

## 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，它的主要功能是截取网络封包，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

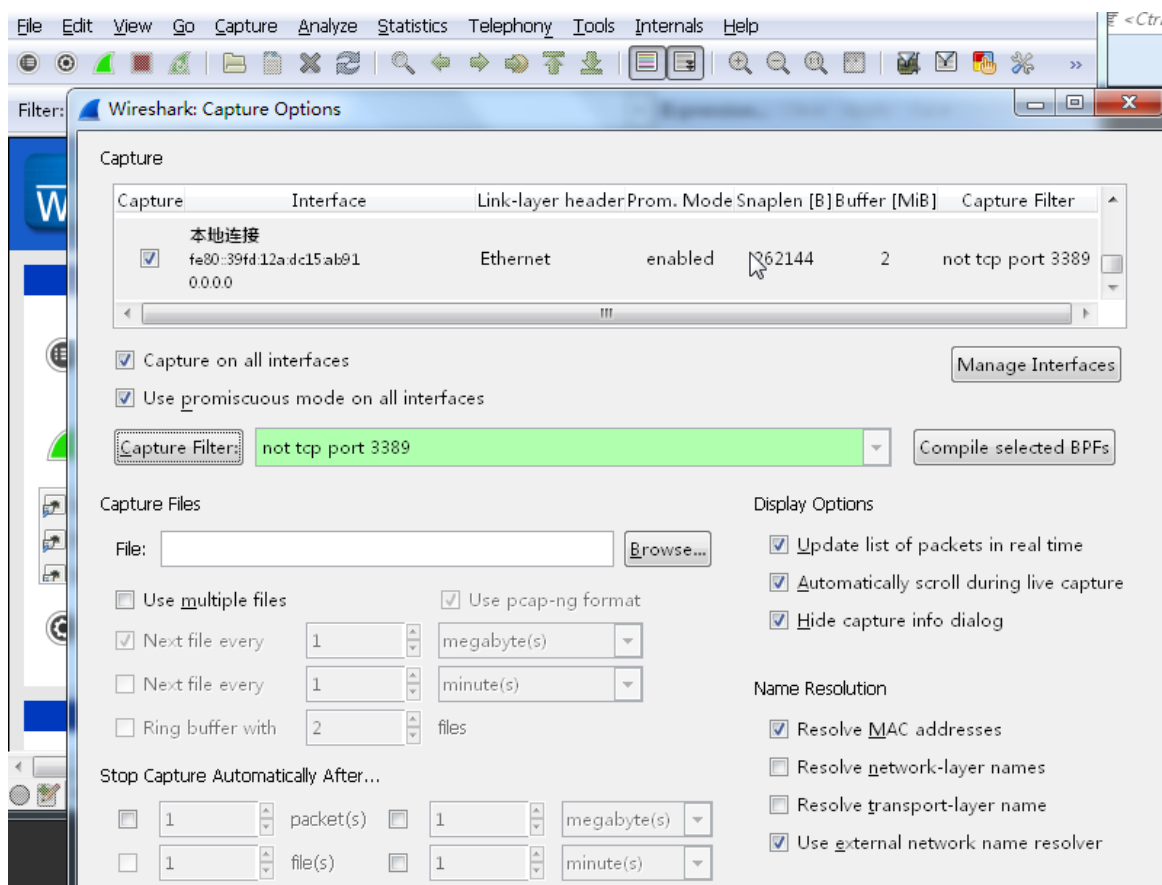
两台相邻的联网计算机，拓扑如下：



### 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

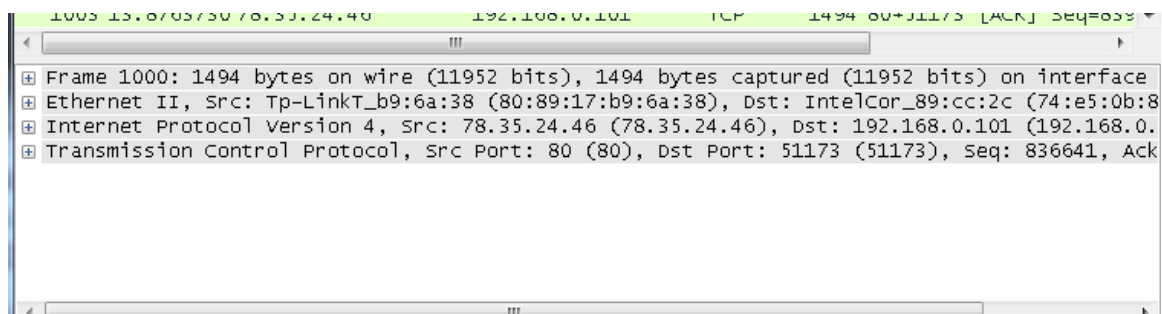
步骤 1：从 ftp 下载 WireShark1.12，并进行安装。在 Capture 菜单中设置抓包相关参数。选择 Interfaces 选项可以选择可操作的网络适配器；通过 Options 选项设置抓包模式、过滤器、数据包限制字节、存档文件模式、停止规则、名字解析等参数（Capture Filter: not tcp port 3389）。然后点击开始进行捕获数据包。如下图所示。



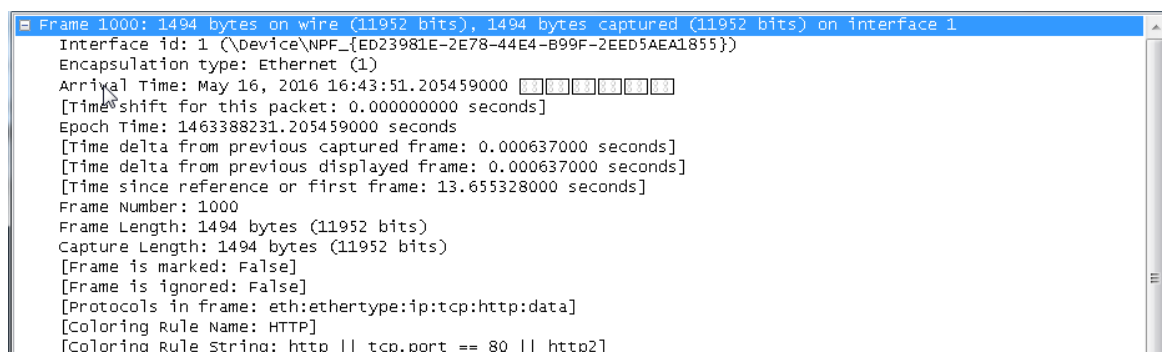
步骤 2: Wireshark 下数据包的解析。

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。

```
+ Frame 1000: 1494 bytes on wire (11952 bits), 1494 bytes captured (11952 bits) on interface 1
+ Ethernet II, Src: Tp-LinkT_b9:6a:38 (80:89:17:b9:6a:38), Dst: IntelCor_89:cc:2c (74:e5:0b:89:cc:2c)
+ Destination: IntelCor_89:cc:2c (74:e5:0b:89:cc:2c)
+ Source: Tp-LinkT_b9:6a:38 (80:89:17:b9:6a:38)
+ Type: IP (0x0800)
```

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：

```
+ Frame 1000: 1494 bytes on wire (11952 bits), 1494 bytes captured (11952 bits) on interface 1
+ Ethernet II, Src: Tp-LinkT_b9:6a:38 (80:89:17:b9:6a:38), Dst: IntelCor_89:cc:2c (74:e5:0b:89:cc:2c)
+ Internet Protocol Version 4, Src: 78.35.24.46 (78.35.24.46), Dst: 192.168.0.101 (192.168.0.101)
+ Version: 4
+ Header Length: 20 bytes
+ Differentiated Services Field: 0x88 (DSCP 0x22: Assured Forwarding 41; ECN: 0x00: Not-ECT (Not ECN-Capable))
+ Total Length: 1480
+ Identification: 0xf030 (61488)
+ Flags: 0x02 (Don't Fragment)
+ Fragment offset: 0
+ Time to live: 49
+ Protocol: TCP (6)
+ Header checksum: 0x2c19 [validation disabled]
+ Source: 78.35.24.46 (78.35.24.46)
+ Destination: 192.168.0.101 (192.168.0.101)
+ [Source GeoIP: Unknown]
+ [Destination GeoIP: Unknown]
```

