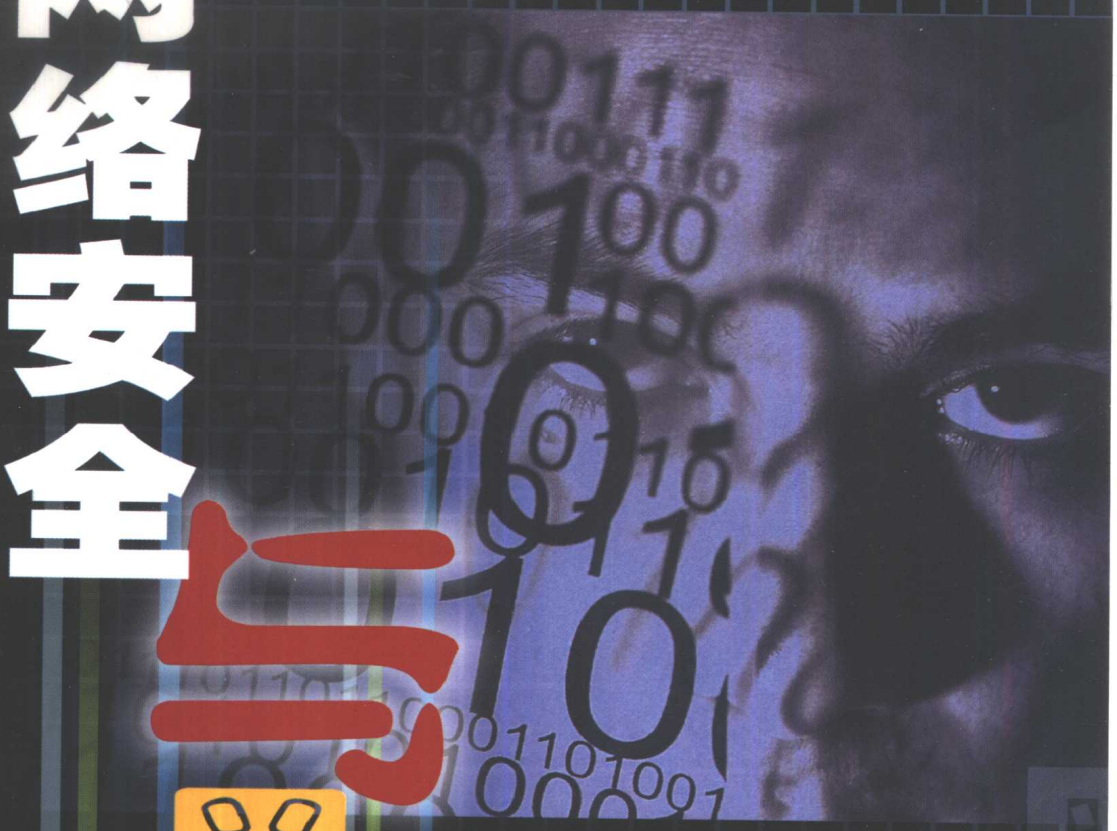
北京科海培训中心

网络安全与黑客工具防范



赵斌斌 编著

科学出版社

北京科海培训中心

网络安全与黑客工具防范

赵斌斌 编

科学出版社

2001

内 容 简 介

全书从网络安全基础知识入手，分别介绍扫描工具的防范方法、网络监听工具的防范对策、目前流行的特洛伊木马的防范对策、各类口令破解工具的防范对策、网上常用攻击工具的防范方法及常用的个人防火墙工具。

