实验三　网络嗅探与 Ftp 密码破解实验

一　实验目的

1、理解网络嗅探的原理，协议封装的过程，典型嗅探工具的使用。
2、获得网络传输过程中的敏感数据的方法；
3、理解主机扫描的概念，能应用工具对主机进行扫描。

二　实验原理

嗅探的原理

FTP 是文件传输的一个协议，基于不同的操作系统，有不同的 FTP 应用程序，而这些应用程序都遵守同一种协议以传输文件。

Telnet 是通常网络连接所采用的一种协议，通常采用明文进行数据传输，可以通过嗅探的方式捕获用户名和密码。

Wireshark 是一个网络封包分析软件，它的主要功能是撷取网络封包，并尽可能地显示出最为详细的网络封包资料。Wireshark 使用 Winpcap 作为接口，直接与网卡进行数据报文交换。

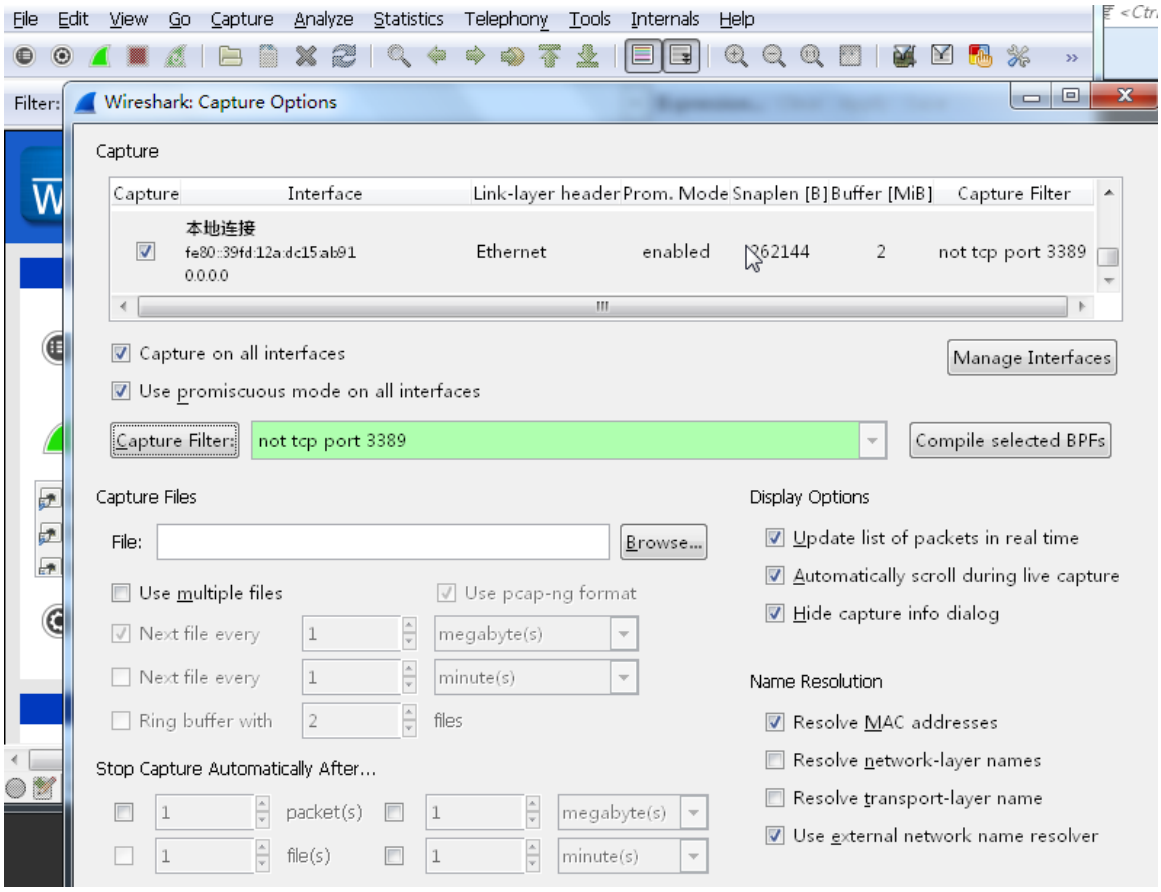
三　实验环境

两台相邻的联网计算机，拓扑如下：

四　实验内容和任务

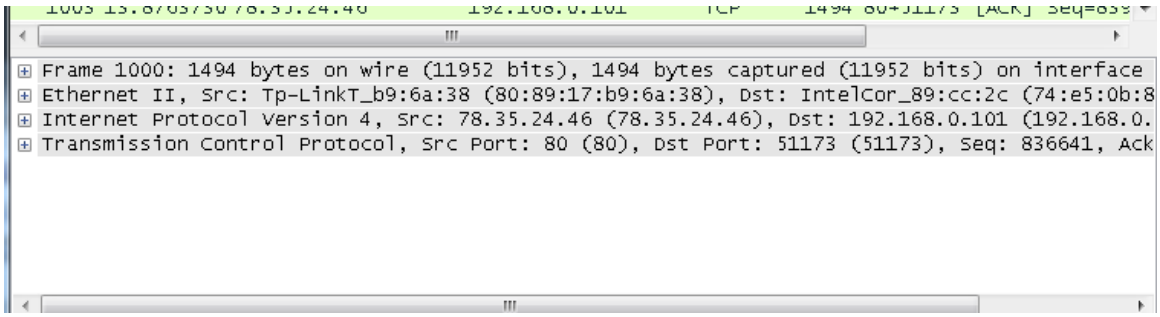
