系统安全与黑客防范手册

精英科技 编著

中国电力出版社
www.infopower.com.cn

系统安全与黑客防范手册

精英科技 编著

中国电力出版社

内 容 提 要

本书讲解了网络安全和系统防护的各方面知识，为读者找出系统缺陷、增强系统安全提供了帮助。

本书共分 16 章，依次介绍了网络安全与网络编程基础知识、黑客攻击手段、黑客工具、计算机网络安全与防范。基础知识部分主要介绍了网络协议、操作系统和网络编程等内容。接下来的两部分着重对扫描工具、特洛伊木马、网络监听工具做了深入剖析，最后一部分则从防火墙、操作系统安全、Internet 安全及系统管理员安全等角度讨论了如何确保网络系统的安全。

本书适合具有一定网络安全和系统维护基础的读者阅读。

图书在版编目（CIP）数据

系统安全与黑客防范手册/精英科技 编著.-北京：中国电力出版社，2001

ISBN 7-5083-0738-0

Ⅰ.系… Ⅱ.精… 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 066548 号

TN391/06

中国电力出版社出版、发行

（北京三里河路 6 号 100044 http://www.infopower.com.cn）

三河市实验小学印刷厂印刷

各地新华书店经售

*

2002 年 1 月第一版 2002 年 1 月北京第一次印刷

787 毫米×1092 毫米 16 开本 32 印张 717 千字

定价 **45.00** 元

前　言

信息网络国际化、社会化、开放化、个人化的特点使国家的“信息边疆”不断延伸，甚至到了每一个上网者个人。我们借助网络漫游在虚拟世界之中，远程教育、网上(在家)办公、网上购物、网上炒股、电子商务等都已经成为现实。同时国际上围绕信息的获取、使用和控制的竞争愈演愈烈，信息安全成为维护国家安全和社会稳定的一个焦点，各国都给予了极大的关注与投入。对于我们消费者来说，是什么原因使我们的顾客仍然不敢也不愿意通过 Internet 进行交易呢？为什么在我们为企业架设网络的时候总是要问一个类似的问题：这个和 Internet 连接的计算机网络会不会被黑客利用？是的，这个重要的原因就是“安全”。

信息安全的概念在 20 世纪经历了一个漫长的历史阶段。从信息的保密性（保证信息不泄漏给未经授权的人）扩展到信息的完整性（防止信息被未经授权的篡改，保证真实的信息从真实的信源无失真地到达真实的信宿）、信息的可用性（保证信息及信息系统确实为受权使用者所用，防止由于计算机病毒或其他人为因素造成的系统拒绝管理）、信息的不可否认性（保证信息行为人不能否认自己的行为）等。信息安全需要“攻、防、测、控、管、评”等多方面的基础理论和实施技术。

然而，现在通常有一种误解，以为网络安全纯粹是技术上的事。实则不然，这里我们需要强调的是网络安全并不仅仅是技术问题，而是一个认识问题，是一个社会问题。随便打开哪个计算机方面的网站，都能找到“黑客”或“病毒”方面的字样。但可以说，许多这方面的报道都部分地夸大了，有的就是为了吸引注意力。这往往造成反面影响，使得大家都认为那些破坏网络安全的人在技术上都是“天才式”的人物，从而无意中吸引了一些想要证明自己是“高智商”的年轻人的注意。于是，产生了希望能突破别人安全系统，干点能证明自己能力的事的人，也不考虑违法不违法了。这种误解的另一方面使大多数人觉得，网络安全是高深莫测的事，是技术人员的事。其实，网络安全，人人有责。比如，在一家公司里，你有一个账号能访问公司服务器上的一些商业机密文件。但你无意中将你的账号和密码泄露了出去，或你的账号和密码能很容易被“黑客”攻破。这就对你的公司的网络安全构成了威胁。如果你在网上购物，没有注意到相关的安全事项，可能会对你的经济带来威胁。对于网络安全技术来讲，有道德的人就能用来保护社会利益，而邪恶之徒则用来从社会或他人之处获取非法利益。这些都是从一个人的社会价值取向来决定的，从而，使得网络安全也成为了一个社会问题。

从理论上讲，没有一个计算机系统是绝对安全的。除非你不开机，或将它放在保险箱里，与外界没有任何联系。因此，为了验证系统的安全性，最好的办法就是想办法突破这个系统，发现这个系统的缺陷。那么突破或者叫作入侵应该是讲解网络安全技术的基础。只有对入侵方法有了充分的认识后，才能对系统的缺陷进行分析，找出问题的所在，才能从根本上增强系统的安全性。本书在介绍一些黑客手段及技术的同时，特别注意让读者掌握如何从安全角度重新考虑和分析这些问题。这也可以说是本书的一个特点。下面我把本书的轮廓向大家作一个介绍。

