"十五"国家重点电子出版物规划项目·计算机网络技术和网络教室系列

应对黑客实战

网络攻击防护编码设计

北京希望电子出版社 总策划
谭毓安 编 写

北京希望电子出版社
Beijing Hope Electronic Press
www.bhp.com.cn

"十五"国家重点电子出版物规划项目·计算机网络技术和网络教室系列

应对黑客实战

网络攻击防护编码设计

北京希望电子出版社 总策划
谭毓安 编 写

北京希望电子出版社
Beijing Hope Electronic Press
www.bhp.com.cn

内容简介

这是一本关于网络攻击与防护编码设计方法和技巧的书，包括防火墙、加密、信息摘要、身份鉴别、病毒等，并对书中收录的大量的程序作了详细的分析和注解，力图使读者能够彻底地了解这些技术，并提高程序设计水平。同时书中也涉及到安全领域最新的一些发展，例如红色代码病毒、微软 IIS 漏洞等。

该书面向中高级网络程序设计人员作为自学指导，也可作为高校计算机专业本科/专科的信息安全课程教材使用。

敬告：破坏计算机安全的行为违反我国有关法律规定，对计算机系统实施攻击要承担相应的法律责任，请合法使用本书的内容来加强计算机的安全，而不是破坏计算机安全。

本版 CD 为配套书。

盘书系列名：“十五”国家重点电子出版物规划项目·计算机网络技术和网络教室系列

盘　书　名：应对黑客实战 网络攻击防护编码设计

总　策　划：北京希望电子出版社

文本著作者：谭毓安

责任编辑：赵文博

CD 制作者：希望多媒体开发中心

CD 测试者：希望多媒体测试部

出版、发行者：北京希望电子出版社

地　　址：北京中关村大街 26 号，100080

网址: www.bhp.com.cn

E-mail: lwm@hope.com.cn

电话: 010-62562329,62541992,62637101,62637102,62633308,62633309（发行部）

010-62613322-215（门市）　010-62547735（编辑部）

经　　销：各地新华书店、软件连锁店

排　　版：希望图书输出中心　马君

CD 生产者：北京中新联光盘有限责任公司

文本印刷者：北京媛明印刷厂

开本 / 规格：787 毫米×1092 毫米　16 开本　20.75 印张　478 千字

版次 / 印次：2002 年 3 月第 1 版　2002 年 3 月第 1 次印刷

印　　数：1-5000

本　版　号：ISBN 7-900088-47-4

定　　价：35.00 元（本版 CD）

前　言

计算机的安全是一个越来越令人关注的重要问题，同时也是一个十分复杂的课题。随着计算机和 Internet 的应用领域不断扩大和深入，计算机病毒也在不断产生和传播，计算机网络不断地被非法入侵，造成的损失非常巨大，甚至危害到国家和地区的安全。

自从 Internet 网诞生之日起，网络上的入侵事件不断发生。特别是 1988 年 11 月 Robert T. Morris 的蠕虫程序，令数千台主机乃至整个网络瘫痪。由于 TCP/IP 本身在安全方面的设计缺陷，以及软件（操作系统和应用软件）上的漏洞，使其极易受到“黑客”的攻击。一些著名网站包括政府网站都成了牺牲品，机密资料被泄露，主页被替换。攻击者可以窃听网络上的信息，窃取用户的口令、数据库的信息；还可以篡改数据库内容，伪造用户身份，否认自己的签名；更有甚者，攻击者可以删除数据库内容，摧毁网络节点，放置后门程序等等。因此，必须采取有力措施来保护网络安全。“知己知彼，百战不殆”，必须对黑客的攻击技术和系统的漏洞进行深入的了解，才能够保护自己的计算机系统不受伤害。

计算机病毒是另一种威胁。根据美国国家安全协会 ICSA（International Computer Security Associate）的统计报道，98%的企业都曾有过病毒感染的问题，63%都曾因为病毒感染而失去文件资料。全世界目前已有 50000 种以上的电脑病毒，从文件型病毒、宏病毒、CIH 病毒以及 ILOVEYOU 病毒，甚至包含在 HTML 文件中的病毒，层出不穷。而利用 Internet，一种病毒能够在几天之内传遍全世界。

密码学是安全研究方面的一个最古老的领域之一，密码算法的发展与计算机技术的发展息息相关。著名的 DES 算法在发布时被认为是安全的，然而，计算机的运算速度的飞速提高，使用密钥穷举法可以攻破 56 位的 DES 密钥。传统密钥系统不能解决数字签名、密钥交换等问题，因此提出了公开密钥系统。

密码学大师 Shamir 在 1995 年国际密码学会议上对商业安全提出的十项建议，具有很好的参考价值。

（1）不要追求绝对的安全。不同程度的安全，相应地要求付出不同的代价。在成本和风险之间作出一个合理的折衷选择。

（2）要解决最根本的问题，而不要专注于表面上的问题。如果问题没有从根本上得到解决，迟早会从另外的角度再次出现。

（3）不要使用由下而上的策略解决问题。必须将计算机安全和组织管理结合起来，采用由上之下的方法。安全策略对计算机的使用都会带来一定的限制，采用自下而上的方法，使用者就会倾向于使自己少受限制而牺牲系统的安全。例如，要求使用者必须定期更换密钥。