4.1 实验内容 1 利用 WireShark 获取 Ftp 传输协议中的敏感信息

步骤 1：从 ftp 下载 WireShark1.12，并进行安装。在 Capture 菜单中设置抓包相关参数。选择 Interfaces 选项可以选择可操作的网络适配器；通过 Options 选项设置抓包模式、过滤器、数据包限制字节、存档文件模式、停止规则、名字解析等参数（Capture Filter: not tcp port 3389）。然后点击开始进行捕获数据包。如下图所示。

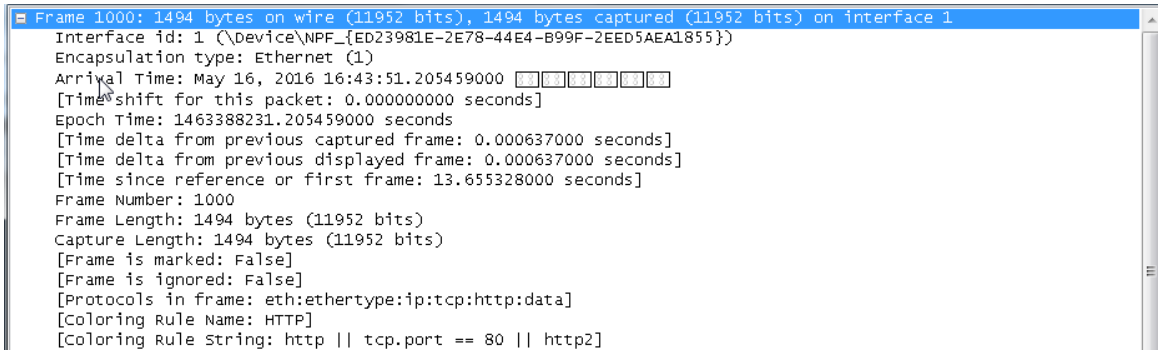


步骤 2：Wireshark 下数据包的解析。

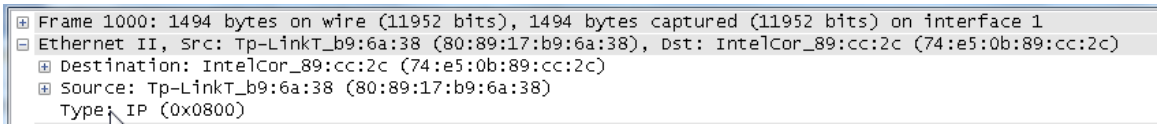
Ethernet 的帧结构为目的 MAC 地址+源 MAC 地址+上层协议类型+数据字段+校验位。Wireshark 利用树形结构显示协议如下：