本书分为四个部分：网络安全与网络编程基础知识、黑客攻击手段揭密、黑客工具及计

算机网络安全与防范。

在基础知识部分中，我们主要介绍了网络协议（TCP/IP）、操作系统和网络编程等内容。其中一些可能对初学者存在一些困难，但如果不是从事专业研究，不用抠得很细，主要是有些基本的知识以后可以为后续各章打下良好的基础。接下来的两部分我们对黑客的攻击手段及常用的工具做了比较深入而全面的介绍，这里我们着重对经典扫描工具、特洛伊木马、网络监听工具做了深入的剖析，然后给出几个黑客攻击的实例，供大家研究。相信读者在阅读之后不会再对黑客感到神秘和恐惧。在熟悉了形形色色的黑客手段，了解了威胁网络安全的各种根源以后，最后一部分里我们从防火墙、操作系统安全、Internet 安全以及系统管理员安全等诸多角度讨论了如何确保我们计算机网络系统的安全，几乎涵盖了现在普遍使用的所有安全手段。

这本书无论是对刚刚对黑客技术产生兴趣的读者，还是已经具备了一定专业知识的从业人员都具有极大的参考价值。由于编者水平有限，对一些问题理解不深，同时成书仓促，书中难免存在相当多的错误，希望能给予批评指正。

目　录

前　言

第 1 章　TCP/IP 原理与技术概述 1
1.1　不同的协议层 1
1.2　路由器和路由协议 6
1.3　域名系统 7
1.4　标准服务 9
1.5　基于 RPC 的协议 13
1.6　文件传输协议 17
1.7　r 命令 20
1.8　信息服务 21
1.9　X11 系统 24
1.10　信任模式 25

第 2 章　套接字选项和 I/O 控制命令 26
2.1　套接字选项 26
2.2　IOCTLSOCKET 和 WSAIOCTL 51
2.3　小结 62

第 3 章　原始套接字 63
3.1　原始套接字的创建 63
3.2　Internet 控制消息协议 64
3.3　Internet 组管理协议 67
3.4　IP_HDRINCL 的使用 68
3.5　小结 71

第 4 章　黑客行径概述 72
4.1　攻击的目的 72
4.2　攻击类型 74
4.3　实施攻击的人员 83
4.4　攻击的三个阶段 84

第 5 章　扫描 85
5.1　什么是扫描器 85
5.2　工作原理 85
5.3　经典扫描工具 SATAN 85
5.4　端口扫描工具 150

5.5 其他扫描工具 162

第 6 章 特洛伊木马简介 165

6.1 特洛伊木马简介 165
6.2 木马的类型 166
6.3 冰河浅析 167
6.4 BO2000 173
6.5 如何破解木马 180
6.6 一个典型特洛伊木马的源程序 212

第 7 章 网络监听工具 216

7.1 网络监听的原理 216
7.2 网络刺客 217
7.3 sniffer 218
7.4 检测网络监听的方法 229

第 8 章 缓冲区溢出攻击 231

8.1 缓冲区溢出的概念和原理 231
8.2 缓冲区溢出的漏洞和攻击 232
8.3 缓冲区溢出的保护方法 233
8.4 有效的组合 238
8.5 结论 238

第 9 章 攻击 Web 服务器 239

9.1 如何攻击服务器 239
9.2 IIS 安全 243
9.3 CGI 安全性 250
9.4 使用他人 CGI 脚本时的注意事项 272

第 10 章 其他常见最新攻击漏洞 274

10.1 Windows 2000 安全漏洞 274
10.2 ASP 漏洞 276
10.3 Windows NT 漏洞 278

第 11 章 黑客入侵过程实例 286

11.1 黑客入侵策略 286
11.2 SQL 攻击 288
11.3 聊天类 攻与防 298
11.4 一次入侵过程的公开分析 301
11.5 总结 310

第 12 章 TCP/IP 安全 311

12.1 TCP 安全 311
12.2 IP 安全综述 314

第 13 章　防火墙 325
13.1　防火墙的工作原理 325
13.2　防火墙的安放位置 326
13.3　数据包过滤网关 327
13.4　应用级网关 345

第 14 章　基本的加密技术 375
14.1　密码基础知识 375
14.2　加密技术的实践应用 PGP 378

第 15 章　Intranet 网络系统安全指南 420
15.1　企业网络系统的部署和安排 421
15.2　企业网络系统安全的几项关键技术 425
15.3　认证 450
15.4　秘密联络：虚拟专用网络（VPN） 451
15.5　病毒防火墙 462
15.6　企业 Intranet 应用实务的安全事项 467
15.7　企业实务应用中的安全事项 471

第 16 章　Windows NT 与网络安全 474
16.1　Window NT 安全基础 474
16.2　Window NT 安全机制 477
16.3　Window NT 网络安全配置及应用 484

