 IP 地址是 192.168.0.38，在本机上运行 Wireshark 捕获报文，使用 “ip.addr == 192.168.0.38”作为过滤条件，能否过滤出本机发出/收到的 ARP 报文？为什么？  能，免费ARP指主机发送ARP查找自己的IP地址，通常发生在系统引导期间进行接口配置时。与标准ARP的区别就是免费ARP分组的目的IP地址字段封装的是自己的IP地址，即向所在网络请求自己的MAC地址。  4. ping 同一局域网内的主机和局域网外的主机，都会产生 ARP 报文么？所产生的 ARP 报文有何不同，为什么？  Ping查找地址那就都会产生ARP报文。它们的发送端mac地址不同，同一局域网则是该连接的交换机mac,局域网外则是目的端交换机的mac  5. ARP 请求数据包是支撑 TCP/IP 协议正常运作的广播包。如果滥发或错发 ARP 广播包会产生那些不良影响？如何发现和应对？  一个数据帧或包被传输到本地网段 (由广播域定义)上的每个节点就是广播；由于网络拓扑的设计和连接问题，或其他原因导致广播数据在网段内大量复制，传播数据帧，导致网络性能下降，甚至网络瘫痪。  通过在网络正常状况下Mac 地址表的扫描，做好记录，当网络出现问题的时候 可以通过对比mac 地址表的方法来查出中arp 攻击的电脑。  6. 什么是免费 ARP（Gratuitous ARP）？它的作用是什么？请使用 Wireshark 进行捕捉和分析。  Gratuitous ARP不同于一般的ARP请求，它并非期待得到IP对应的MAC地址，而是当主机启动的时候，将发送一个Gratuitous arp请求，即请求自己的IP地址的MAC地址。  免费ARP有两个方面的作用。1.验证IP是否冲突。2.更换物理网卡 | | |

**注意：**

1. **实验关键步骤和结果需要截图后粘贴到相应位置，截图要注明学号和姓名。**
2. **提交实验报告时，文档名改为：学号-姓名-实验名称.docx。**