计算机网络实验报告

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	15-1 班
学号	15331151		实验名称_ _Ftp 协议分析实验
学生	李佳		

一. 本人承担的工作

在周一的实验课上，我们先整体浏览了一遍实验题目并大概对每个题目进行了分析与解答，但由于对所学知识掌握并不是十分牢固，再加上对 wireshark 很多操作不是很了解，因此我们决定先自行学习书本及 PPT 知识，了解 wireshark 的使用方法，然后在周五晚上一起进行实验。

1.在课堂上我们浏览并概括讨论了一下实验题目和相关要求，梳理了一下实验的思路，对实验的内容、实验对应的知识点有了基本的把握；

2.在课后，我复习了书本的第一章实验基础，并自学了第二章网络嗅探与协议实验并回顾了老师提供的课件；对于 wireshark 的使用，我在网络上学习了一些相关的博客，大概掌握了基础的操作流程和方法；

3.在三个人都完成了基础知识内容的自学后，我们对一些练习题目进行了讨论和分析对比，对于不懂的地方上网搜索思路和解答，最后得到基本一致的认识；

4.在周五的实验开始前，作为小组长，我安排了这次实验的具体分工：我们三个人一起进行讨论和分析，共同完成实验报告；我作为主操作，进行网络抓包以及实验数据的分析，以及实验报告的编写；李辉旭同学在共同分析题目后进行实验报告所需数据的截取和收集；黎皓斌同学在共同分析实验数据过程中对于大家不了解的地方同步进行记录和搜索，并分享讨论；

二. 遇到的困难及解决方法

1. 首先就是对于 wireshark 操作的不了解，因为大家都是首次接触这个软件，所以在课上讨论时的操作都显得很陌生。对于这个问题，我在网上学习了一些相关的博客，还浏览了资料包的相关 PPT，并同时进行操作练习，有了很大的长进；

2. 对于 TCP 流的三次握手和四次挥手，虽然知道总的作用是什么，但并不了解握手和挥手的每一条报文都分别对于客户端和服务器起到了什么作用。在查阅后发现，TCP 的三次握手建立连接：第一次握手：客户端发送 SYN 包(建立连接标志)到服务器，等待服务器确认；第二次握手：服务器接收了客户端发送的 SYN 包，确认客户的 SYN 包(标志位 ACK)，发送一个 SYN 包到客户端表示确认连接；第三次握手：客户端接收到服务器发送的 SYN+ACK 包，向服务器再发送一个确认信息 ACK，完成三次握手，建立 TCP 连接。四次挥手断开 TCP 连接：第一次挥手：客户端发送一个 FIN，告知服务器传送完毕请求关闭连接；第二次挥手：服务器收到 FIN 包，发回一个 FIN+ACK 包，确认收到；第三次挥手：服务器向客户端发送 FIN 包，关闭与客户端的连接；第四次挥手：客户端发回一个 ACK 包确认，双方成功断开连接。

3. 在进行网络抓包时直接开始抓取，发现没有任何抓取结果，在查看后发现并没有选择捕获的接口，由于在我电脑实验使用的是路由器，所以在选择 WLAN 接口后开始抓取，得到了数据；

4. 对于实验提供的两个数据的分析，发现直接在 info 中查看每一次的具体信息数量非常庞大，而且很不直观，对于账户密码以及连接模式等都不能很好的进行分析。在学习后发现，可以通过打开“分析”->“追踪流”->“TCP 流”，这样流的内容就显得非常直观，便于分析回答；

5. 对于 TCP 工作流的计数，可以参考 http://kakadu.blog.51cto.com/4050768/1232299。在回答题目中有几个 TCP 流时，我们的意见有一点偏差，最后我提出了只有在第二次挥手时 ACK 和 SYN 同时为 1，因此可以通过过滤 tcp.flags.syn == 1 and tcp.flags.ack == 1 来得到有多少个第二次握手，那么就有多少个 TCP 流，顺利解决了问题；

6. 在做课本上的实验时，抓取网络包后进行 ip.addr == a.b.c.d 过滤，发现得到的全是 DNS 协议报文，没有题目提到的 Echo 和 Stamp 分组；在询问 TA 和检查后得知，没有在抓包的时候 ping 我的网关 IP，导致没有相关协议报文；

三. 体会与总结

做完本次 Ftp 协议分析实验，觉得相对来说还是比较简单，因为实验数据已经提供，我们只需要进行分析比较即可，很多不懂的地方查阅资料后便可得到解答。最大的收获就是能够大概了解 wireshark 这个工具的使用，掌握了相关的过滤规则，并且对于得到的数据可以看懂它的每部分代表了什么，然后也对于一些协议进行了学习，这对以后的实验有很大的帮助。其次，通过本次实验，我也学习到了一些常用的 FTP 命令，比如 ls(显示服务器上的目录)，open(连接 ftp 服务器)，cd(切换远端 ftp 服务器上的目录)，put(上传)，bye(结束与远程计算机的 FTP 会话并退出 ftp)等，同时，对于 FTP 的两个 TCP 连接（控制连接和数据连接）以及连接模式（主动模式和被动模式）有了比较深入的了解。

我认识到课后的自学以及合理利用网络解决困惑是非常重要的学习手段，因为课堂的时间并不能保证我们理解消化所要掌握的知识，对于知识的具体、透彻、牢固掌握其实是十分困难的，这就要求我们必须自己在课后多加学习，并且多问多看多查；除此之外。对于所学知识的不断回顾和再次理解也是十分重要的。

最后，我们必须要意识到小组合作这种方式的重要性和意义所在，现在的工程和项目很少是由一个人单打独斗就能很好完成的，我们需要小组成员共同讨论，提供思路，共同努力，互相监督。在这次实验中，就是因为三个人共同的努力和认真，才会比较顺利和快速的完成实验。如果没有其他两个组员，我肯定又会犯很多粗心的小错误，而且对于不懂的地方不能及时得到解答。所以小组成员一起讨论一起协作是关键。

希望以后的实验中我们能继续努力，更好的掌握知识完成实验。

【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