通过本书的学习，读者能够对各类黑客工具的原理有所了解，更重要的是能掌握保护系统安全的方法。本书适用于网络系统管理、维护人员和广大上网用户。

图书在版编目(CIP)数据

网络安全与黑客工具防范/赵斌斌编. —北京：
科学出版社，2001.3
ISBN 7-03-009267-8

Ⅰ.网… Ⅱ.赵… Ⅲ.计算机网络—安全技术
Ⅳ.TP393.08

中国版本图书馆 CIP 数据核字(2001)第 09379 号

科学出版社出版
北京东黄城根北街 16 号
邮政编码：100717
北京朝阳科普印刷厂印刷
科学出版社发行 各地新华书店经销
*
2001 年 3 月第 一 版 开本：787×1092 1/16
2001 年 3 月第一次印刷 印张：19 1/2
印数：1—5 000 字数：474 000

定价：25.00 元

前　言

近年来 Internet 技术的迅速发展有目共睹，电子商务的热潮更是一浪高过一浪。尽管电子商务的前景得到用户普遍的肯定，但当前在国内甚至国外都没能普及到大部分的用户群。那么究竟是什么限制了电子商务的发展呢？根据一项调查显示，在制约其发展的原因中排在第一位的就是网络安全问题。

其实网络安全问题由来已久，而且学术界和商业界早就意识到了这一点。然而这几年网络安全问题非但没有解决，反而日益严重起来。对于商业网站，经常传出被黑客攻击的消息。即使像 Yahoo、CNN 这样的网络大站也不能幸免于难。对于个人用户，也常有邮箱被炸、私人信息被窃取、系统被攻击等种种遭遇。而且这些攻击都越来越普遍，越来越易于被一般人所掌握。因为有许许多多的黑客工具来帮助攻击者发起这些攻击。这些黑客工具的存在，使得进行网络攻击不再是高级黑客的专利，而变成了像发送一封 E-mail 一样的容易。

正是这些黑客工具使得许多网站和普通用户损失惨重。尤其是一些小的从个人网站发展起来的商业网站，因为技术力量和资金都有限，面对这些攻击毫无对策。安全问题成了这些站点生存发展的关键问题。

所以本书就此提供了全面防范常用黑客攻击手段的方法和对策。我们知道，黑客使用的攻击工具都是针对特定系统的某种弱点或漏洞，当我们知道各种黑客工具的攻击原理之后，我们就更能深刻理解防范的办法。在本书的每个黑客工具的分析之后，都提供了相应的防范方法，以帮助读者保护自己系统的安全。

本书的第 1 章是网络安全基础，介绍了 Internet 安全的脆弱性与常见攻击方法，Internet 安全防范技术与产品及安全管理标准、规范与对策。

第 2 章介绍了针对网络扫描工具的防范方法。各种操作系统下的扫描器都有涉及。扫描器是黑客进攻你的系统前的预备措施，通过它，黑客可以很快地找到系统的弱点。不过，从另一方面说，扫描器的使用对于检测自己系统的安全状况也有很大作用。

第 3 章介绍了网络监听工具（Sniffer）的防范对策。这些工具包括 Windows 平台下的天行网络刺客、NetXRay、IPMan 和 UNIX 下的 Sniffit 等。这一章还通过分析网络监听的实现原理提出了具体的防范方法。

第 4 章介绍了现在流行的特洛伊木马的防范对策。这类木马工具包括最著名的 BO2000、功能最强的 SubSeven、最易用的冰河等。

第 5 章介绍了各种口令破解工具的防范对策。这些工具包括 Windows NT 口令破解工具、UNIX 口令破解工具、Windows 98 口令破解工具、Web 口令破解工具、E-mail 口令破解工具等等，涵盖了各个操作系统及多种网络服务。

第 6 章则介绍了网上一些常用攻击工具的防范方法。这些工具可以直接给对方的系统造成危害，而不是像以上几章中的工具一样只起辅助攻击的作用，因此用户对于防范这类攻击工具的要求是很迫切的。这一章的目的就是为了帮助用户防范此类黑客工具的攻击。

