**实验一 FTP 协议分析实验**

**实验目的和要求**

学习 Serv-U FTP Server 服务软件的基本配置和 FTP 客户端命令的使用，分析FTP 报文格式和 FTP 协议的工作过程。

**实验原理**

FTP 是文件传输协议 （File Transfer Protocol）的简称。

FTP 基于 TCP 协议，它通过两个 TCP 连接来传输一个文件，一个是控制连接，另一个是数据连接。相应的，在进行文件传输时，FTP 需要两个端口，分别用于控制连接端口 （用

于给服务器发送指令以及等待服务器响应）和数据传输端口 （在客户机和服务器之间发送

一个文件或目录列表） 。

两种连接的建立都要经过一个 “三次握手”的过程，同样，连接释放也要采用 “四次

握手”方法。控制连接在整个回话期间一直保持打开状态。数据连接是临时建立的，在文件

传送结束后被关闭。

FTP 的连接模式有两种，PORT 和 PASV。PORT 模式是一个主动模式，PASV 是被动模式，这里都是相对于服务器而言的。

当 FTP 客户以 PORT 模式连接服务器时，它首先动态地选择一个端口号连接服务器的 21 端口，注意这个端口号一定是 1024 以上的，因为 1024 以前的端口都已经预先被定义好，被一些典型的服务使用或保留给以后会用到这些端口的资源服务。经过 TCP 的三次握手后，控制连接被建立。这时客户就可以利用这个连接向服务器发送指令和等待服务器响应了。当需要从 （或向）服务器传送数据时，客户会发出 PORT 指令告诉服务器用自己的那个端口来建立一条数据连接 （这个命令由控制连接发送给服务器），当服务器接到这一指令时，会使用 20 端口连接客户指定的端口号，用以数据传送。

当FTP 客户以 PASV 模式连接服务器时，控制连接的建立过程与 PORT 模式相同，不同的是，在数据传送时， 客户不向服务器发送 PORT 指令而是发送 PASV 指令， 服务器收到 PASV命令后选择一个端口号发送给客户，客户选择一个本地端口号与服务器发送过来的端口建立一条数据连接。

微软自带的 FTP 客户端命令工具不支持 PASV 模式。

**实验内容与步骤**

在 PC1上安装 Serv-U FTP Server，启动后出现图 6-6 所示界面。

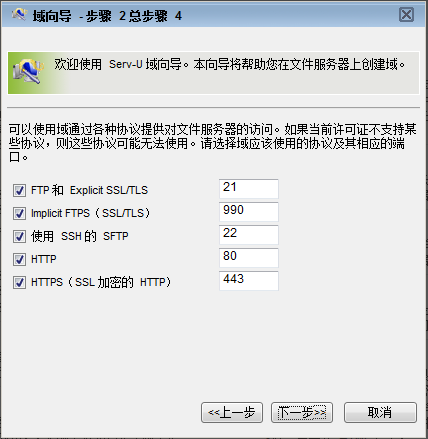


点击窗口上方的新建域，打开添加新建域向导,按照如图 6-7（a）-(d)所示完成如下操作：

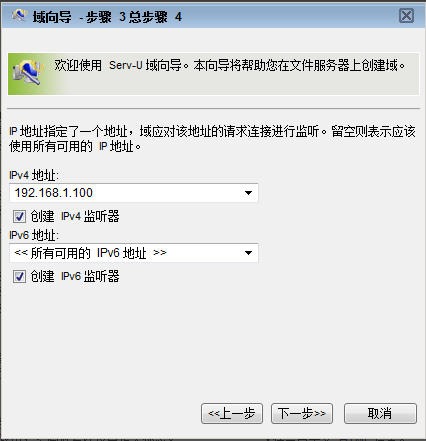
添加域名：test.com（可以填入任意内容）；设置域端口号：21（默认）；添加域 IP 地址：本地计算机的ip；