第 1 章　TCP/IP 原理与技术概述

20 世纪 60 年代初，DARPA（美国国防部高级研究项目局）投资建立了一个项目，通过一个名为 ARPANet（阿帕网）的网络将全国各地的大学及硬件部门连接起来。1983 年，TCP/IP 协议取代了早先的 ARPANetNCP（网络控制协议）。用来运行这个网络的 TCP/IP 协议是开放、简单和易于使用的。网络的规模迅速扩大，最终成为现在人所共知的 Internet（因特网）。Internet 也就是运行 TCP/IP 协议套件的所有网络的一个大集合。在 80 年代，人们普遍使用的还有另一些网络协议体系——ISO（国际标准化组织）的 OSI、IBM 公司的 SNA 以及 DEC 公司的 DECnet 等等。然而，所有这些协议没一个是简单的，也不像 TCP/IP 那样是开放的。正是由于这个原因，TCP/IP 协议套件才得到了广泛的实施、开发和支持。

所有网络协议体系均包括下述基本组件：

协议堆栈——由相互间通信、高效率传输数据包的各个层构成。

定址系统——提供独一无二标识一个目的地（目标主机）的能力。为了实现大范围内的通信，有必要将通信实体惟一地标识出来。

路由（选择）——决定一个特定数据包的传送路径，令其最终抵达目的地，这就是所谓的“路由选择（Routing）”。

TCP/IP 不是一个单一的协议，事实上是一组数据通信协议集，其中的每个协议提供一些特定的服务。这些协议包括从一台机器到另一台机器传递信息的路由、电子邮件和新闻的发送，甚至远程登录的使用。本章将简要介绍 TCP/IP 协议簇。虽然这些内容对很多读者来说是非常熟悉的，但仍建议不要跳过这一章。这里的重点是在 TCP/IP 的安全上，故突出讨论了协议和可能危险的领域，然后对 TCP/IP 的安全做了详尽的阐述。

1.1　不同的协议层

TCP/IP 是一个通信协议集的缩写。

图 1-1 示出了这一数据流的方案。每一横排都是一个不同的协议层（protocol layer）。顶层包括各种应用：邮件传送、登录、视频服务等等。它们调用较低层对数据进行存取和递交。在蜘蛛网络的中间部分就是网际协议（Internet Protocol，IP）[Postel,1981b]。IP 是一种数据包多路复用器，由较高层协议来的报文都有一个 IP 报头预先挂在数据包上，然后它们被送到相应的设备驱动器上以便于传输。下面将首先进行对 IP 层的研究。

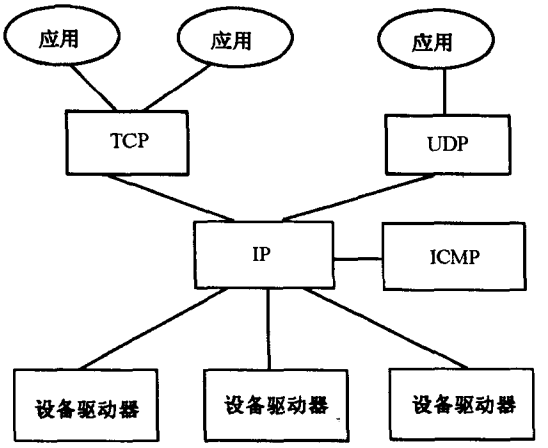

图 1-1 涉及 TCP/IP 不同层协议的示意图

1.1.1 IP

IP 数据包（packet）是一捆一捆的数据，它是 TCP/IP 协议簇的基础数据形式。每个数据包都携有一个 32 位的源地址、宿地址、一些选项位、一个报头校验和以及数据包的有效数据。一个典型的 IP 数据包有几百个字节长。这些数据包数十亿次地通过以太网、串行通信线、FDDI 环路、数据包无线连接、异步传输模式（ATM）链路等在世界上穿越流动。

IP 层没有虚拟电路（virtual circuit）或“电话呼叫”的概念：每个数据包都是独立的。IP 是一种不可靠的数据报（datagram）服务方式。数据包的递交是没有保证的，它只被递交一次，或按任意一种特定顺序递交。对数据包的正确性没有任何检验机制。IP 报头中的校验和也只覆盖该报头。

事实上，送出的数据包是否真的来自某一给定源地址也是没有保证的。从理论上讲，任何主机都可用任意一个源地址发送一个数据包。虽然有许多操作系统在这一方面实行控制并确保它按正确的源地址值发出，但是，除非在某一小心控制的环境下，否则就不能依赖源地址的有效性。一般来说，鉴别和安全问题必须利用较高层协议的机制。