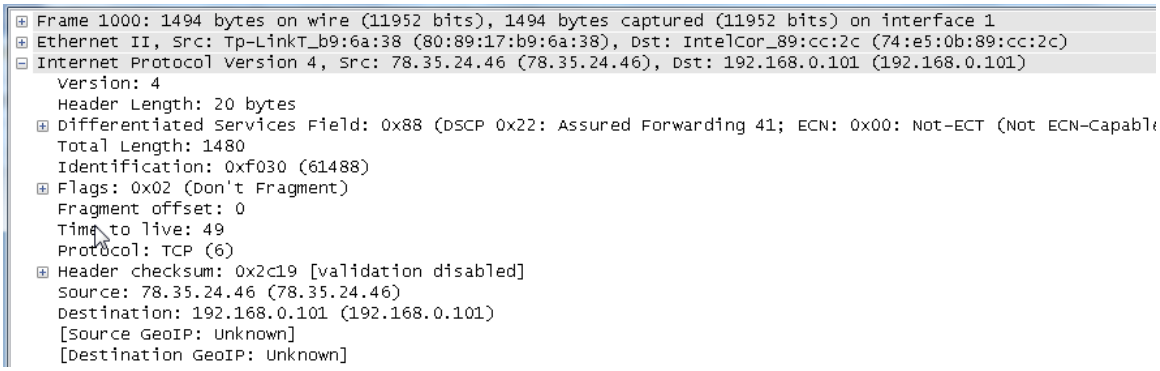
第一行为 WireShark 添加的该帧的相关统计信息，包括捕获时间、编号、帧长度、帧中所含有的协议等信息；具体见下图。



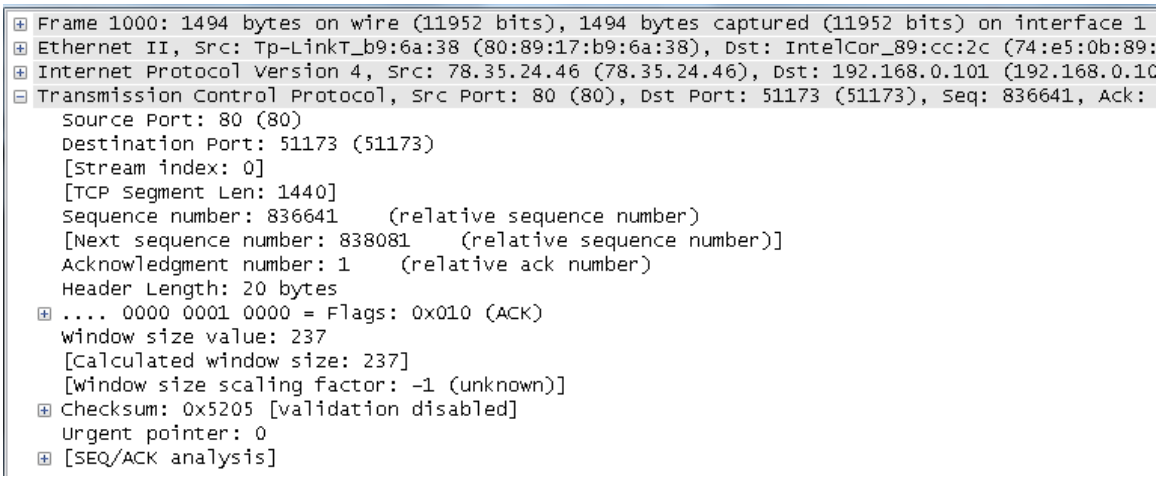
第二行为链路层信息，包括目的 MAC 地址，源 MAC 地址、上层协议类型等，如下图所示。



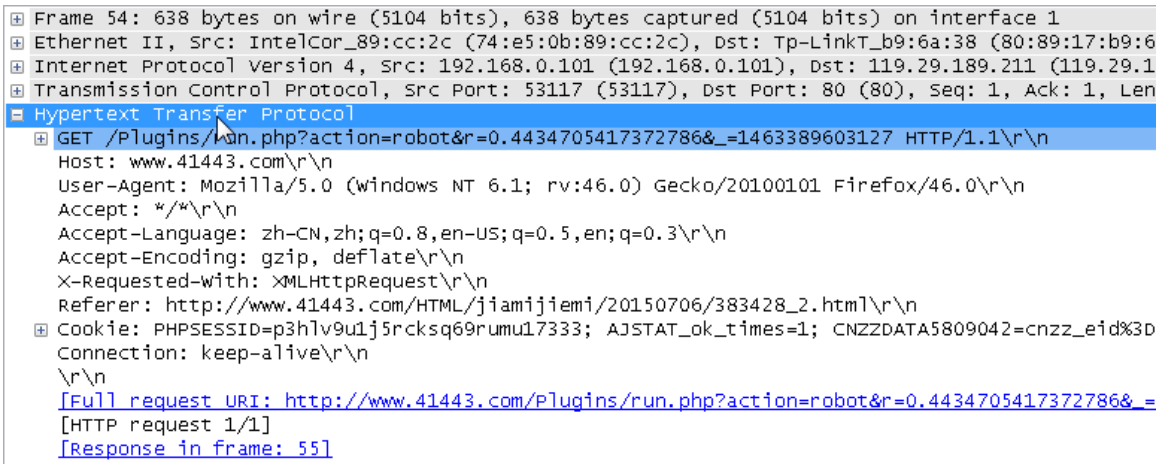
第三行为网络层信息，如此处为 IP 协议。细节包括版本、头部长度、总长度、标志位、源/目的 IP 地址、上层协议等。如下图所示：



