# 虚拟专用网

**【实验目的】**

通过使用Sniffer pro软件，掌握Sniffer（嗅探器）工具的使用方法，实现捕捉FTP， HTTP等协议的数据包，以理解TCP/IP协议中多种协议的数据结构、会话连接建立和终止的过程、TCP序列号、应答序号变化规律。

  通过实验了解FTP、HTTP等协议明文传输的特性，以建立安全意识，防止FTP、HTTP等协议由于传输明文密码造成的泄密。

**【实验环境】**

  一台Window2000 Client PC机、一台Window2000 Server PC机，以Cisco交换机连接组成局域网，并且都安装了SnifferPro软件、LeapFTP3.0.1.46（FTP客户端软件）、Flashget下载工具（或者其他软件下载工具）和IE浏览器。

  每两个学生为一组：其中学生A进行Http或者Ftp连接，学生B运行SnifferPro软件监听学生A主机产生的网络数据包。完成实验后，互换角色重做一遍。

**【实验原理】**

网络嗅探器Sniffer的原理

   网卡有几种接收数据帧的状态：unicast（接收目的地址是本级硬件地址的数据帧），Broadcast（接收所有类型为广播报文的数据帧），multicast（接收特定的组播报文），promiscuous（目的硬件地址不检查，全部接收）；

   以太网逻辑上是采用总线拓扑结构，采用广播通信方式，数据传输是依靠帧中的MAC地址来寻找目的主机；

   每个网络接口都有一个互不相同的硬件地址（MAC地址），同时，每个网段有一个在此网段中广播数据包的广播地址；

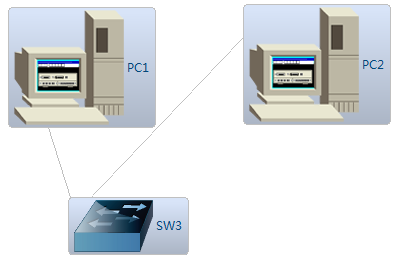
   一个网络接口只响应目的地址是自己硬件地址或者自己所处网段的广播地址的数据帧，丢弃不是发给自己的数据帧。但网卡工作在混杂模式下，则无论帧中的目标物理地址是什么，主机都将接收；

   通过Sniffer工具，将网络接口设置为“混杂”模式。可以监听此网络中传输的所有数据帧。从而可以截获数据帧，进而实现实时分析数据帧的内容。

**【实验内容和步骤】**

1、实验步骤一 搭建实验环境

  实验平台拖出一台WindowsXP PC机、一台Window2003 Server PC机以及Cisco Switch,两台PC通过交换机连接，PC1连接端口fa1/3,PC2连接端口fa1/5,实验拓扑图如下图所示：



启动PC机以及交换机，PC机启动完成后，【网上邻居】->【属性】->【本地连接】->【属性】->【Internet协议（TCP/IP）】,配置IP地址；打开交换机配置界面，配置交换机端口IP地址，相应的IP地址如下表1-1所示：

|  |  |
| --- | --- |
|  | 分配IP地址 |
| Client PC1 | 192.168.1.10/24 |
| Client PC2 | 192.168.1.111/24 |
| Switch vlan1 | 192.168.1.100 |

打开交换机配置界面，配置交换机, Switch1中添加VLAN1，并且将ports3－5 添加到VLAN1中，具体命令如下所示：

Switch1:

enable

configure terminal

vlan database

vlan 1

exit

exit

config terminal

interface range fa1/3 – 5

switchport access vlan 1

no shut

int vlan 1

ip address 192.168.1.100 255.255.255.0

no shut

配置完成后，ping命令三者之间均可通。

2、实验步骤二:熟悉sniffer pro工具的使用

  Sniffer软件是NAI公司推出的功能强大的协议分析软件，实验中使用此软件来获取网络中传输的FTP，HTTP，Telnet等数据包，并进行分析.（安装步骤可按照指导自动进行），安装非常简单，setup后一路确定即可，序列号在sniffer打包文件的sn.txt中，输入即可，第一次运行时需要选择你的网卡，

设置监控网卡

  Sniffer安装完成以后，从“开始”菜单运行，显示“Settings”对话框，在“Selecting settings for monitoring”列表框中单击选择要监控的网卡，单击“确定”按钮，Sniffer 就会监控该网卡中传输的数据，如图1-1所示。如果以后要改变监控设置，可以选择“File”菜单中的“Select Settings”选项，同样会出现该对话框，用来改变要监控的网卡。

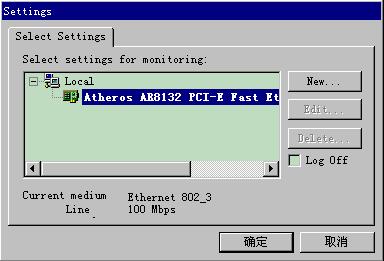


             图1-1 选择网卡示图

  如果在“Settings”对话框中没有显示要监控的网卡，可以将其它网卡添加到该列表框中。单击“New”按钮，显示如图2所示“New Settings”对话框，可以设置新添加的网卡。