一个长距离传送的数据包将经过多个跳点（hop）。每次跳转都终止于一个主机或路由器上，然后根据路由信息将该数据包向前传送至下一个跳点。在传送期间，如果数据包对于一个跳点显得过长，则该数据包可以被分割成更小的数据片。如果通信过于拥挤堵塞，路由器可以将数据包丢弃。数据包在到达远端时可能不按顺序，甚至还可能有重复发送。通常对这些行为是不通知的：较高协议层（例如 TCP）才处理上述问题，并给应用提供一条可靠电路。

如果一个数据包对下一个跳点显得太大，它就要被分割成小包，即将其分为两个或更多的数据包，每个数据包都有它自己的 IP 报头，而有效数据只是原来的一部分。这些小片以各自的方式分别到达最终目的地。在传输过程中，分片的数据包还可能进一步分片。在这些小片数据包到达目标机器时，它们被重新组装。中间跳点均不进行组装。

1. IP 地址

IP 中的地址是一个 32 位长的数字，被分成两个部分，分别是网络部分和主机部分。其准确的边界取决于地址的头几位，详细情况示于表 1-1。主机地址部分为全“0”和全“1”

的地址，均为保留地址。

表 1-1　地 址 格 式

类　别	高　位	网络部分（位）	主机部分（位）	地址总数
A	0	7	24	16777214
B	10	14	16	65534
C	110	21	8	254
D	1110	多目传送组（实验用）		268435456
E	1111			——

一般来说，地址中的主机部分又进一步划分为子网和主机地址。子网地址用于组织机构内的路由。用于子网的位数由本地决定，一种最通用的策略是把一个 B 类网络划分成 254 个子网。

然而大多数人并不实际使用 IP 地址，他们宁愿使用域名。这个域名通常由一个叫做域名系统（Domain Name System）的特殊分布式数据库进行转换。

这些子网分割方案正在浪费地址资源，并将最终造成因特网用完 IP 地址，虽然有约 32 个主机可以连入因特网也仍是远远不够。现在有人已经提出了一些改变 IP 地址格式以大量扩展地址空间的计划，但是尚未付诸实施。

2. IP 安全标签

IP 有许多可以表达信息的选项字段，但人们通常都不用它们。对于我们的目的，重要的选项是安全标签以及严格限制和放松源路由的选项。

IP 安全选项［Housley,1993;Kent,1991］目前主要用于军事场合，虽然也有人主张将这一选项定义为一个商业变量。每个数据包都用它包含信息的敏感性进行标记。这个标签包括一个安全级别（机密、绝密等）和部门：核武器、密码学等。

讨论完整的安全标签和强制性访问控制（mandatory access control）远远超出了本书的范围，这里只作一个极为简要的概述。第一，标签指出了发送和接受进程的最终安全级别。一个进程不得用较低安全级别的方式写到介质上，因为那样会泄露机密信息。基于显而易见的原因，也许不需要从介质中读出更高级别的信息。通常将这两种限制相结合，用来限定连接两端的进程处于准确的相同级别上。要了解更多的信息可参见[Amoroso，1994]。

某些系统，例如 Unix 系统 V / MLS［Flink and Weiss,1988,1989］，对每个进程都维持着一个标签。因此它们可以把相应的选项字段贴在每个数据包上。在更传统的计算机上，路由器可以将这选项贴到通过给定电缆接收的所有数据包上。

在网络自身内部，安全标签的主要目的是包含路由决策。一个有“绝密”标记的数据包，不得经过表明为只供“最低秘密”级通信的链接进行不安全传送。第二个用途是控制密码装置。如果采用等级为“绝密”的算法和密钥进行适当加密，那么同一数据包的确可以经过不安全电路予以路由。

1.1.2　ARP

IP 数据包常通过以太网发送。以太网设备并不识别 32 位 IP 地址：它们是以 48 位以太网地址传输以太网数据包的。因此，IP 驱动器必须把 IP 目的地址转换成以太网目的地址。

在这两种地址之间存在着某种静态的或算法的映射，常常需要查看一张表。地址解析协议（Address Resolution Protocol，ARP）［Plummer,1982］就是用来确定这些映像的。

ARP 工作时，送出一个含有所希望的 IP 地址的以太网广播数据包。目的地主机，或另一个代表该主机的系统，以一个含有 IP 和以太网地址对的数据包作为应答。发送者将这个地址对高速缓存起来，以节约不必要的 ARP 通信。

如果有一个不被信任的节点对本地网络具有写访问许可权，那么也会有某种风险。这样一台机器可以发布虚假的 ARP 报文，并将所有通信都转向它自己，然后它就可以扮演某些机器，或者顺便对数据流进行简单的修改。

ARP 机制常常是自动起作用的。在特别安全的网络上，ARP 映射可以用固件，并且具有自动抑制协议达到防止干扰的目的。

1.1.3 TCP

传输控制协议（Transport Control Protocol，TCP）［Postal，1981c］为用户进程提供可靠的虚拟电路。丢失或受损的数据包都被重传。如有必要，进来的数据包被重组，以便与原来的传输顺序匹配。