第四行为传输层信息，包括源/目的端口、序列号、期望的下个序列号、确认号、头部长度、标志位、窗口长度、校验和等。如下图所示：

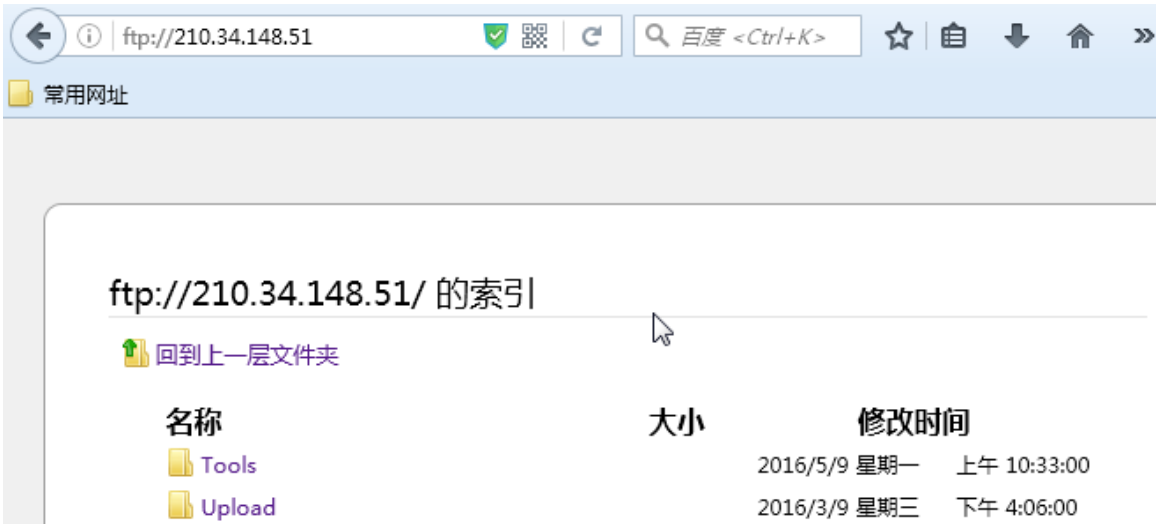


第五行为应用层信息，内容由具体的应用层协议决定，此处为 HTTP 协议，现实的是响应内容。

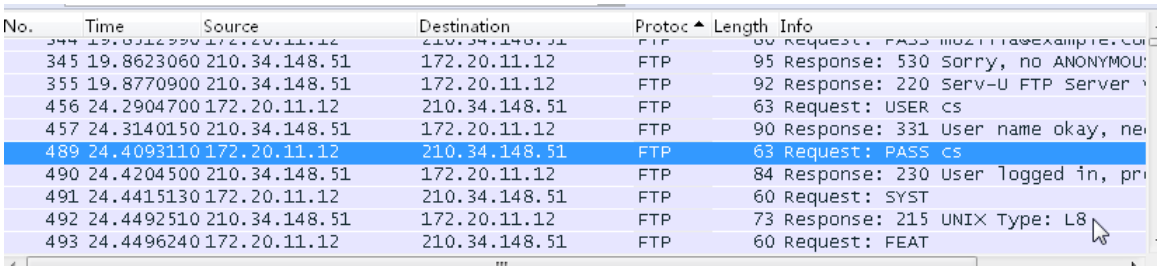


步骤 3:单击 Start 开始抓包。

步骤 4：在地址栏中输入 ftp://210.34.148.51，默认帐号是用户名 test，密码 test.



