实验 4 网络嗅探与防范

## 实验目的

通过使用 Sniffer 软件来掌握 Sniffer 工具的使用方法，实现捕捉 HTTP、FTP、SMTP、 TELNET 等协议的数据包，理解 TCP/IP 主要协议的数据结构、会话连接建立和终止的过程、 TCP 序列号应答号的变化规律。

通过实验了解 HTTP、FTP、SMTP 等协议明文传输的特性，以建立安全意识。

## 实验准备

（1）比较和选择一种较常用的 Sniffer 工具，推荐使用 Sniffer Pro 或者 Ethereal（Wireshark）。

（2）设计实验环境。

（3）设计实验方案和实验步骤。

## 实验内容

使用一种 Sniffer 工具进行网络监听，主要集中在 HTTP、FTP、SMTP、TELNET 协议 方面，并分析监听结果。

通过熟悉该 Sniffer 工具，完成：

（1）用该工具监听用户通过网页登陆邮箱的过程，分析捕获数据包，了解数据包所使用的网络协议。

（2）在主机上进行 FTP 登陆，并进行嗅探，把嗅探到的重要信息找出来，尤其是用户名和密码。

为了减少分析的数据量，必须有效地设置过滤规则。

完成嗅探工作之后，设计一种安全方案对局域网嗅探器进行防范，付诸实施，然后再打开嗅探器，看是否还能够捕获到上述数据。

## 实验要求

（1）在嗅探过程中，得到的数据包太多，分析起来极其麻烦，这个问题可以通过设置过滤选项来解决。请在做实验时研究怎么设置这些选项，把设置的详细步骤和终结果写出来。

（2）描述防范网络嗅探的方案，说明能够防范的原因。