（4）不要过度地使用密码技术，造成使用者的不方便。

（5）不要使用太复杂的方法。复杂方法在未经过彻底验证之前，其中隐含漏洞的机会就越大。简单的技术，不一定不安全；复杂的技术不一定就更安全。

（6）不要过于依赖昂贵的设备。信息安全并不是仅仅靠设备、技术就能完全解决的，人员的配合、制度的建立和实施甚至更重要。

（7）不要使用单一防线策略。要考虑到安全措施被攻破后的应对措施和事先的备份等。

（8）不要忽视系统中的“异常”。对可能的攻击迹象，应追查其原因。还应该及时获得系统的补丁，对系统进行升级。当一个漏洞被发现并被公布后，利用这个漏洞的攻击也就随之而来。

（9）不要过于依赖管理员的操作。人都是有可能犯错误的，对于例行的备份操作，如果完全靠人来进行，有可能被忘记，或者操作失误等等。

（10）不要假设内部人员都是可靠的。对组织内部的成员，也要有一定的制度和措施对其进行限制。内部的破坏比外部更容易，危害更大。

本书在内容上可以分为三大部分。

第一部分包括第 1 章和第 2 章，介绍网络攻击技术，计算机系统的漏洞，入侵检测系统和防火墙技术。

第二部分包括第 3 章、第 4 章和第 5 章，介绍密码学知识，传统密钥系统和公开密钥系统，几种最常见的加密算法，如 DES、RSA 等，然后是数字签名和报文摘要，也就是保证信息的完整性，最后是鉴别，包括计算机如何鉴别用户的身份，以及计算机和计算机之间的相互鉴别。

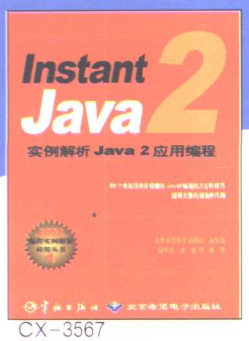
第三部分包括第 6 章和第 7 章，介绍计算机病毒的概念、运行方式以及防治手段，对几种典型的病毒如 2708、Friday、CIH、ILOVEYOU、红色代码等病毒进行了详细的分析。

书中采用大量的图表，并结合程序实例来分析计算机和网络安全的各种技术，目的是使读者从底层了解这些技术。只有这样，才能对这些技术有一个全面的把握，同时，也能够提高程序设计水平和了解相关知识。在涉及到相关的其他知识时，尽量地做一些介绍，例如 PE 文件格式、函数调用和堆栈之间的关系等等。

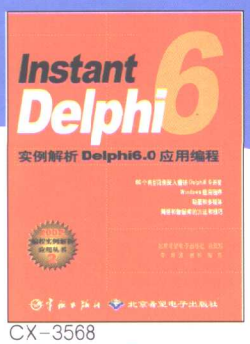
由于作者本人水平有限，书中定会有诸多不当之处，望各位读者原谅，尤其希望能提出宝贵意见。同时，书中引用了同行们的一些研究成果，在此一并表示感谢。

