



警示

1. 实验心得体会如有雷同，雷同各方当次实验心得体会成绩均以 0 分计。
2. 在规定时间内未上交实验报告的，不得以其他方式补交，当次心得体会成绩按 0 分计。
3. 报告文件以 PDF 文件格式提交。

本报告主要描述学生在实验中承担的工作、遇到的困难以及解决的方法、体会与总结等。

院系	数据科学与计算机学院	班 级	教务二班
学号	18342138	实验名称	
学生	郑卓民	Ftp 协议分析实验	

一. 本人承担的工作

负责本次实验中的 ftp 数据包例 2 实验以及课后题在线捕获数据包实验。

二. 遇到的困难及解决方法

1. 一开始对 TCP 流的概念理解不足，不知道怎样一个过程算一个 TCP 流，最后通过网上查阅知道一个 TCP 流就是一个 TCP 的完整连接过程，从握手到挥手的过程。同时知道 wireshark 里面可以使用 tcp.stream eq (num) 来筛选出某个 TCP 流。
2. 由于 ppt 中没有讲述 FTP 的连接模式是什么，所以对 FTP 的连接模式不了解，最后通过查阅教材，知道 FTP 的连接模式分为主动模式与被动模式。
3. 在 ping 的过程中，捕获不到 timestamp 的数据包，通过查阅资料知道，timestamp request 对应于 icmp 协议的 type=13，而此项已被废除不用，现在的 timestamp 在 icmp echo 报文里的 option 栏里显示详情。

三. 体会与总结

本次实验主要锻炼使用 wireshark 进行网络数据包捕获的能力，第一部分针对 FTP 连接分析了有关数据包的内容，第二部分针对 ping 命令的操作分析了 icmp 数据包的内容。通过本次实验，更加熟练地运用 wireshark 进行抓包分析，并且对 tcp、IP、ftp 以及 icmp 等相关内容有了更深的理解。

【交报告】

上传报告: <ftp://222.200.180.109/>

说明:上传文件名: 小组号_学号_姓名_XX 实验.pdf