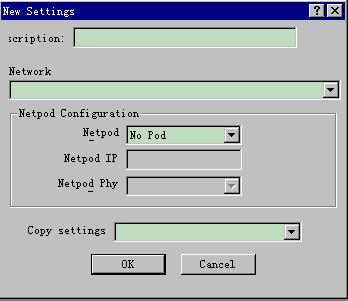


           图1-2 添加新网卡示图

使用说明

 启动该Sniffer Pro软件后可以看到它的主界面，选好后即可启动软件，如下图1-3所示，网络监视面板剪辑，Dashboard可以监控网络的利用率，流量及错误报文等内容，

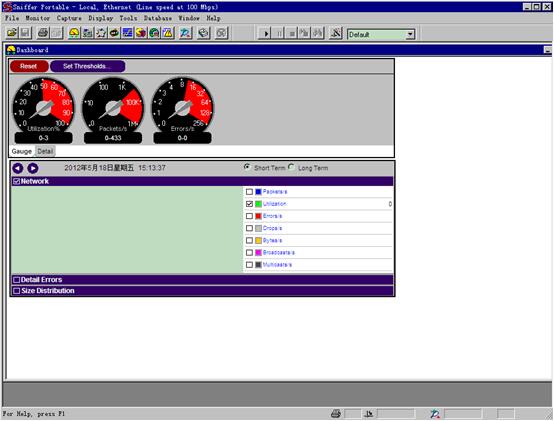


                    图1-3 主界面示图

从Host table可以直观地看出连接的主机，如图1-3所示，显示方式为IP

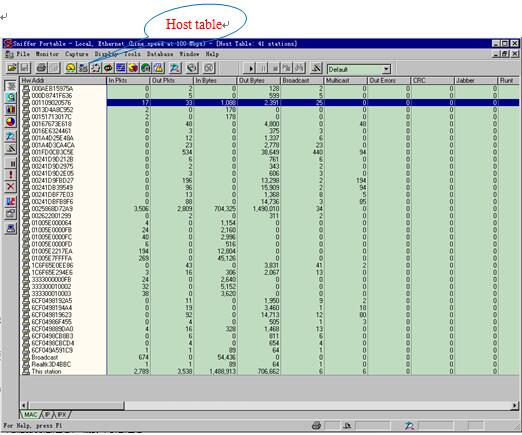


                  图1-3  Host table界面

3、实验步骤三：抓某台机器的所有数据包

  如图1-4所示，本例要抓192.168.199.103这台机器的所有数据包，如图中①选择这台机器。点击②所指图标:

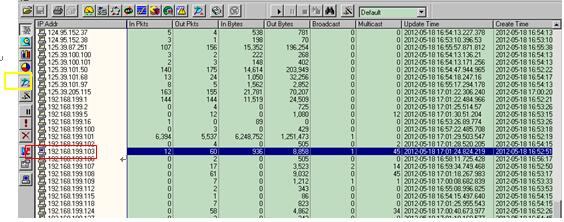


                     图1-4 抓包操作（一）示图

出现图1-5界面，等到图1-5中箭头所指的望远镜图标变红时，表示已捕捉到数据。

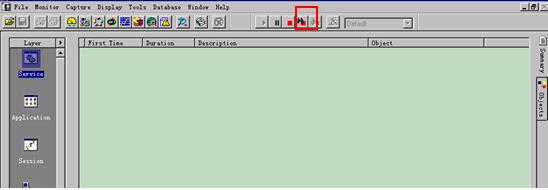


                图1-5 抓包操作（二）示图

点击该图标出现图1-6界面，选择箭头所指的Decode选项即可看到捕捉到的所有包。

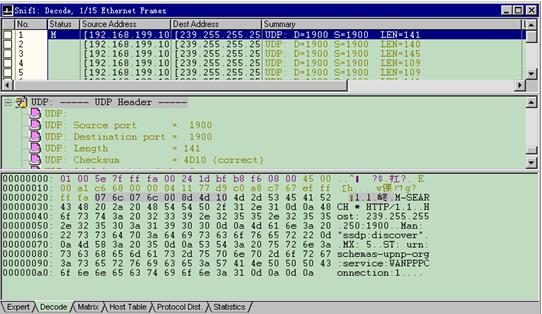


                 图1-6 抓包操作（三）示图

3.1实验步骤四：捕获FTP数据包并进行分析

  假设A主机监视B主机的活动，首先A主机要知道B主机的IP地址，B主机可以在命令符提示下输入ipconfig查询自己的IP地址并通知A主机。

  选中Monitor菜单下的Matirx或直接点击网络性能监视快捷键，此时可以看到网络中的Traffic Map视图。如图1-7所示，可以单击左下角的MAC，IP或IPX使Traffic Map视图显示相应主机的MAC地址，IP地址或IPX地址。图4显示的是IP地址，每条连线表明两台主机间的通信。