第 7 章介绍了常用的个人防火墙工具。对于普通用户来说，有了一个好的防火墙，就像有了一个网络安全主管，它能够全方位地保护系统的安全。

通过本书，希望读者能够对各类黑客工具的原理有所了解，更重要的是能掌握保护系统安全的方法。如果读者在本书的学习过程中能有所获益，那么本书的目的也就达到了。

也许会有人认为本书会使网络更加不安全，但如果他认真读完本书，就不会这么认为了。因为在每种工具的分析之中都贯穿了相应防御措施。这些措施无论对于网络管理员还是普通上网用户都是十分有益的。另外本书提供了一些工具的链接地址，由于众所周知的原因，笔者并不保证这些地址的长期有效性。

如果读者对本书有什么批评建议，或者想与本人探讨网络安全问题，欢迎给我来信，我的 E-mail：binbinzhao@china.com。

编　者

目 录

第 1 章　网络安全概述

随着 Internet 和 Intranet 的迅速发展，计算机网络对安全的要求已经越来越高。尤其是当今网络技术被广泛应用于社会生活直至军事战略等各个方面，所以网络安全问题已超越其本身而达到国家安全问题的高度。本章将介绍网络安全的一些基础知识。它包括 Internet 的安全状况、常见的攻击方法、Internet 安全防范技术和相关法律法规等。通过本章的学习，读者应当对网络安全有一个整体的认识。

1.1　Internet 基础

本节将介绍 Internet 的一些基础知识，包括 Intenet 的现状、技术要素和常用的服务。这些知识有助于读者理解网络安全。

1.1.1　Internet 发展与现状

Internet 的迅速发展可谓有目共睹。Internet 从 1969 年开始，最初起源于军事领域应用的目的。直到 1993 年以后，才开始应用于商业。它的发展速度是惊人的，现在，它已经覆盖了 175 个国家和地区，上网机器达数千万台，而用户数量已达到几亿人。

我国国内 Internet 的发展也是极其迅速。1987 年 9 月 20 日，钱天白教授发出我国第一封电子邮件“越过长城，通向世界”，揭开了中国人使用 Internet 的序幕。而后的这十几年里，国内 Internet 的发展日新月异。

1993 年 3 月 2 日，中国科学院高能物理研究所租用 AT&T 公司的国际卫星信道接入美国斯坦福线性加速器中心（SLAC）的 64K 专线正式开通。专线开通后，美国政府以 Internet 上有许多科技信息和其他各种资源，不能让社会主义国家接入为由，只允许这条专线进入美国能源网而不能连接到其他地方。尽管如此，这条专线仍是我国部分连入 Internet 的第一根专线。专线开通后，国家自然科学基金委员会大力配合并投资 30 万元，使各个学科的重大课题负责人能够拨号连入高能物理研究所的这根专线，几百名科学家得以在国内使用电子邮件。

1994 年 4 月 20 日，NCFC 工程通过美国 Sprint 公司连入 Internet 的 64K 国际专线开通，实现了与 Internet 的全功能连接。从此我国被国际上正式承认为有 Internet 的国家。此事被我国新闻界评为 1994 年中国十大科技新闻之一，被国家统计公报列为中国 1994 年重大科技成就之一。

1995 年 5 月，中国电信开始筹建中国公用计算机互联网（CHINANET）全国骨干网。

1995 年 7 月，中国教育和科研计算机网（CERNET）连入美国的 128K 国际专线开通。

1995 年 8 月 8 日，建在中国教育和科研计算机网（CERNET）上的水木清华 BBS 正式开通，成为中国大陆第一个 Internet 上的 BBS。

1996 年 1 月，中国公用计算机互联网（CHINANET）全国骨干网建成并正式开通，全国范围的公用计算机互联网络开始提供服务。

1997 年，中国公用计算机互联网（CHINANET）实现了与中国其他 3 个互联网络（即中国科技网（CSTNET）、中国教育和科研计算机网（CERNET）、中国金桥信息网（CHINAGBN））的互联互通。