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：

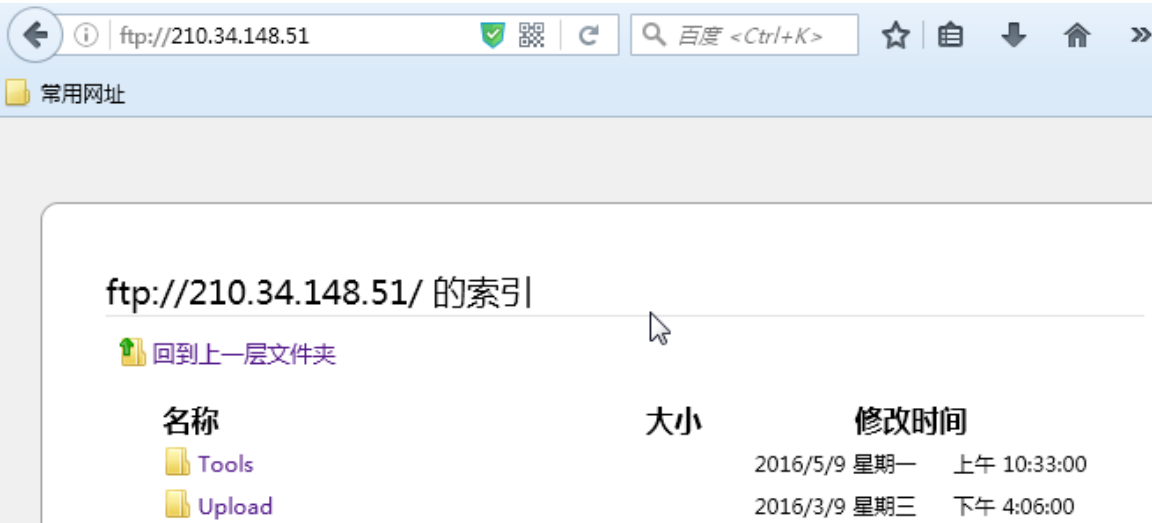
```
+ Frame 1000: 1494 bytes on wire (11952 bits), 1494 bytes captured (11952 bits) on interface 1
+ Ethernet II, Src: Tp-LinkT_b9:6a:38 (80:89:17:b9:6a:38), Dst: IntelCor_89:cc:2c (74:e5:0b:89:cc:2c)
+ Internet Protocol Version 4, Src: 78.35.24.46 (78.35.24.46), Dst: 192.168.0.101 (192.168.0.101)
+ Transmission Control Protocol, Src Port: 80 (80), Dst Port: 51173 (51173), Seq: 836641, Ack: 1
+ Source Port: 80 (80)
+ Destination Port: 51173 (51173)
+ [Stream index: 0]
+ [TCP Segment Len: 1440]
+ Sequence number: 836641 (relative sequence number)
+ [Next sequence number: 838081 (relative sequence number)]
+ Acknowledgment number: 1 (relative ack number)
+ Header Length: 20 bytes
+ ... 0000 0001 0000 = Flags: 0x010 (ACK)
+ Window size value: 237
+ [Calculated window size: 237]
+ [Window size scaling factor: -1 (unknown)]
+ Checksum: 0x5205 [validation disabled]
+ Urgent pointer: 0
+ [SEQ/ACK analysis]
```

