Internet 顾问(连载五)

第五章 如何寻找和使用软件及其他?

Internet 是一个庞大的集程序、图象、电子杂志于一体的大仓库。本章集中讨论如何在 Internet 这个大软件库中寻找你所需要的软件。

1. 什么是 FTP?

FTP 代表文件传输协方议(File Transfer Protocol)。它是一个用来从 Internet 上的计算机上拷贝文件的工具。使用 FTP 程序,你可以登录到一台远程计算机上;向它发送文件或从它那里接收文件。FTP 与 Telnet 不同之处是:它不能用来运行程序,你只可以用它在计算机之间移动文件。

在你使用 FTP 在你的主机与远程节点之间传输文件之前,必须先登录到该远程计算机上。在使用 Telnet 时你必须有一个自己的帐户,同样地,当你使用 FTP 进入另一计算机时也必须事先获得许可。系统管理员们通常不喜欢陌生人在他们本系统的文件中游来荡去,随意加载或下载文件。

如果你拥有两台 Internet 宿主机的完全权限,你可以从其中一台上向另一台拷贝文件。这种方式通常称为特许 FTP(full - privilege FTP),坦白地讲,FTP 本身并没有什么特别吸引人的地方,但它却是 Internet 上传输文件的既成事实的标准。尽管 FTP 界面单调,用途单一,但当它和 Internet 的匿名 FTP 文档结合使用时便威力大增。

2. 什么是匿名 FTP(anonymous FTP)?

对 FTP 的大部分使用并不是用来将自己的文件在计算机之间移来移去。FTP 主要用来获得软件文档。许多软件库都支持匿名 FTP。有成千上万的节点都提供匿名 FTP 服务,可以将任何你所感兴趣的东西都下载到你的个人计算机上,从电子图书和电子杂志到卫星云图,从公用应用程序到游戏等等,任你选择。

有一些系统管理员使他们的计算机面向 Internet 上所有的用户开放,任何用户都可以进入该系统并共享其文件。与特许 FTP 不同,当你以匿名 FTP 方式进入某一节点时并不需要拥有自己的帐户,你所需的只是并不保密的一个单词:anonymous。几乎所有的 Internet 节点都支持特许 FTP,但只有一少部分允许匿名 FTP 访问。但对于 Internet 这样的庞然大物来讲,这些少量的提供匿名 FTP 服务的节点也很快变得成千上万。

其实匿名 FTP 一词并不准确。当你进入某一匿名 FTP 节点时,你并不一定是匿名的。实际上,在你传输文件之前许多节点都要求输入你的 e-mail 地址。有少数 FTP 节点对所有进出该节点的文件都作记录。所以匿名一词在这里是指任何人都可以进入该节点,而不仅仅限于拥有该计算机的特许帐户的用户。

3. 如何使用 FTP?

使用 FTP 很象使用 UNIX。一些 FTP 的命令(比如 cd. pwd 和 ls)的功能与使用方法与其在 UNIX 中一样。如果你已经对 UNIX 相当熟悉的话,那么使用 FTP 便不成问题。即使你从未用过 UNIX,也不必担心,你会发现 FTP 很好使用。

要使用 FTP,你的本地主机上必须装有 FTP 程序,并且须明确你所要连接的节点地址。在我们系统上,通常是用如下方式来启动 FTP 程序:先键入 ftp,然后在 open 后跟一个节点名,这样便打开了一个连接。你也可以直接输入:ftp 紧跟节点名,这样作可以把启动 FTP 程序和打开一个节点这两件工作结合起来。比如,要连接到 netcom 上的 FTP 服务器可以键入:

ftp ftp. netcom. com。

如果你是用自己的帐户使用 FTP(也就是说你使用的是全特权 FTP 而不是匿名 FTP),你应输入自己的用户名和口令。在允许匿名 FTP 的系统中,请用 anonymous 作为用户名。你也可能会被要求输入口令。当提示你键入口令时,应该键入你的 e-mail 地址。但这一点也并非是必须的,不过这对尹对方的系统管理员来说是一种礼貌,因为系统管理员通常希望明了是谁在使用该系统的资源与设备。有一些节点在允许你进入之前要求输入有效的 e-mail 地址,但大多数节点并不这么要求。在有些系统中你必须使用"guest"作为口令而不是 e-mail 地址。

要注意在你以匿名 FTP 方式登录到一个节点时千万不要输入自己帐户的口令。应该输入你的 e-mail 地址,或者是"guest"这个单词。

4. 如何使用 FTP 发送文件?

