华南理工大学

密码学与安全协议课程实验报告

实验题目:网络数据包监听与分析

|  |
| --- |
| **实验概述** |
| 【实验目的及要求】    实验目的：了解Wireshark软件的主要功能，通过对数据包的分析，跟踪用户会话和网络行为。  实验要求：了解、熟悉Wireshark软件的主要模块和特点，能用Wireshark采集数据包并对其进行网络安全事件的深入分析。  【实验原理】     根据网络传输协议的实现原理。  【实验环境】     安装Wireshark软件的PC机。 |
| **实验内容** |
| 【实验方案设计】   1. 用Wireshark 软件打开文件：dave.CAP. 2. 在过滤输入框输入ip.addreq 137.28.108.11来筛选与Dave的活动有关的内容，其中137.28.108.11是Dave的IP地址 3. 第一个frame是我们所感兴趣的Telnet会话的一部分。 4. 使用第3步得到的地址（你必须使用十六进制格式）来对捕获的包进行过滤。在过滤输入框输入eth.addreq aa:00:04:00:fa:ba and eth.addreq aa:00:04:00:8c:c7来过滤这两个地址之间的通信报文（也可以直接右键点击第一个报文，选择对话过滤器🡪 Ethernet 来直接对该对话进行过滤） 5. 下面在将焦点转义到 telnet通信上来。在刚才的过滤规则下加入andtelnet。 6. 用方向键在frame间移动。 7. 关闭所有的窗口。   【实验过程】（实验步骤、记录、数据、分析）   问题1：新Filtered1窗口有多少筛选得到的frame？（点击工具栏中的统计🡪捕获文件属性来查看统计信息）  回答：筛选得到221个frame    问题2：在第一个frame中看到的上层协议是什么？  回答：telnet    问题3：此frame中DLC地址是什么？  回答： aa:00:04:00:fa:ba和aa:00:04:00:8c:c7  问题4：这两个地址对应的十六进制表示是什么？  回答： aa:00:04:00:fa:ba和aa:00:04:00:8c:c7    问题5：新的过滤后的Filtered 2窗口有多少被筛选到的frame？  回答：453    问题6：你看到前面的35个frame的上层协议是什么？  telnet  问题7：为什么你的答案会与第4步的答案不一样？  回答：因为过滤的条件不一样  问题8：新的过滤后的有多少筛选后的frame？  回答：228    问题9：尝试用tcp.porteq 23 (telnet 服务的默认端口为23)来代替telnet进行过滤，新的过滤后的有多少筛选后的frame？是否和问题8中的相同？如果不同，是为什么？  回答：441。不同。因为用 and telnet 进行过滤，过滤出来的协议是telnet，而用tcp.porteq 23过滤，过滤出来的协议是tcp。      问题10：Dave看起来是否像是“关心商务”？(提示：检查16进制解码部分的报文内容)  回答：不是。因为telnet会话部分的内容不是商务的内容。    问题10：请看最后一个过滤窗口的IP地址。为什么我们能看到除Dave 的 IP外的更多内容？  有可能发送给别的目的机的数据包需要通过Dave进行中转      【结论】  Wireshark软件主要用于对数据包的抓取和对数据包的过滤。通过对数据包的分析（协议、ip地址、Mac地址等），可以跟踪用户会话和网络行为。 |