**深 圳 大 学 实 验 报 告**

**课程名称：­ 计算机安全导论**

**实验项目名称­： 包分析实验**

**学院： 计算机与软件学院**

**专业： 软件工程（腾班）**

**指导教师： 陈飞**

**报告人： 黄亮铭 学号： 2022155028 班级： 腾班**

**实验时间： 2024年10月26日 - 2024年11月08日**

**实验报告提交时间： 2024年11月08日**

**教务部制**

|  |
| --- |
| 实验目的与要求：   * 理解TCP、IP协议 * 掌握包分析方法 * 了解Wireshark的使用 |
| 实验环境：   * SimpleISES客户端 * Foxmail，Telnet * Wireshark |
| 实验原理：  参考实验手册 |
| 实验内容：   1. FTP/邮件密码监听 2. Telnet密码嗅探 3. Wireshark软件使用方法 |
| 实验步骤与结果：  （依照实验内容，逐条撰写实验过程与实验所得结果：包括网络架构，核心数据包，调试过程。请附上相关截图，及注意格式排版的美观。实验提交时，以上为评分依据，请不删除本行）  WireShark安装   1. 打开*C:/software*目录，点击WireShark安装包。     图1:安装页面   1. 一直点击next按钮，全部选择默认即可，除了在提示是否安装*WinPcap*时需要手动勾选。     图2:安装*WinPcap*   1. 安装完成后，*勾选”Run WireShark 2.0.2(64-bit)”*，然后点击Finish，软件成功打开，说明软件安装成功。  |  |  | | --- | --- | |  |  |   图3:打开*WireShark*  Wireshark界面功能介绍   1. *WireShark*主界面如下图所示。主界面中央的波动的线代表网卡传输信息的波动。     图4:主界面   1. 我们可以点击本地连接进入以本地连接为数据捕获借口的抓包信息。该界面分为三部分，最上面的是封包列表，中间的是封包的详细信息，最下面的是解析器。     图5:抓包信息   * 1. 封包列表表示所有被捕获的包，这里可以看到收发双方IP地址、协议端口号和封包内容等。   2. 该部分信息按照OSI layer进行分组，可以分别点击查看。   3. 解析器：显示的内容和b中的相同，但是是以16进制展示的。  1. 顶部还有一行菜单栏：起停按钮、设置按钮和对数据包的操作。此外，还有一个显示过滤器，可以让我们查看需要的内容，忽略无关的内容。     图6:菜单栏和过滤器  Wireshark的使用   1. 打开*WireShark*，点击本地连接。然后打开命令行，输入命令：*ping 192.168.1.3 -t*，一段时间后再按下*Crtl+C*停止*ping。*最后回到*WireShark*点击菜单栏从左往右第二个按钮（红色，点击之后会变灰色）。     图7:操作结果   1. 在显示过滤器中输入*icmp*并回车，发现所有类型为icmp的数据包均被筛选出来。然后调整封包列表条目大小，显示info信息。     图8:操作结果   1. 点击保存按钮，然后选择存储的位置即可保存捕获的数据包。     图9:保存文件   1. 如果需要再次查看捕获的数据包，可以打开*WireShark*软件，选择*“打开已保存的捕获文件”*就可以再次查看。  |  |  | | --- | --- | |  |  |   图10:打开捕获文件  Wireshark统计工具的功能详解   1. 打开*WireShark*软件，选择菜单栏中的“统计”，然后点击“捕获文件属性”，打开对应的栏目。     图11:操作结果   1. 捕获文件属性栏目可以查询到第一个分组和最后一个分组的到达时间，同时也可以知道捕获的文件来源于哪一个接口。此外，我们还可以查询到一些更加详细的信息（如果定义了过滤条件，这里只会显示过滤后的数据）。     图12:捕获文件属性   1. 关闭上述栏目，然后选择菜单栏中的“统计”，再点击“协议分级”，打开对应的栏目。     图13:操作结果   1. 该栏目可以查询到所有被捕获到的文件的协议和它们之间的层级关系。分组百分比参照同级别的协议。     图14:协议分组统计   1. 关闭上述栏目，然后选择菜单栏中的“统计”，再点击“对话”，打开对应的栏目。     图15:操作结果   1. 在该栏目中，我们可以选择不同的选项卡调整显示的内容。     图16:对话显示   1. 在目标主机的终端上输入命令：*service httpd status*。