网络嗅探与协议分析实验实验心得

16337341 朱志儒

第一次做 HTTP 协议分析时，我发现一个非常严重的问题，那就是计算机网络的基础知识非常的不扎实。比如说，实验中 HTTP 报文的种类、HTTP 报文格式等问题我都答不上来，必须依靠书本或是网络才能正确回答。我觉得通过实验的方式来考察我的基本知识是非常好的。

这三次实验中的分析 FTP 协议实验给我的映像最为深刻，因为分析 FTP 协议实验报告是我写的。在做分析实验的过程中，我了解到了许多。之前在理论课上学的 TCP 三次握手过程和四次挥手终止连接的过程不是非常深刻，但这些都可以在这次实验中清楚的观察到，可以清晰地看到客户端和服务器分别在三次握手和四次挥手时期的交流过程，可看到 SYN、FIN、Seq 和 ACK 的变化过程。在写实验报告时，我分析了 FTP 的具体工作过程，了解了 FTP 的工作方式，让我对 FTP 协议有了更深一步的理解。

由于分析 FTP 协议需要建立一个 FTP 服务器，我就在网上找了一个教程，搭建了一个 FTP 服务器。之后又需要让 FTP 服务器将传输的文件加密，于是我又自学使用 FileZilla 将传输的文件进行加密。这次分析 FTP 协议实验提高了我的自学能力。

这三次实验一直有一个问题困扰着我，那就是书上所说的报文号到底是指什么。这个报文号是指 wireshark 所捕获的报文序列号呢？还是指 TCP 报文段中的报文段序列号（Seq）呢？这个问题让我琢磨不透。希望下次老师可以在课堂上介绍一下。