现在我国上网计算机数达到 650 万台，其中专线上网计算机 101 万台，拨号上网计算机 549 万台。上网用户人数为 1690 万，其中专线上网的用户人数约为 258 万，拨号上网的用户人数约为 1176 万，同时使用专线与拨号的用户人数为 256 万。除计算机外同时使用其他设备（移动终端、信息家电）上网的用户人数为 59 万。CN 下注册的域名数为 99734。国际线路的总容量为：1234M。

说明：以上数据摘自 CNNIC（中国互联网络信息中心）在 2000 年 7 月公布的中国互联网络发展状况统计报告。

另外在这次调查结果中有一道题的结果值得我们特别关注：

问：如果您没有进行过网络交易，您最担心的问题是什么？

1. 交易的安全可靠性：46.01%
2. 网上提供的信息是否可靠：16.81%
3. 售后服务：12.29%
4. 是否按时交货：9.84%
5. 价格是否比较便宜：7.28%
6. 交易的界面是否简单易懂：3.94%
7. 商品品牌：1.31%
8. 其他：2.52%

我们可以看到，交易的安全可靠性是直接影响电子商务发展的主要原因。

1.1.2 Internet 发展的技术要素

庞大的 Internet 由以下几个技术要素构成：

- 使用了一个统一有效的网络互联协议族 TCP/IP；
- 在 TCP/IP 之上开发了许多出色的服务软件；
- 采用主干－地区－园区的分层网络结构；
- 较早利用光缆，保持了信息传输通畅；
- NSFnet 作为主干网络，连接大学和科研机构。

在这些要素中，TCP/IP 协议族是最基本的。TCP/IP 协议族中的协议共同工作，提供对 Internet 上数据传输的支持。也可以这么说，这些协议几乎提供了当今 Internet 上所有的实用服务，在 1.1.3 节中将会有这些服务的简单介绍。

TCP/IP 族可以分为两类，它们是：

网络层协议

网络层协议管理数据传输的具体结构，这些协议在系统一级运行，对于用户一般是透明的（不可见的）。

比如 IP（网际）协议。IP 是无连接的、不可靠的数据报协议，主要负责在主机之间寻址和选择数据包的路由。

无连接意味着交换数据之前不能建立会话。不可靠意味着传递没有担保。IP 总是尽力传递数据包。IP 数据包可能丢失、不按顺序传递、重复或延迟。IP 不尝试从这些错误类型中恢复。所传递的数据包的确认以及丢失数据包的恢复是更高层协议的责任，如 TCP。

IP 数据包，也称作 IP 数据报，由 IP 报头和 IP 负载组成，如图 1.1 所示。

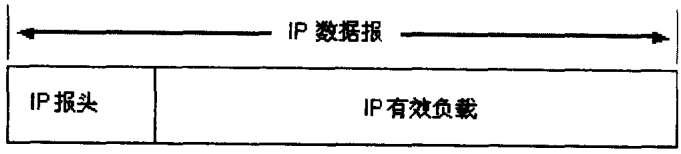


图 1.1　IP 数据包的格式

IP 报头包含如表 1.1 所示的字段用于寻址和路由：

表 1.1　IP 报头字段及其功能

IP 报头字段	功能
源 IP 地址	IP 数据报最初的源 IP 地址
目标 IP 地址	IP 数据报最终的目标 IP 地址
生存时间（TTL）	指定数据报被路由器丢弃之前允许通过的网段数量。TTL 是由发送主机设置的，以防止数据包不断在 IP 互联网络上永不终止地循环。转发 IP 数据包时，要求路由器至少将 TTL 减小 1

除非用户使用一些监听工具（Sniffer），否则用户不会看到系统中 IP 的工作。

为使数据的路由选择和传递成为可能，连接到 Internet 上的计算机都必须有一个惟一的地址，也就是 IP 地址。

每个 TCP/IP 主机由逻辑 IP 地址标识。这个地址对每个使用 TCP/IP 通讯的主机来说是惟一的。每个 32 位 IP 地址标识网络上系统的位置，就像街道地址标识城市街道上的住宅一样。每个 IP 地址内部都分成两部分，网络 ID 和主机 ID：