顺序是按每个数据包中的序列号（sequence number）来维系的。每个被发送的字节，以及开放和关闭请求，均被单独标上不同的序列号（见图 1-2）。除最开头的那个数据包外，在一个会话期间，传输的所有数据包都包括一个确认号，它给出了下一个成功接收的序列字节的序列号。

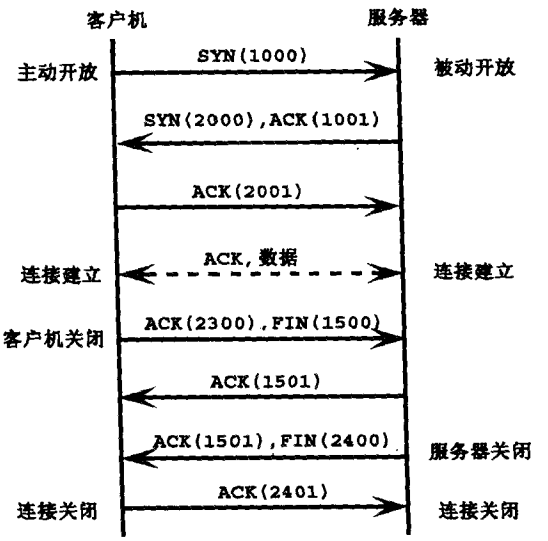

图 1-2 TCP 会话样图

每个 TCP 报文都被标记为来自一个特定的主机和端口号（port number），以及抵达的目的地主机和端口号。以下四元：

＜本地主机，本地端口，远程主机，远程端口＞

惟一地标识了一个特定的电路。同一台机器上许多不同的虚拟电路拥有相同本地端口号，不但是允许的，而且是十分普遍的。只要远程地址和端口号不同，每条虚拟电路就都能正确地

工作。

SYN（同步或开放请求）位置位的初始数据包，传输连接自己的初始序列号。初始序列号是个随机数。此后所有发出的数据包都带有置了位的 ACK（确认）。注意 FIN（最终）的确认位以及独立的关闭操作。

服务器（server）——希望通过 TCP 提供某些服务的进程——在一个特定端口上进行侦听（listen）。按惯例，服务器端口号的数字较低。这种常规并不总是好事，有时也可能产生安全问题。我们将在后面看到这一点。所有标准服务器的端口号都假定为对调用者是知道的，侦听端口从某种意义上说是半开放的，只有本地主机和端口号是已知的（严格地讲，甚至本地主机地址都是不必知道的，因为计算机上可能有不止一个 IP 地址，而连接请求通常能够连接到机器的合法地址中的任何一个地址上）。在一个连接请求数据包到达后，数据包中的其他字段就被填写。如果合适，本机操作系统将复制该侦听连接，以便对同一个端口的进一步请求也可以进行。

客户机（client）使用提供的服务。客户进程在它们的本地主机上很少要求有特定的端口号，虽然也允许这样做。它们通常接受本地操作系统通过选择而指定给它们的端口号。

大多数 Unix 系统的 TCP 和 UDP 都强制性地规定，只有超级用户（root）可以产生一个小于 1024 的端口号。这些都是特权端口（privileged port）。其意图在于远程系统能够信任写到这些端口上的鉴别信息。这种限制仅是一种惯例，而并不是协议规范必须要求的，故某些合适的工具不必遵守这一惯例。无论如何，在像 PC 这样的单用户机器上这个问题是毫无意义的。真实的含义很清楚：只有当其确保源系统有这样一条规定，有强制执行的能力并得到合适的管理时，才可相信端口号是神圣不可侵犯的。

前面提到过的序列号还有另外的功能。由于一个新连接的初始序列号需经常改变，因而 TCP 可以探测来自以前同一电路（即来自以前使用过的相同的四元地址和端口号）上的陈腐数据包。这具有最现实的安全利益：除非连接的两端都已对对方的初始序列号予以确认，否则不能建立完全的连接。如图 1-2 中第三条线。

这里也潜伏着威胁。如果一个攻击者能够预测到目标机器选择的（序列号）起始点——Morris 认为在一定条件下这的确是可能的［Morris,1985;Bellovin,1989］——那么，攻击者就有可能欺骗目标机器，让其相信它正与一台可信任的机器对话。那时，依赖于 IP 源地址进行的鉴别（例如，在 1.7 节中讨论的 r 命令），就可以被用来穿透目标机器系统。这就叫做序列号攻击（sequence number attack）。

