山东大学 软件 学院

信息安全导论 课程实验报告

|  |  |  |  |
| --- | --- | --- | --- |
| 学号：201600301079 | 姓名： 崔玉峰 | | 班级： 2016级软件4班 |
| 实验题目：实验二Sniffer网络侦听和pcap编程（选做） | | | |
| 实验学时：4 | | 实验日期： 2018/ | |
| 实验目的：  Sniffer实验可以非常直观地演示安全问题之一，即网络窃听。在早期共享式(hub)以太网以及现在交换式(switch)以太网上，这种安全问题都很突出。  实验目的：  （1）了解和验证网络安全威胁最基本的一种形式：网络窃听。  （2）掌握网络侦听工具的用途和用法。  实验内容：  （1）查阅资料，回顾以太网的工作原理。  （2）使用Sniffer类工具软件（wireshark）侦听网络传输信息，包括通信内容及账户/口令等敏感信息。  （3）用winpcap/libpcap库的开发例子。 | | | |
| 硬件环境：  PC  CPU : intel-i5  RAM: 8G | | | |
| 软件环境：  操作系统：windows10 侦听软件：wireshark 本机IP： 121.250.213.1 | | | |
| 实验步骤与内容：   1. **安装Wireshark** 2. **可以直接从官方网站中下载最新版**   **<https://www.wireshark.org/>**       1. **安装并勾线默认即可，安装成功可以显示一下界面：**     通过点击鱼鳍按钮就可以开始侦听网络，可以通过设置过滤条件来滤掉其他协议内容，监听固定IP的请求等等过滤条件，并且可以查看每个网络帧，包的详细内容功能十分强大。   1. **用Wireshark观察分组**   **本机ip为121.250.213.141**   1. **ping一个本网段但是未开机的机器的IP地址，可以引发ARP报文。**          1. **ping一个最近未曾访问过的网站的域名，可引发本机和DNS服务器之间的交互，可以观察到DNS报文，它是封装在一个UDP报文中的。** 2. **在随意的地方找一个网站并执行ping命令**      1. **设置拦截条件UDP并查看**     可以看到访问了DNS服务器  **具体报文内容如下：**       1. **访问某个网页，可以制造HTTP流量，顺便可以看到TCP会话，包括三次握手的过程。也可能会有DNS报文。** 2. **通过浏览器访问网站www.csdn.net（ip: 47.95.164.112）** 3. **设置拦截tcp协议**     可以看到双方确实进行了三次握手  121.250.213.141-->  **47.95.164.112**  **47.95.164.112**--> 121.250.213.141  121.250.213.141-->  **47.95.164.112**   1. **FTP到某个站点，可以观察FTP流量。** 2. **访问数据库课程的ftp网站**   **ftp://211.87.227.230/**     1. **设置拦截ftp协议**     可以看到网站正在请求登录名和密码   1. **用Wireshark观察口令：** 2. **选择一个网站http://space.bilibili.com/93680863?**      1. **登录并拦截http请求查看情况**      1. **并没有查看到登录明文口令应该是接口被加密了** | | | |
| 结论分析与体会：    做过计网实验以后，对于此类网络侦听软件非常熟悉了，但是因为在计网实验中只测试的都是简单的样例，给定的情况观察帧头帧尾。但是通过此次实验真真正正的开始进行了真实的网络监听，虽然看到的多是一些十六进制数据，但是通过了解了网络协议之后还是能通过其中的观察到很多东西的。这也要求我们要更加关注网络窃听，比如对于一些重要的文件数据要进行加密传送，选择可靠安全的网络协议 | | | |