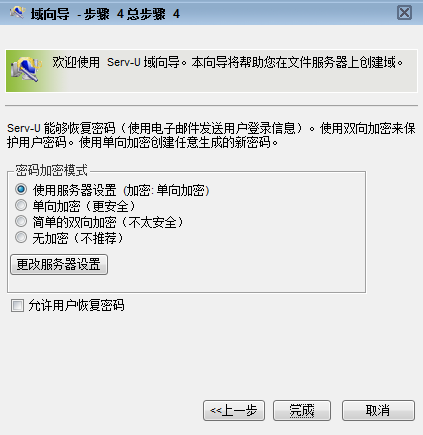
(a)添加域名



(b)设置域端口号

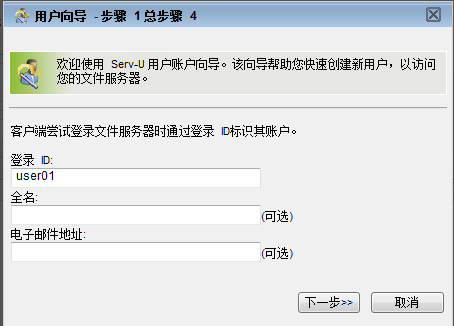


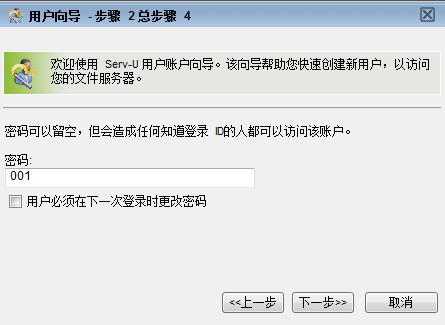
(c)添加域服务器的 IP 地址

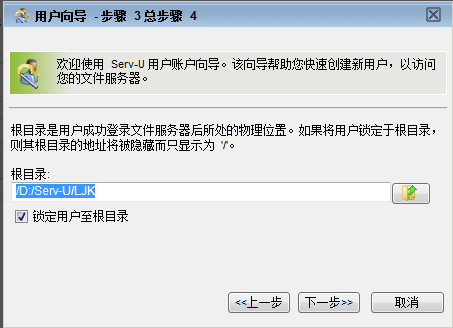


(d)设置登录密码加密方式

完成上述操作后，还需要创建用于实验的 FTP 用户帐号。打开添加新建用户向导，添加用户名：学号；添加密码：001；设置用户主目录（登陆文件夹）；设置是否将用户锁定于主目录：是（默认）。完成后界面如图 6-8 所示：







登录 ID 对于该域必须是唯一的，但服务器上其它域可能有帐户拥有同样的登录 ID。要创建匿名帐户，请指定登录 ID 为 "anonymous"，密码为空。如果需要为新建的用户设置目录访问权限，在图 6-8 的用户属性界面中，点击“目录访问”标签按钮，按照图 6-9 所示进行配置：



步骤 3：在 pc 上运行 Wireshark，开始截获报文。

步骤 4：在 PC 命令行窗口中登录 FTP 服务器，根据步骤 2 中的配置信息输入用户名和口令，参考命令如下：

C:\ >ftp

ftp> open

To 192.168.1.100 //登录 ftp 服务器

Connected to 192.168.1.100.