在PC2上配置IIS的ftp

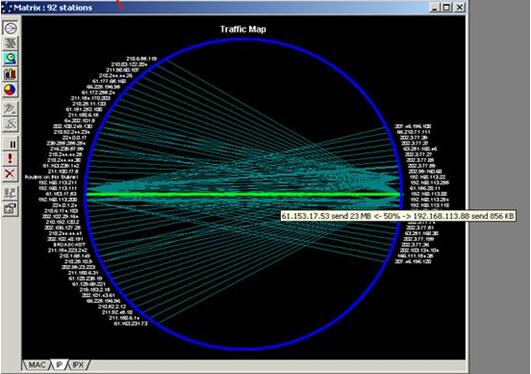


                   图1-7   Matrix视图

单击菜单中规定Capture->Define Filter->Advanced，再选中IP->TCP->FTP,如图1-8所示，然后单击OK

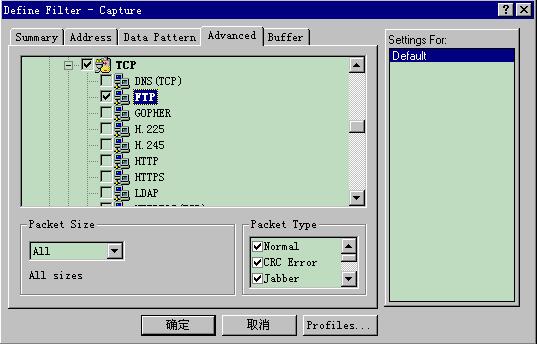


                        图1-8  过滤器选项

（4）回到Traffic Map视图中，用鼠标选中要捕捉的B主机IP地址，选中后IP地址以白底高亮显示，此时，单击鼠标右键，选中Capture或者单击捕获报文快捷键中的开始按钮，Sniffer则开始捕捉指定IP地址主机的有关FTP协议的数据包，如图1-9所示

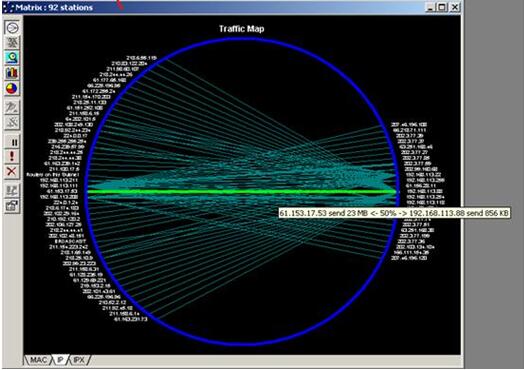


            图1-9 捕捉指定IP主机的数据包

(5).开始捕捉后，单击工具栏中的Capture Panel按钮，显示出捕捉的Packet的数量

(6).B主机开始登陆一个FTP服务器，如图1-10所示

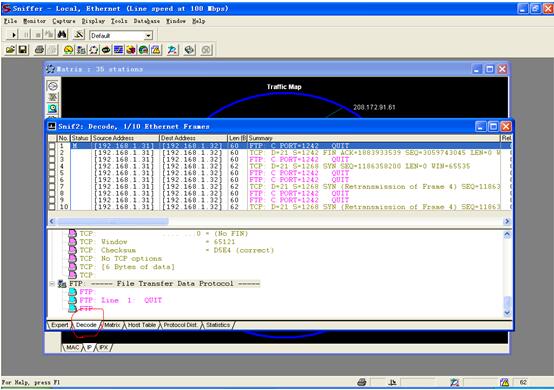


                     图1-10 捕捉界面

4、实验步骤四：捕获HTTP数据包并进行分析

同步骤三

单击菜单中的Capture->Define Filter->Advanced,再选中IP->TCP->HTTP，然后单击ok

同步骤三

B主机登录一个Web服务器（网站），并输入自己的邮箱地址和密码

同步骤三

停止抓包后，单击窗口左下角的Decode选项，窗中会显示所捕捉的数据，并分析捕获的数据包

在捕获的窗口的低端，我们可以看到B主机的重要信息

由步骤三和步骤四的实验我们可以看出，Sniffer可以探查出局域网内流动的任何信息，尤其是用户名和密码之类敏感的数据，所以在局域网内的安全就至关重要了，其实只要在电脑内安装上网络防火墙，并把Windows操作系统的安全级别提高，Sniffer工具就可能嗅探不到任何信息。