进而有两点也值得注意。第一，Morris 所说的攻击依赖于能够生成一个到目标机器的合法连接。如果这些连接被防火墙等所阻断，那么攻击就不会成功。另外，一个网关机器如果扩展到对内部机器有太多的信任，它本身也会是脆弱的，这取决于所涉及的准确配置情况。第二，序列号攻击的概念可以推而广之。除 TCP 外的其他许多协议，同样是脆弱的［Bellovin,1989］。实际上，TCP 建立连接的三次握手机制，提供了比其他协议更多的保护。

1.1.4　UDP

用户数据报协议（User Datagram Protocol，UDP）［Postel，1980］扩展到应用程序，其可靠性与 IP 使用的服务级别相同。数据包递交基于尽力递交，没有差错修正、重传、丢失、拷贝或重新排序的数据包探测。在 UDP 中甚至差错探测也是选项。

弥补这些缺点的是 UDP 的管理开销很少，特别是无需建立连接。这就使 UDP 最适用于

那些询问/响应的应用中，在那些应用中需要交换的信息量相对较少，无需 TCP 建立/取消连接所引起的开销。

当 UDP 用于传输大量数据时，其网络上的传输行为非常糟糕。其协议本身缺乏流量控制特性，因此它可能使主机和路由器陷入困境，并可能引起大量数据包丢失。

UDP 使用与 TCP 相同的端口号和服务器规范，但地址空间是分开的。与此类似，服务器通常（并不都是）占用低位数端口号。UDP 没有电路的概念。所有以给定端口号为传送目标的数据包均送往同一进程，而不管其源地址或端口号。

欺骗 UDP 数据包比欺骗 TCP 数据包容易得多，因为 UDP 没有握手或序列号。因此在使用来自 UDP 数据包的源地址时必须特别谨慎小心。应用程序必须自己设法进行鉴别。

1.1.5 ICMP

因特网控制报文协议（Internet Control Message Protocol，ICMP）［Postel,1981a］是一个用来左右 TCP 和 UDP 连接行为的低层机制。它可通知主机一条到达目的地的较好路径，报告路由中出现的问题，或者在网络出现故障时终止连接。它给系统和网络管理员提供了一个最重要的低层监视工具：ping 程序［Stevens,1990］。

在一给定主机上收到的许多 ICMP 报文，是针对一个特定连接的，或是由那台机器送出一个数据包引发的。在这种情况下，IP 报头和传输报头的前 64 位都包含于 ICMP 报文中。其意图是限制 ICMP 命令产生的变化范围。因此，一条 Redirect（重定向）报文或 Destination Unreachable（目标不可达）报文应该是针对确定连接的。不幸的是，旧的 ICMP 方法中并不使用这一额外信息。当这一报文到达后，某些主机对之间的所有连接将受到影响。假如收到一个 Destination Unreachable 报文，说有些数据包不能到达主机 FOO.COM，那么所有通向 FOO.COM 的连接都将被取消。即使源报文是特定端口的防火墙过滤器所触发的，情况也是如此。因此，应考虑使防火墙有节制地产生 ICMP 报文，否则可能取消来自同一机器的合法调用。我们还应注意到，黑客团体的一些人喜欢滥用 ICMP 去取消连接。过去已侦破过开发这种伤害他人的程序案例。

更糟糕的事件是使用 Redirect 报文。正如下面几节所解释的，任何人，只要他能够利用你的路由知识，篡改到达目的地的合适路由，就能够穿透你的机器。只有主机，而不是路由器，能服从 Redirect 报文，并且仅当这一报文来源于一个直接连接到网络上的路由器时，才被采纳。然而，并不是所有路由器（或者，在某些情况下，还有它们的管理员）对此都很谨慎。

有人可能会滥用 ICMP，以产生一个到达目的地的新路径。如果发生这种事情，你的确就已处于严重的麻烦中了。

1.2 路由器和路由协议

Routing 是指这样一个过程，即在网络中发现、挑选和使用路径，从而由一个地方抵达另一个（或别的多个）地方。

Open Systems Networking：TCP/IP and OSI

—David M.Piscitello 和 A.Lyman Chapin

路由协议是动态发现合适的因特网路径的机制。它们是运行 TCP/IP 的基础。路由信息

建立两条路径：从调用的机器到目的地机器以及返回的路径（后者常常是前者的逆过程。当不是这样的时候，就叫做不对称路由（asymmetric route），这并非好事）。从安全方面看，返回路径常常更为重要。当一个目标机器被袭击时，反向流动的数据包通过什么路径到达发起袭击的主机呢？如果敌人对这一路由机制稍加破坏，那么目标机器就会被欺骗，愚蠢地相信敌人的机器确实是可信任机器。如果发生这种情况，依赖于源地址校验机制的鉴别机制便会失效。

