实验报告

|  |  |
| --- | --- |
| 实验名称：Wireshark入门 | |
| 实验台号：2 | 实验时间：2019年11月12日 |
| 实验小组：第2组  成员及本次实验分工:於文卓 | |
| 实验目的：   1. Wireshark的基本介绍，包括显示界面、开始界面等· 2. 了解Wireshark的相关设置，包括首选项设置，抓包选项设置，过滤器设置等 | |
| 实验环境说明：  笔记本电脑一台(Win10系统),Wireshark(Version 3.0.3) | |
| 实验过程、步骤（可另附页、使用网络拓扑图等辅助说明）及结果：   1. 什么是Wireshark   Wireshark（前称Ethereal）是一个网络数据包分析软件。网络数据包分析软件的功能是截取网络数据包，并尽可能显示出最为详细的网络数据包数据。Wireshark使用WinPCAP作为接口，直接与网卡进行数据报文交换。  网络管理员使用Wireshark来检测网络问题，网络安全工程师使用Wireshark来检查资讯安全相关问题，开发者使用Wireshark来为新的通讯协定除错，普通使用者使用Wireshark来学习网络协定的相关知识。当然，有的人也会“居心叵测”的用它来寻找一些敏感信息……。Wireshark相对于tcpdump而言，界面更友好，功能更强大。   1. 界面认识   欢迎界面如下。Wireshark是捕获机器上的某一块网卡的网络包，当你的机器上有多块网卡的时候，需要选择一个网卡     1. 菜单栏常用功能，从左到右依次是开始捕获分组、停止捕获分组、重新开始捕获分组。打开、保存、关闭、重新加载文件。和分组的查找以及转换      1. 过滤器主要有两种，一种是显示过滤器，就是主界面上的那个。用来在捕获的记录中找到所需要的记录。还有一种是捕获过滤器，用来过滤捕获的封包，以免捕获太多的记录。在捕获->捕获过滤器中设置。      1. 封包列表中展示的是获取的数据包,面板中显示了编号、时间戳、原地址、目标地址、协议、长度以及封包信息等。也可以修改不同规则的颜色。        1. 数据包的保存   完成数据包的捕获后，可能我们并不急着马上做分析，或者说当前能做的分析还不够完整，需要后面来加深……如此种种，我们需要用文件保存这些数据包。保存数据包也有三种方式，   1. 使用Ctrl+S组合键 2. 菜单栏：依次点击"File"-->"Save" 3. 主工具栏 的按钮      1. 首选项中的一些配置 2. 调整界面位置   可以调整抓包页面的布置，这根据个人喜好，不过以经验来说还是默认的最好用     1. 捕获窗口的一些设置   第一个和第二个选项使得转包的时候前端实时滚动显示抓包详情。第三个选项默认是隐藏转包协议比例显示，比较耗费资源。MAC地址解析会自动将MAC地址转化成易识别设备名。第五第六个如果勾选，会自动将重要ip地址转化成域名，方便识别。 | |
| 实验总结（遇到的问题及解决办法、体会）：  本实验主要是带我们了解了Wireshark的入门。Wireshark是非常流行的网络封包分析软件，功能十分强大。可以截取各种网络封包，显示网络封包的详细信息。使用Wireshark的人必须了解网络协议，否则就看不懂Wireshark。为了安全考虑，Wireshark只能查看封包，而不能修改封包的内容，或者发送封包。Wireshark能获取http，也能获取https，但是不能解密HTTPS，所以Wireshark都不懂HTTPS中的内容。  总结，如果是处理HTTP，或者其他协议比如TCP，UDP就用Wireshark。  Wireshark中的过滤是非常重要的，能帮助我们快速在上千条记录中快速找到自己需要的部分。 | |
| 器材、工具领用及归还负责人：於文卓 | 实验记录人：於文卓 |
| 实验执笔人：於文卓 | 报告协助人：於文卓 |
| 小组成员签名：於文卓 | |
| 验收人： | 成绩评定： |