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。

```
+ Frame 54: 638 bytes on wire (5104 bits), 638 bytes captured (5104 bits) on interface 1
+ Ethernet II, Src: IntelCor_89:cc:2c (74:e5:0b:89:cc:2c), Dst: Tp-LinkT_b9:6a:38 (80:89:17:b9:6a:38)
+ Internet Protocol Version 4, Src: 192.168.0.101 (192.168.0.101), Dst: 119.29.189.211 (119.29.189.211)
+ Transmission Control Protocol, Src Port: 53117 (53117), Dst Port: 80 (80), Seq: 1, Ack: 1, Len: 54
+ Hypertext Transfer Protocol
+ GET /Plugins/run.php?action=robot&r=0.4434705417372786&_id=1463389603127 HTTP/1.1\r\n
+ Host: www.41443.com\r\n
+ User-Agent: Mozilla/5.0 (Windows NT 6.1; rv:46.0) Gecko/20100101 Firefox/46.0\r\n
+ Accept: */*\r\n
+ Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3\r\n
+ Accept-Encoding: gzip, deflate\r\n
+ X-Requested-With: XMLHttpRequest\r\n
+ Referer: http://www.41443.com/HTML/jiamijiem/20150706/383428_2.html\r\n
+ Cookie: PHPSESSID=p3h1v9u1j5rcksq69rumu17333; AJSTAT_ok_times=1; CNZZDATA5809042=cnzz_eid%3D%3D\r\n
+ Connection: keep-alive\r\n
+ \r\n
+ [Full request URI: http://www.41443.com/Plugins/run.php?action=robot&r=0.4434705417372786&_id=1463389603127]
+ [HTTP request 1/1]
+ [Response in frame: 55]
```

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：

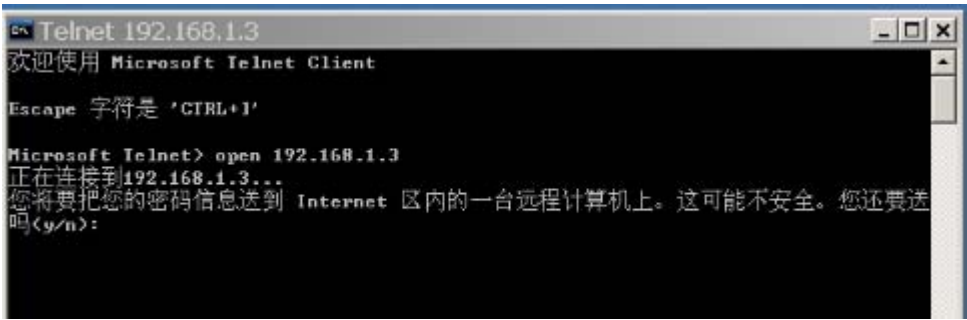
No.	Time	Source	Destination	Protocol	Length	Info
344	19.8312990	172.20.11.12	210.34.148.51	FTP	60	Request: PASS moztfraseexample.com
345	19.8623060	210.34.148.51	172.20.11.12	FTP	95	Response: 530 Sorry, no ANONYMOUS access here
355	19.8770900	210.34.148.51	172.20.11.12	FTP	92	Response: 220 Serv-U FTP Server v5.0.6
456	24.2904700	172.20.11.12	210.34.148.51	FTP	63	Request: USER cs
457	24.3140150	210.34.148.51	172.20.11.12	FTP	90	Response: 331 User name okay, new password please
489	24.4093110	172.20.11.12	210.34.148.51	FTP	63	Request: PASS cs
490	24.4204500	210.34.148.51	172.20.11.12	FTP	84	Response: 230 User logged in, prepare to upload files
491	24.4415130	172.20.11.12	210.34.148.51	FTP	60	Request: SYST
492	24.4492510	210.34.148.51	172.20.11.12	FTP	73	Response: 215 UNIX Type: L8
493	24.4496240	172.20.11.12	210.34.148.51	FTP	60	Request: FEAT

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：

A screenshot of a Telnet window titled 'Telnet 192.168.1.3'. The window shows a command prompt where the user has entered 'ipconfig'. The output displays the IP configuration for the '本地连接 4' (Local Area Connection 4) Ethernet adapter. The configuration includes: Connection-specific DNS Suffix, IP Address (192.168.1.3), Subnet Mask (255.255.255.0), and Default Gateway (192.168.1.1). The prompt returns to 'C:\Documents and Settings\Administrator>'.

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。