有多种方法攻击标准路由设备。最容易的办法是利用 IP 的松散源路由（loose source route）选项。利用它，启动 TCP 连接的人能够指定一条到达目的地的显式路径，从而忽略路由选择进程。根据 RFC1122［Braden，1989b］，目的地机器必定以与此相反的路径作为返回路由，不管它是否合理，随之而来的便是攻击者可以模仿目标机器信任的任何机器。

防范源路由问题最容易的办法就是拒绝含有该选项的数据包，许多路由器提供了这一工具。虽然存在源路由选项，但很少出于合法的理由使用它。例如，可以利用它确定网络故障。禁止这个选项不会对自己造成伤害。此外，某些 rlogind 和 rshd 版本根本拒绝与源路由选项打交道。这个选项是个劣项，因为可能还存在有其他具有相同弱点，但却没有相同保护措施的协议。

攻击路由的另一种做法是用路由协议本身做游戏。例如，将一个假的路由信息协议（Routing Information Protocol，RIP）[Hedrik，1988]数据包注入网络中，这很容易做到。一般来说，主机和路由器都会相信它们。如果从事攻击的机器比真实的源机器更靠近目标机器，那么就很容易将通信流改向。很多 RIP 的实施方法甚至接收主机专用路由，因此更难于探测。

某些路由协议，如 RIP2.0 版［Malkin，1993］和开放的最短路径优先（Open Shortest Path First，OSPF）［Moy，1991］都提供鉴别字段。有以下三个原因限制了它们的应用。第一，目前所定义的鉴别机制仅为一个简单的口令。凡是有能力做路由协议游戏的任何人，都有能力通过本地以太网电缆来收集他所喜欢的所有口令。第二，如果在路由对话中，一个合法的对话者受到破坏，那么他的报文（被源地址标记为正确的、合法的报文）就不再是可信任的了。最后，在大多数路由协议中，每台机器只对它的邻居讲话，并重复它们所讲的内容，这通常都是不加鉴别的。这样一来，欺骗性的东西也就传播出去了。

并不是所有的路由协议都会遭到这样的厄运。两台主机之间进行的对话难以被破坏，虽然类似于前面提到的序列号攻击仍可能成功。不过，更强的防御还是在拓扑上。路由器能够也应该进行配置，以便它们能够知道哪些路由器才能合法地出现在一条给定的电路上。一般说来，这是一件困难的事情，不过可以合理定位防火墙路由器，以相对简单的方式实现这一方案。下一章将进一步讨论这一概念。

1.3　域名系统

域名系统（Domain Name System，DNS）[Mockapetris,1987a,1987b;Lottor,1987;Stahl,1987]是一个分布式数据库系统，用于将主机名映射到 IP 地址，反之亦然。（在 DNS 普遍实施后，某些销售商将其叫做 DNS 捆绑（bind）。）在其常规操作模式中，主机向 DNS 服务器发送 UDP 询问。服务器响应，要么给出正确的答案，要么提供一个更聪明的服务器的信息。询问也可经由 TCP 进行，但是 TCP 操作常常是保留给区域传输（zone transfer）的。区域传输被备份服务器用来获得名字空间中它们自己那一部分的一个全拷贝。它们也可以被黑客用来快速获得目标机器列表。

许多不同种类的记录由 DNS 存储。缩写的列表见表 1-2。

DNS 名字空间是一个树形结构。为了操作简易，子树能被授权给其他服务器。逻辑上使用两种不同的树。第一种树将如同 NINET.RESEARCH.ATT.COM 这样的主机名映射到如同 192.20.225.3 这样的地址。其他每个主机的信息可以用选项形式包括其中，如 HINFO 或 MX 记录等。第二种树是反向询问（inverse query），同时包含 PTR 记录。在这种情况中，它会将 3.225.20.192.IN-ADDR.ARPA 这类信息映射成 NINET.RESEARCH.ATT.COM。两种树之间并无强制联系，不过某些站点为了某些服务曾尝试将这两种树连接起来。

表 1-2 一些 DNS 记录的类型

类 型	功 能
A	一个特定主机的地址（Address）
NS	名字服务器（Name Server）。把一个子树委派给另一个服务器
SOA	开始授权（Start Of Authority）。指示子树的开始；包含高速缓存和配置参数，并给出该区域负责人的地址
MX	邮件交换（Mail Exchange）。给主机命名，该主机为指定的目标处理收到的邮件。目标中可包括*.ATT.COM 一类的通配符，以使单个 MX 记录对整个子树的邮件进行重定向
HINFO	主机类型和操作系统信息。忽略它或提供不准确的信息
CNAME	主机实名的别名
PTR	用于将 IP 地址映射到主机名

这样的分离可能导致麻烦。一个控制了部分反向映射树的黑客可以使其说谎。即，反向记录可以错误地包含你的机器所信任的一台机器的名字。然后，攻击者尝试利用 rlogin 进入你的机器，而你的机器，因为相信该假记录，将会接受该调用。