步骤 5：在 WireShark 界面中，找到登录帐号（cs）和密码（cs），如下图所示：

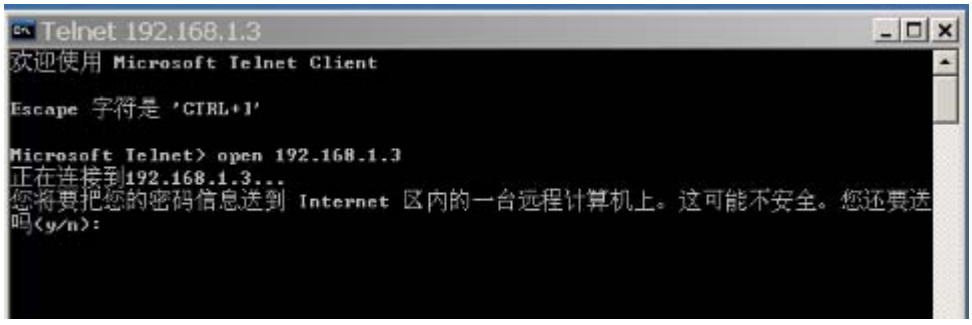


建议进入虚拟机试验环境进行实验。

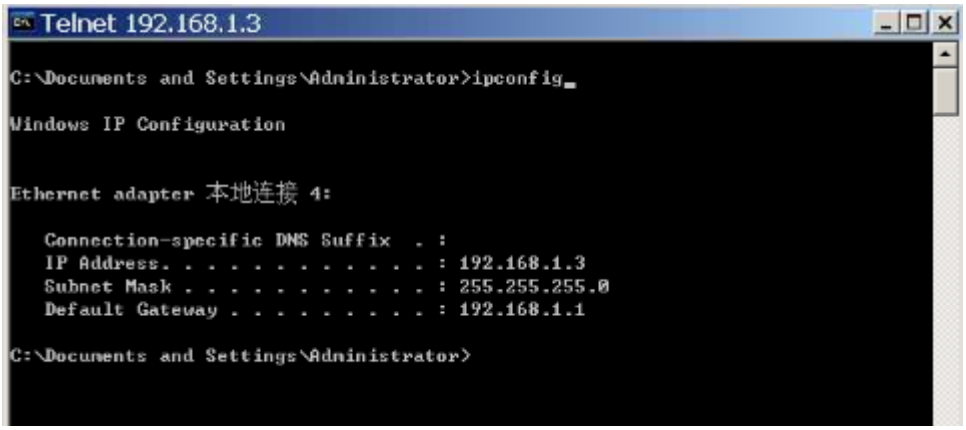
4.2 实验内容 2　利用 WireShark 获取 Telnet 传输协议中的敏感信息

利用 Telnet 明文传输特性，捕获用户名和密码。

步骤 1：在命令行模式下，输入 telnet 命令，进入 telnet 模式。然后输入 open 192.168.1.3（你隔壁电脑的 IP 地址）。如下图所示：



步骤 2：输入 N，继续进行，进入 Telnet 服务。然后输入用户名和密码（Simplexue123），密码不回显。点击回车，即可远程连接到被攻击主机。输入 ipconfig 即可查看 IP 等信息，如下图：



步骤 3：数据传输过程分析。

完成 telnet 连接过程后，Wireshark 也抓到了此次过程的各个数据包。通过检查通讯的 Telnet 数据包，可以找到刚才登录过程中的用户名和密码数据信息。

建议进入虚拟机试验环境进行实验。

4.3 实验内容 3 ftp 密码远程破解（在奇安信虚拟机平台上完成）

步骤 1 搭建一个 ftp 服务器

步骤 2 利用镰刀 ftp 爆破工具对 ftp 访问密码进行破解（基于字典进行破解）。

4.4 实验内容 4 局域网信息探测（在奇安信虚拟机平台上完成）

步骤 1 解压并运行 SoftPerfect Network Scanner 软件

步骤 2 应用 SoftPerfect Network Scanner 对本机进行局域网信息探测，给出探测结果。

五．实验报告要求

按照实验步骤要求，对每一步实验结果的截图。