- 网络 ID，也叫做网络地址，标识大规模 TCP/IP 网际网络（由网络组成的网络）内的单个网段。连接到并共享访问同一网络的所有系统在其完整的 IP 地址内都有一个公用的网络 ID。这个 ID 也用于惟一地识别大规模的网际网络内部的每个网络。

- 主机 ID，也叫做主机地址，识别每个网络内部的 TCP/IP 节点（工作站、服务器、路由器或其他 TCP/IP 设备）。每个设备的主机 ID 惟一地识别所在网络内的单个系统。

下面是一个 32 位 IP 地址的范例：

10000011 01101011 00010000 11001000

要简化 IP 寻址，IP 地址用带句点的十进制符号表示。32 位 IP 地址分成 4 个 8 位字节。8 位字节数转换成十进制数（基数是 10 的编号系统），并用英文句号分隔。因此，前面的 IP 地址范例转换成带句点的十进制数就是 131.107.16.200

Internet 团体定义了 5 种类型的地址：A 类、B 类和 C 类地址，用于指派 TCP/IP 节点，D 类、E 类保留。

地址类定义了每个地址的网络 ID 和主机 ID 使用哪些位。地址类还定义了每个网络能支持多少网络和主机。

表 1.2 用 w.x.y.z 指定任意给定 IP 地址中的 4 个 8 位字节数。这个表用于显示：

- 任意给定 IP 地址的第 1 个 8 位字节数（w）如何有效地表示地址类。
- 地址中的 8 位字节数如何分成网络 ID 和主机 ID。
- 每个网络可用于每个类的可能网络和主机数量。

表 1.2 IP 地址类定义结构

类别	w 的值	网络 ID	主机 ID	网络数量	每个网络的主机数量
A	1~126	W	x.y.z	126	16，777，214
B	128~191	w.x	y.z	16，384	65，534
C	192~223	w.x.y	Z	2，097，152	254
D	224~239	为多播寻址保留	N/A	N/A	N/A
E	240~254	为实验性应用保留	N/A	N/A	N/A

提 示

因为 IP 地址标识网络上的设备，所以网络上的每个设备都必须分配惟一的 IP 地址。通常，多数计算机只安装一个网卡，因此只需要一个 IP 地址。如果计算机安装了多个网卡，则每个适配器都需要自己的 IP 地址。

显然，IP 地址是难以被用户记住的。于是，Internet 允许为每台计算机命名，并允许用户通过输入计算机名字来代替其 IP 地址。为了实现计算机名到 IP 地址的转换，Internet 提供了专门的服务：DNS（Domain Name System）。

计算机在 Internet 上的名称称为域名（Domain Name）。下面就是一台服务器的域名：

infosec	.cs .pku.	edu.	cn
机器名	单位	领域	国家（地区）

它表示的是中国（cn）教育网（edu）北京大学（pku）计算机系（cs）一台名为 infosec 的计算机。图 1.2 显示了 DNS 的基本使用方法，DNS 根据计算机名称搜索其 IP 地址。

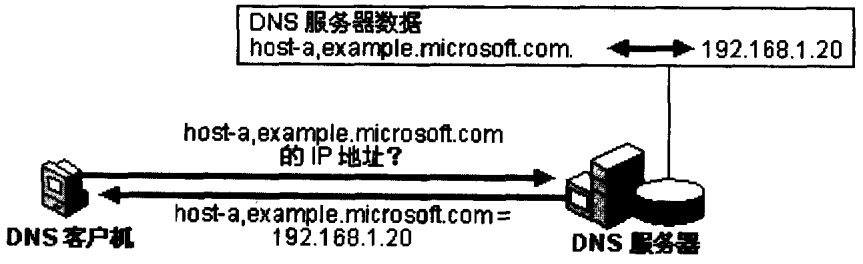


图 1.2　域名解释示意图

本例中，客户机查询服务器，请求配置成使用 host-a.example.microsoft.com 作为其 DNS 域名的计算机的 IP 地址。由于服务器能够根据其本地数据库应答查询，因此服务器将以包含所请求信息的应答回复客户机，即包含 host-a.example.microsoft.com 的 IP 地址信息的主机（A）资源记录。