大多数较新的系统对这类攻击具有免疫力。经由 DNS 恢复了假定存在的主机名后，它们就使用这个名字去获得它的 IP 地址集。如果用于这一连接的实际地址不在这个列表内，那么这次调用就被弹回来并记录一次安全违规。

交叉检查可通过两种方法实施，一是通过库存子程序，它由地址生成主机名（在很多系统上叫做 gethostbyaddr）；二是通过后台守护程序，它们基于主机名延伸信任。重要的是要知道你的操作系统是怎样进行检查的，如果不知道，你就不能安全地替换确定的部分。无论如何，部件探测到一个异常事件就应记录下来。

这类攻击具有更多样化的危害。在这种形式中，攻击者在开始调用前，先污染目标机器的 DNS 响应高速缓存。当目标机器不进行交叉检查时，它看起来似乎成功，并且入侵者获得了访问权。这类攻击的变种包括用假响应淹没目标 DNS 服务器，使它拒绝服务。

虽然实施 DNS 的最新软件可以解决这一问题，但要确保没有更多的安全漏洞也是不现实的。我们强烈建议，暴露的机器不要依靠基于名字的鉴别。基于地址的鉴别，虽然也脆弱，但还是相对好得多。

在 DNS 解析器的许多实现中，有一个很有效的特性，该特性也存在危险[Gavron,1993]。如果所考虑的名字和用户名使用公共部分时，它们允许用户略去后缀部分。

例如，假定在 FOO.DEPT.BIG.EDU 中有一个人想连接到某个 BAR.COM 目的地址。解

析器在用（正确的）BAR.COM 进行尝试之前，会用 BAR.COM.DEPT.BIG.EDU，BAR.COM.BIG.EDU 和 BAR.COM.EDU 去尝试。因而便藏有风险。如果有人生成一个 COM.EDU 的域，他们就能拦截任何流向.COM 下的通信。进而，如果他们有任何通配符 DNS 记录，这种情况就会更糟。

除鉴别问题外，DNS 还存在其他问题。它包含一个站点的丰富信息：机器名和地址、组织结构等等。例如，考虑一个有趣的事，一个侦探会感觉到他是在了解一个名叫 FOO.7ESS.ATT.COM 的机器，然后他就能够转储整个 7ESS.ATT.COM 域的信息，以便研究到底有多少计算机被安排来开发这一新的电话交换技术（迄今为止，我们知道在 AT&T 根本就没有 7ESS 这个项目）。

很难把这个信息对好奇者保密。限制区域传输到授权的辅助服务器，是一个好的开端，但聪明的攻击者也会千方百计通过 DNS 反向询问，彻底地搜索你的网络地址，得出一个主机名列表。然后，他们可以正向查表并检索其他有用信息。

1.4　标准服务

1.4.1　SMTP

当一个未联网的公司成员被问及他们希望从因特网连接中得到什么好处时，电子邮件是首选答案。如果你正在谈论有关因特网上电子邮件传输的话题，那么你通常会谈到与简单邮件传输协议（Simple Mail Transport Protocol，SMTP）有关的问题。SMTP 使用一个简单而稍为神秘的协议传输 7 位 ASCII 文本字符。

注意，调用者用 MAILFROM 命令指定一个返回地址。在这一等级上，没有可靠方法供本地机器用来对返回地址进行校验。你并不确切地知道是谁利用 SMTP 把邮件发送给你的。如果需要信任或保密的话，必须使用更高等级的机制。一个机构至少需要一个邮件专家。这有助把网关中的邮件器（mailer）集中起来，即使网络内部全部与因特网相连接。然后网络内部的管理员只需要将他们的邮件送到网关邮件器。网关确保送出去的邮件报头与标准的一致性。当这个机构有一个报告邮件器故障的确认触点时，它就变成了一个很好的因特网公民了。

邮件网关也是一个给公司内每个人的邮件起一个团体邮件别名的最好地方（有条件的话，邮件别名列表必须妥为保存：它们对业界间谍极具诱惑力）。

从安全观点来看，基本的 SMTP 本身是完全无害的。然而，它可能成为拒绝服务（denial-of-service）攻击的根源，这种攻击的目的是阻止合法使用机器。假如我安排 50 台机器，每台给你邮寄 1000 个 1MB 的邮件报文。你的系统能处理如此大的负荷量吗？假脱机目录够大吗？

邮件别名可能给黑客提供某些有用的信息。例如：

VRFY<postmaster>

VRFY<root>

这样一些命令常把邮件别名转换成实际的登录名。这就提供了线索：谁是系统管理员，一旦攻击成功哪个账号可能最可用。这涉及到一个策略，即这些信息是否敏感。后面将要讨论的 finger 服务还可提供更多的信息。