220 Serv-U FTP Server v6.2 for WinSock ready...

User(none): user01 //输入用户名

331 User name okay, need password. //输入用户密码

Password:001 //通过认证，登录成功

230 User logged in, proceed. //通过认证，登录成功

ftp> quit //退出 FTP

221 Goodbye!

步骤 5：停止截获报文，将截获的报文保存为 FTP-1-学号.pcap。

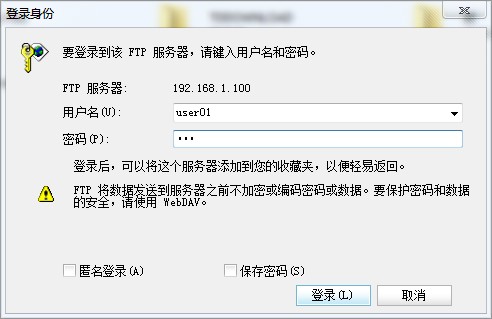
步骤 6：在 PC上再次运行 Wireshark，开始截获报文。

步骤 7：在 PC上打开浏览器窗口，地址栏输入 ftp://[ftpip]；如果未启用匿名帐户，连接断开并提示图 6-10(a) 所示对话框。如果启用了匿名帐户，则出现如图图6-10(b)所示对话框，显示出匿名帐户所允许访问的目录内容。

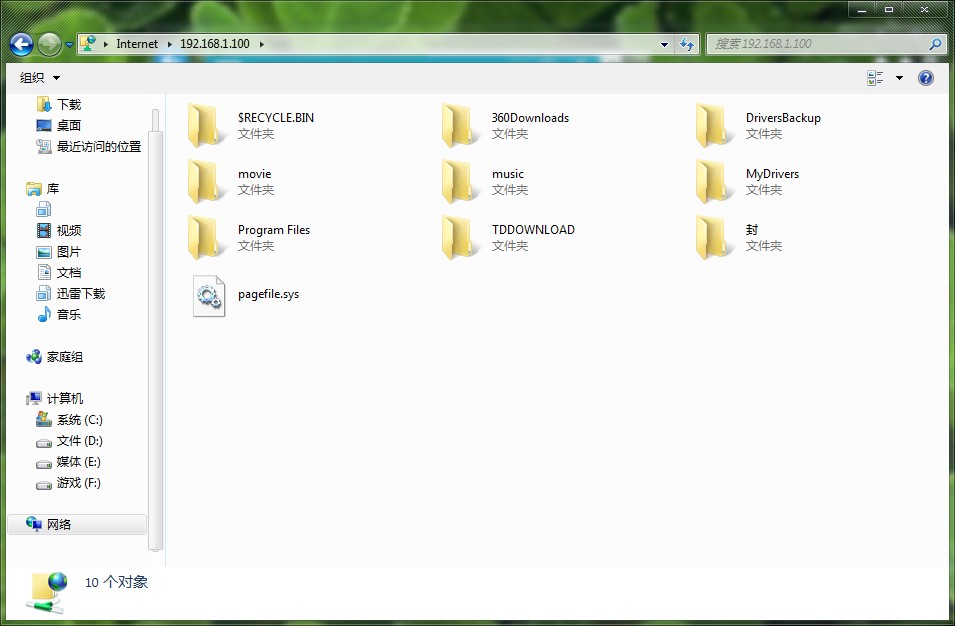


(a) FTP 文件夹错误

此时，右击窗口中空白处，弹出快捷菜单，选择“登陆…”，弹出图 6-11（a）所示登陆对话框，输入用户名 学号 和密码 001 即可登陆 FTP 服务器；



(a) FTP 登陆对话框

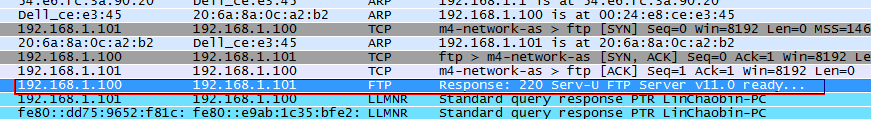
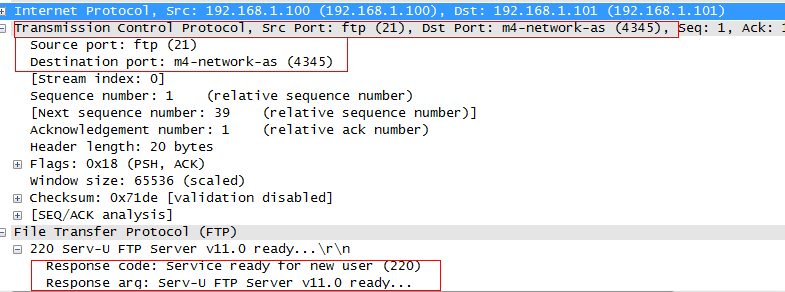