此例显示了单个客户机和服务器之间的简单 DNS 查询。实际上，DNS 查询比这更复杂，而且包含此处未显示的其他步骤。详细信息，请参阅相关书籍。

应用层协议

与网络层协议不同，应用层协议的有些部分对于用户是可见的。如文件传输协议（FTP）。用户请求与某个 FTP 服务器建立连接，传输数据。在命令执行过程中，用户可以看到本地机器与远方主机之间的部分交换信息。比如正在执行的命令的结果、状态的改变、文件传输的字节数等。

1.1.3　Internet 服务

下面将介绍 Internet 上常见的一些服务（Telnet FTP WWW SMTP），这些服务相对来说应用极广泛，而且存在的安全性问题也比较严重。现在黑客的攻击目标也是这些常见的服务。其他的一些服务，如 GOPHER、WHOIS、NEWS 等，因为现在使用得不多，这里就不一一介绍了。

远程登录（Telnet）

在 RFC854 中对 Telnet 的定义是这样的：

“远程登录协议的目的是提供一个全面的、双向的、面向 8 比特字节的通讯工具，其目标是提供终端设备与面向终端进程建立接口的标准方法。”

Telnet 允许执行被登录主机上的命令和程序，就像在本地运行一样。要使用 Telnet，你只需启动 Telnet 客户程序。在 UNIX 下，使用的命令格式如下：

```
# telnet www.host.com
```

这个命令向 www.host.com 发出一个 Telnet 连接请求。

在 Windows 下，选择：“开始”->“运行”，在弹出的窗口中键入：telnet www.host.com，如图 1.3 所示。

图 1.3 使用 Telnet 连接服务器

如果 host 运行有 Telnet 服务的话，一般会出现登录界面。如果用户的账号口令验证正确，就得到一个 Shell，在这个 Shell 里，你可以与在控制台上一样运行你的账号权限内的所有程序。

文件传输协议（FTP）

文件传输协议（FTP）是从一台计算机传输文件到另一台计算机的标准方法。在 Windows 下常见的 FTP 客户端软件有：Cute_Ftp，Ws-Ftp，Leep FTP 等。对于黑客们而言，他们是不会使用这些软件的，而是使用 UNIX 或 Windows 自带的命令行方式的 FTP 程序，这样他们才可以做更多的事。