用 FTP 向别的节点发送文件是一个简单的过程。发送单个文件用 put 命令，发送多个文件可用 mput 命令。

比如说，在你的本地主机上的当前工作目录下包含如下五个文件：

atari-8bit-FAQ
Internet-Services-FAQ
Internet-Services-List
Internet-Tools
Privacy-Anonymity-FAQ

你可以将它们之中的任何一个或者全部发送到一个远程 FTP 节点上去。首先通过 FTP 连接到另一主机上，然后找到你所要将文件发送到的该远程机上的目的地目录，最后用 put 或 mput 将文件发送出去。比如：

put privacy-Anonymity-FAQ

将发送一个文件，而：

mput Int *

将发送本目录中的三个文件。

5. 从哪儿能得到 IBM PC 机用的软件？

Usenet 有若干个 newsgroup 是关于基于 DOS 的计算机软件的。

在 comp.binaries.ibm.pc 组中你会找到“二进制”(“binaries”)软件，也就是可以立即执行的软件，它们可以在基于 DOS 的计算机上运行，比如 IBM PC、AT 以及其他兼容机等。在最近一次查阅 comp.binaries.ibm.pc 组时，它包括了如下图所示的一些最新版本的防病毒软件：

```
17 unread articles in comp.binaries.ibm.pc -- read now? [+ynq]+
Reading overview file.
 1351 v25i085: scanv113.zip, VirusScan V113 Virus Scanner (part 01/06)
 1352 v25i086: scanv113.zip, VirusScan V113 Virus Scanner (part 02/06)
 1353 v25i087: scanv113.zip, VirusScan V113 Virus Scanner (part 03/06)
 1354 v25i088: scanv113.zip, VirusScan V113 Virus Scanner (part 04/06)
 1355 v25i089: scanv113.zip, VirusScan V113 Virus Scanner (part 05/06)
 1356 v25i090: scanv113.zip, VirusScan V113 Virus Scanner (part 06/06)
 1357 v25i091: clean113.zip, Clean-Up V113 Virus Remover (part 01/07)
 1358 v25i092: clean113.zip, Clean-Up V113 Virus Remover (part 02/07)
 1359 v25i093: clean113.zip, Clean-Up V113 Virus Remover (part 03/07)
 1360 v25i094: clean113.zip, Clean-Up V113 Virus Remover (part 04/07)
 1361 v25i095: clean113.zip, Clean-Up V113 Virus Remover (part 05/07)
 1362 v25i096: clean113.zip, Clean-Up V113 Virus Remover (part 06/07)
 1363 v25i097: clean113.zip, Clean-Up V113 Virus Remover (part 07/07)
 1364 v25i098: vshld113.zip, VirusShield V113 TSR Virus Protection (part 01/04)
 1365 v25i099: vshld113.zip, VirusShield V113 TSR Virus Protection (part 02/04)
 1366 v25i100: vshld113.zip, VirusShield V113 TSR Virus Protection (part 03/04)
 1367 v25i101: vshld113.zip, VirusShield V113 TSR Virus Protection (part 04/04)
What next? [npq]
```

关于发布在 comp.binaries.ibm.pc 组中的软件的一些讨论和出错声明，集中在 comp.binaries.ibm.pc.d 组中。关于在哪儿能找到适合 IBM PC 机使用的软件的一些问题，包括征寻启示和应答信息都包含在 comp.binaries.ibm.pc.wanted 组中。这些组只限制于散发一些公共领域内的免费软件和共享软件，并且这些软件都是基于 DOS 操作系统的。商业软件以及 OS/2 环境下的软件不在此列。

6. 在哪里能找到 Windows 版的软件？

一个巨大的专门存储基于 Windows 的共享软件和免费软件的仓库是：ftp.cica.indiana.edu:/put/pc/win3。它无所不包，从编辑到游戏软件，从波形文件到应用程序，以及 Windows NT 程序，应有尽有。你可以从这里尽情地下载自己所喜欢的软件。并且你还可以使用 Gopher 到 gopher.cica.indiana.edu 来浏览这些文档。

在 Usenet 上，可在 comp.binaries.ms-windows 中查找现成的 Windows 程序。

你还可以在许多 Usenet 论坛中看到关于 Windows 的讨论，它们是：

comp.os.ms－Windows.advocacy
comp.os.ms－Windows.apps
comp.os.ms－Windows.misc
comp.os.ms－Windows.programmer.misc

第六章　保密与安全

1. 如何保障口令的安全性？

在任何一个计算机网络系统中，口令往往都是灾难的导火索。任何一个猜中了你的口令的人都能够阅读你的电子邮件，窥视你的文件，删除你的程序，甚至以你的名义发送电子邮件和 Usenet 消息。这些无疑都是很令人感到尴尬和恼火的，同时也相当危险。

确保你的帐户的安全性相对来讲是比较简单的：你要保证你的口令是任何人都无法猜到的。如果一个口令对你来讲既好记又书写方便，那么这个口令并非是一个最佳选择，因为别人很容易猜到它。下面列出的是不宜作口令的一些单词：