(b) 用户 user01 登陆成功界面

步骤 8：登录完成后将显示用户 学号 可允许访问的目录如图 6-11 (b)，由于该用户在该目录下的访问权限是“完全访问”，可在该用户目录下创建一个名为 ftp-学号的文件夹，并将本地的一个文本文件 f1.txt 粘贴到新建文件夹下，停止截获报文，将截获的报文保存为 FTP-2-学号.pcap。分析两次截获的报文，回答如下问题。

1）对 FTP-1-学号.pcap 进行分析，找到 TCP 三次握手后第一个 FTP 报文，分析并填写下表。

|  |  |  |  |
| --- | --- | --- | --- |
| 源 IP 地址 | 192.168.12.1 | 源端口 | 21 |
| 目标 IP 地址 | 192.168.12.1 | 目标端口 | 11956 |
| FTP 字段 | 字段值 | 字段所表达的信息 | |
| Response Code | Service ready for new user(220) | 服务ojbk | |
| Response Arg | Response arg: Serv-U FTP Server v15.1 ready... | 真的ojbk了 | |

2）在 FTP-1-学号.pcap 中找出 FTP 指令传送和响应的报文，填写下表；

|  |  |  |  |
| --- | --- | --- | --- |
| 过程 | 指令/响应 | 报文号 | 报文信息 |
| User | Request | 253 | USER gongjuren |
| Response | 255 | 331 User name okay, need password |
| Password | Request | 271 | PASS 001 |
| Response | 273 | 230 User logged in, proceed |
| Quit | Request | 317 | QUIT |
| Response | 319 | **221 Goodbye, closing session** |

3）FTP 客户通过什么命令告诉服务器自己准备用哪个端口与服务器建立数据连接的？从 FTP-1-学号.pcap 中找出相应的记录，并计算出这个端口号。

答：

通过PORT命令,在ftp>输入LS后看到



在[FTP1-10172911补充.pcap的395](ftp://FTP1-10172911补充.pcap的395)号报文

可以看到0015

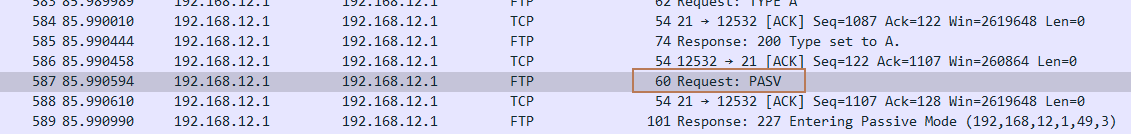
作为端口号21

4）对第二次截获的文件 FTP-2-学号.pcap 进行综合分析，观察 FTP 协议的工作过程。特别观察两种连接的建立过程和释放过程，以及这两种连接建立和释放的先后顺序，将结果填入下表。

|  |  |  |  |
| --- | --- | --- | --- |
| 报文类型 | 所包括的报文序号 | 客户端口号 | 服务器端口 |
| 控制连接的建立 | 277 | 21 | 12529 |
| 数据连接的建立 | 596 | 21 | 12529 |
| FTP 数据传送 | 599 | 12547 | 12546 |
| 控制连接的释放 | ftp1的317 | 11956 | 21 |

5）第二次截获的报文中，FTP 客户是以 PORT 模式还是 PASV 模式连接服务器？你是如何判断的？

答：

 所以PASV





6）FTP 中的匿名帐户是\_\_\_\_\_\_\_\_\_anonymous\_\_\_\_\_\_\_\_\_\_\_；

**五、实验总结**

学会了截取数据的睿智操作