图 1.4 是使用 Windows 自带的 FTP 程序连接一个 FTP 服务器的状况。

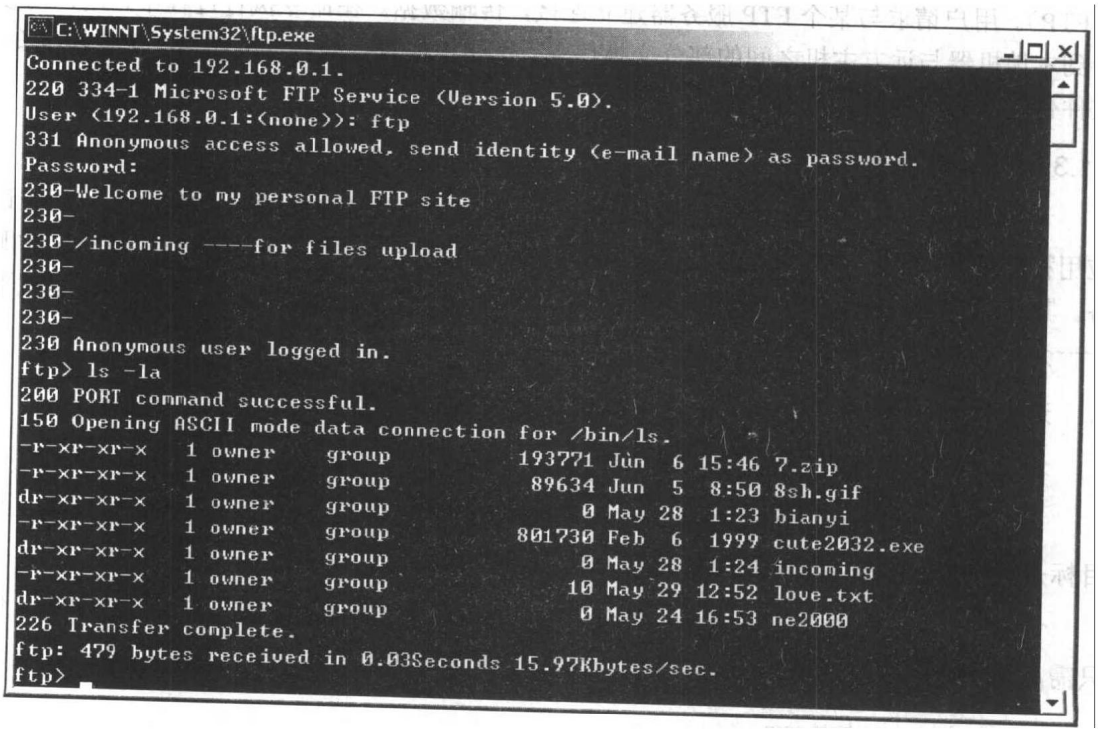


图 1.4 FTP 使用示意图

如果读者想了解 FTP 的具体命令，请查阅相关书籍。

邮件服务（SMTP——简单邮件传输协议）

该协议的目的在 RFC 821 中有明确的描述：

“简单邮件传输协议的目的是可靠并且高效地传输邮件。”

SMTP 是一个非常简洁和高效的协议。用户发出连接请求给 SMTP 服务程序，就可以建立双向连接。然后就可以进行交互式的执行命令。尽管 SMTP 很简单，但邮件服务已经带来了很多的安全漏洞（主要是因为错误的配置）。

WWW 服务

WWW 服务是当今互联网上最流行最重要的服务。该服务通过 HTTP（超文本传输协议）实现。WWW 使得 Internet 更大众化。人们可以使用普通的浏览器，如：Netscape Navigator 或 Internet Explorer 来浏览互联网上丰富的网站。对于 WWW 页面上的每个元素（文本、图像、声音），浏览器都会及时地通知服务器。这样，它将首先读取文本，然后是图像文件、声音文件。

HTTP 并不特别关心请求的数据类型，多媒体的各种成分都可以嵌入 WWW 页面之中。而且 WWW 页面中也可以包含其他的协议，包括 FTP、Telnet 等。经常可以看到有连接到 FTP 站点的链接，比如：ftp：//www.download.com.cn/tools/oicq21b.exe

WWW 服务是安全问题比较突出的，相信读者肯定听说过某某网站被黑客攻击的事件。服务器漏洞、不安全的 CGI 程序、错误的配置都可能是不安全因素。

1.2　Internet 安全的脆弱性与常见攻击方法

俗话说：“知己知彼，百战不殆。”现在就让我们看看 Internet 的脆弱性与常见的攻击方法。

1.2.1　Internet 的脆弱性

我们从两个方面来看 Internet 的脆弱性：

1．从用户角度看

- 对信息被他人利用缺乏控制能力；
- 对信息的漏失或不正当的接触与利用存在疑虑；
- 对政府以处理案件为由而截收信息的动机存在不信任感；
- 担心自己的计算机系统遭到外界的破坏（包括怀有敌意的破坏和收到大批电子邮件广告）；
- 最迫切需要使用时出现计算机系统故障的风险；
- 有关个人钱财、健康状况、购物习惯等信息被窃取。