·password·opensaysme·letmein·qwerty，asdfghjkl 或其他在键盘上相邻的字母组合
·你姓名的起始字母的组合
·你的登录名
·你的电话号码、身份证号码以及其他的能够根据你

的帐户号码查出的关于你的个人信息。

·字典中的任何词

·任何普通的人名(如 Steve、Quinn、Smith、Rover 等等)

为了尽可能地保证安全,你的口令应该由一串毫不相关的字符组成,比如:K＃2WW＞。使用大写字母、小写字母、标点符号以及阿拉伯数字的组合,并且确保你的口令长于六个字符。如果你觉得这样的口令很难记忆的话,你可以将两个不相关的单词用一个标点符号连接起来,用它作口令,比如:explore * grass hopper 或 get * A * life 等等。最后,不要认为你的口令越长越好,实际上有许多系统只检查口令的前八个字符。

2.系统管理员是否会看到我的口令?

在大多数大规模的计算机系统中,系统管理员不能发现你的口令。但是这一点对你并不重要,因为如果系统管理员想要查看你的文件的话,他甚至连口令都不需要。系统管理员以及其他拥有超级用户权限的用户可以随意查阅你的文件,进行拷贝、删除等等操作。这就是为什么要找一家可以依赖的服务供应商的首要原因。

在 Internet 上的有些系统中——尤其是某些种类的公告板系统——并不将你的口令从系统管理员那里屏蔽掉。因此,你决不要在多个系统中使用同一口令。如果你有多个帐户的话,你最好用多个口令。

3.我的电子邮件是否保密?

虽然电子邮件实用、快捷、使用方便,但它却不很保密。就大多数情况来说,除了你和收件人之外没有人会查阅你的电子邮件。但是,由于电子邮件是普通易读的 ASCII 文本格式文件,而且电子邮件要经过许多陌生节点才能到达信宿节点,因此电子邮件可以被看作电子明信片。

这就好比你将信件投入邮筒之后,只知道信会到达目的地,但至于路途当中会发生什么事情你却无法预知。它会在中转站被撕开吗?联邦法律禁止邮递人员私拆信件,邮递人员比起电子邮件大盗来说也更容易被抓住,因为后者可以轻松地复制你的电子邮件而不留下任何蛛丝马迹。因此我建议你在写电子邮件时要三思而后行。

4.谁能阅读我的 e-mail?

在你的宿主计算机与你的信宿节点之间的任何节点都可以截取你的 e-mail。你的系统管理员和邮件接收端的系统管理员也可以阅读它。也可以说,沿着该电子邮件的邮路上的任何用户和系统管理员都能轻松地截取和阅读你的电子邮件。

但你也不必过分担心,由于网上传输的信息量十分庞大,有人来截取和偷看你的电子邮件的可能性很小。究竟有多少信息在 Internet 上川流不息呢?在 1993 年年底,国家科学基金(National Science Foundation)统计的结果是平均每小时有 500 MB 的信息在主干网上传输,其中有百分之十七是电子邮件。如果我们假定每个 e-mail 报文平均长度为 1000 字节(10—15 行)的话,那么每秒钟将会有 8,800 个 e-mail 报文从网上经过。即使你是一个很频繁地发送 e-mail 的用户,比如每十分钟发送一封,你仍然只是沧海一粟。

因此,尽管我知道我的 e-mail 在传送途中有被截取的可能,但这种可能性非常非常小。

5.如何使文件保密?

如果你使用的是基于 UNIX 的 Internet 主机的话,文件的安全性问题便十分微秒和复杂。因为在 UNIX 系统中,每一个文件和目录都拥有自己的进入权限,这些权限与其他的文件和目录都是不相关的。换言之,如果你将主目录的权限设置成为最小级别,但该目录下的文件仍具有被别的用户读取的可能性。

解决这一问题可以分两步走。我建议输入命令:chmod 711 $HOME,该命令允许系统对诸如.forward 和.plan 文件进行正常的操作,但它将阻止用户使用 ls 命令来列出你的主目录之下的内容。更进一步,如果你打算使用你的自定义文件.login 和.profile 的话,你可以用 umask 077 命令。使用该命令后,所有由你建立的文件都被缺省设置成为只能由你对该文件进行读写和写操作的模式,其他的用户对你建立的文件将束手无策。你以后若觉得有必要的话可以用 chmod + r filename 命令来对该文件追加读的权限。如果你对你的帐户的安全保密性能不太了解的话,你可以向系统管理员寻求帮助。但一定要说明 Ls - Ld $HOME 命令的预期结果。

如果你不是在一个 UNIX 系统中的话,你的文件很可能就在你的个人计算机中,这样一来问题就简单多了。但是要记住人们仍然可以进入你的计算机浏览你的文件,因此私人数据应该进行加密处理,或者将其存在软盘上以便存放在安全的地方。(全文完)

(吴小钧 编译)