如果显示服务停止，则输入命令：*service httpd start*启动服务。     图17:启动*httpd*服务   1. 打开浏览器访问：[*http://192.168.1.3*](http://192.168.1.3)。     图18:浏览器访问给定网址   1. *回到WireShark*，关闭上述栏目。然后选择菜单栏中的“统计”，再选择“对话”，接下来点击“请求”，打开对应的栏目。     图19:操作结果   1. 在该栏目中，我们可以观察到所有http请求数据统计结果。发现确实有192.168.1.3的请求。     图20:统计结果  Wireshark抓取ftp登陆用户名和密码   1. 打开*WireShark*软件，双击本地连接进入自动抓取数据包界面。然后返回桌面，点击计算机图标，输入[*ftp://192.168.1.3*](ftp://192.168.1.3)。     图21:操作结果   1. 右键点击空白处，选择登录。     图22:操作结果   1. 在弹出的对话框中输入用户名和密码进行登录（用户名：wireshark，密码：simplexue123）。  |  | | --- | |  | | 图23a：登录操作 | |  | | 图23b：操作结果 |  1. 返回*WireShark*，点击菜单栏中的停止抓包按钮。同时在显示过滤器中输入ftp。     图24:操作结果   1. 查找封包列表的消息，寻找名字为wireshark的用户。查看得出，USER值为wireshark、PASS值为Samplexue123的请求得到的响应为successful，说明ftp登录的用户名和密码正确。     图25:寻找结果  Wireshark抓取telnet密码信息   1. 打开*WireShark*的自动抓包界面，在过滤器中输入*ip.src==192.168.1.4*。     图26:操作结果   1. 打开IP为192.168.1.4的主机。     图27:操作结果   1. 使用命令*telnet 192.168.1.2*连接主机，然后根据提示输入y确认并回车。  |  |  | | --- | --- | |  |  |   图28:连接主机   1. 输入用户名和密码后回车。  |  |  | | --- | --- | |  |  |   图28:输入信息并登录   1. 返回*WireShark*，可以看见Telnet成功连接。     图29:抓包结果   1. 倒序查看每个Info为Telnet Data的数据包，查看结束后将查看到的内容进行倒序，发现数据就是我们的用户名和密码。  |  | | --- | |  | |  | |  |   图30:查看Data  思考题   1. WinPcap的功能是什么？   WinPcap的功能是发送和接收原始数据包，同时监听共享网络上的数据包。   1. 如何将解析器中的数据以二进制的方式显示？   右键点击解析器内空白位置，选择二进制显示即可。   1. 如何保存抓取获得的数据包？   有两种方法保存抓取获得的数据包1）可以关闭WireShark，在关闭时会提醒保存数据包，选择保存，然后选择存储位置即可；2）点击菜单栏中的保存数据按钮，并选择存储位置。   1. 捕捉文件属性中的接口信息是什么意思？   接口信息显示了捕获数据包时使用的网络接口的详细信息。   1. 过滤器中除了ftp作为过滤表达式，还可以写出什么样的过滤表达式以达到筛选定制数据包的目的？   我们可以使用IP地址作为过滤表达式，也可以筛选出定制数据包。  具体的筛选表达式为：*ip.addr==192.168.1.2 and ip.addr==192.168.1.3*。    图31：筛选结果   1. 除了ip.src==192.168.1.4，还有什么办法可以将TELNET的数据包信息罗列出来？   我们可以使用telnet作为过滤表达式填入过滤器中，可以还有什么办法可以将TELNET的数据包信息罗列出来。    图32：筛选结果 |
| 实验结论：  （撰写实验收获及思考）   1. 本次实验，我完成了实验手册要求的内容。 2. 通过本次实验，我了解了如何使用*WireShark*抓取ftp登录的用户名和密码。 3. 通过本次实验，我了解了如何使用*WireShark*抓取telnet密码信息。 4. 通过本次实验，我了解了如何使用*WireShark*的统计工具的功能。 |
| 指导教师批阅意见：  成绩评定：  指导教师签字：  年 月 日 |
| 备注： |

注：1、报告内的项目或内容设置，可根据实际情况加以调整和补充。

2、教师批改学生实验报告时间应在学生提交实验报告时间后10日内。