作者

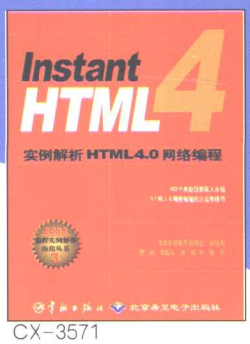
编程的利器，知识的迸发



CX-3567
定价:40.00 元

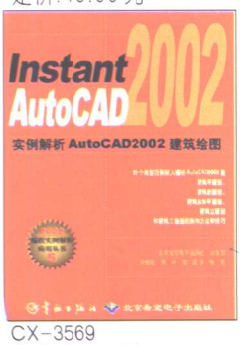


CX-3568
定价:40.00 元

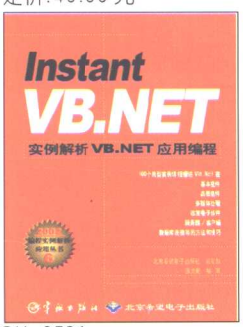


CX-3571
定价:40.00 元

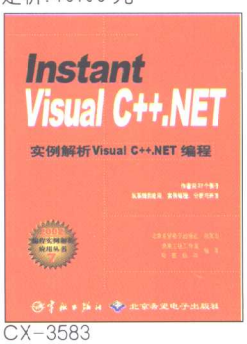
CX-3572
定价:40.00 元



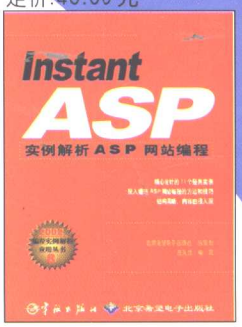
CX-3569
定价:40.00 元



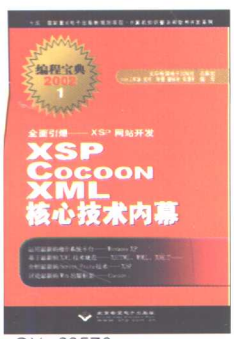
CX-3581
定价:40.00 元



CX-3583
定价:40.00 元

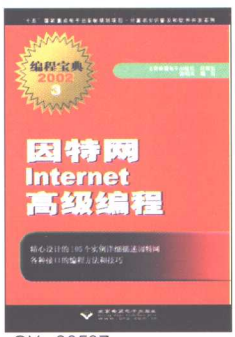


CX-3591
定价:40.00 元

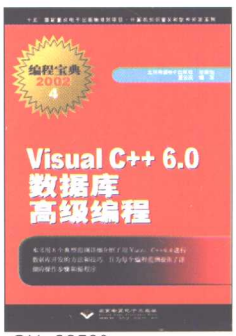


CX-83576
定价: 58.00 元

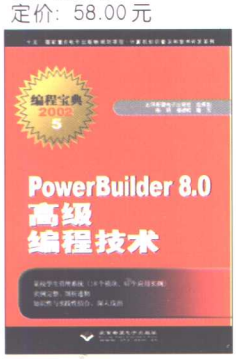
CX-83598
定价: 30.00 元



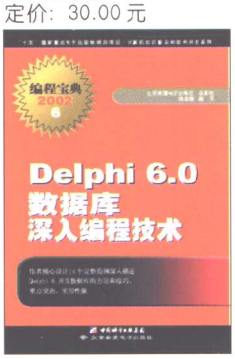
CX-83597
定价: 55.00 元



CX-83599
定价: 35.00 元

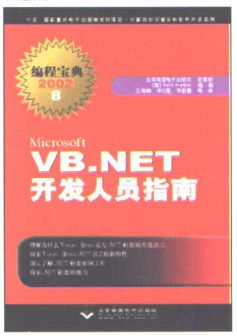


CX-83620
定价: 43.00 元



CX-83611
定价: 35.00 元

CX-83613
定价: 35.00 元



CX-83618
定价: 33.00 元

北京希望电子出版社
Beijing Hope Electronic Press
www.bhp.com.cn

地址：北京中关村 083 信箱北京希望电子出版社（邮编 100080）
电话：010-62562329、010-62633308　传真：010-62579874
E-mail: grh@hope.com.cn

目　录

第 1 章　网络攻击与防护

随着 Internet 的兴起，越来越多的计算机连接到全球网络上，使用者也越来越多，对整个社会产生了极大的影响。然而，网络的兴起也带来了一些前所未有的负面效应，攻击者在任何一个地主都可能向网络系统发动攻击，恶意截取和伪造信息，利用操作系统和其他软件的漏洞入侵计算机，也就是非法进入网络上的计算机系统，访问和控制系统中的各种资源。

由于媒体的大量报道，网络的入侵问题已经引起广泛的关注。通常将网络上的攻击者称为黑客，有关黑客的新闻往往给大众造成了对黑客技术的负面印象，认为黑客道德败坏、专门攻击和破坏网络系统。但我们应正视黑客技术，黑客技术是网络安全技术的一部分。这种技术若被用于破坏之目的，当然要遭到谴责。正面的做法是研究这些攻击技术，找出系统存在的弱点并加以改进，更深层次地有针对性地提高网络安全。

1.1　电子欺骗攻击

电子欺骗(Spoofing)是攻击者通过伪造一个网络数据包，该数据包的源地址被设为目标主机的可信任地址，从而得到目标主机的认证(许可)以访问目标主机上的资源。

TCP/IP 协议本身存在一些不安全隐患，可能受到的攻击包括序列号欺骗、路由攻击、源地址欺骗和授权欺骗等。假设欲攻击的目标主机是连在 Internet 上，不论目标主机运行何种操作系统，由于欺骗攻击是针对 TCP/IP 本身的缺陷，因此都可能被攻击。实际上，电子欺骗通常作为一种进攻手段，用于获得目标主机的信任关系，之后再利用这种信任关系对目标主机进行攻击。

在 Unix 领域中，用户为方便地使用多个主机，可以在主机之间建立信任关系。假如用户在主机 A 和 B 上各有一个独立账号，在使用过程中，在主机 A 上使用时需要输入在 A 上的相应账号，在主机 B 上使用时必须输入在 B 上的账号，两个账号在主机 A 和 B 上互不相关。为了避免这种不便，可以在主机 A 和主机 B 中建立起两个账号的相互信任关系。即在主机 A 和主机 B 上的用户 home 目录中创建.rhosts 文件，文件中包含对方主机的主机名和账号。建立信任关系后，在任何一个主机上都可使用以 r 开头的远程调用命令,如：rlogin，rcall，rsh 等，而不需要口令验证。信任关系是以基于 IP 地址(与主机名对应)的，.rhosts 文件中包含本主机允许或拒绝的 IP 地址(主机名)。

1.1.1　TCP 序列号预测

IP 层的作用是发送和接收数据包，并且保证它的完整性。由于 IP 不是面向连接的，所以 IP 层不保持任何连接状态的信息。每个 IP 数据包独立地发送出去，而不需要关心上一个和下一个数据包的情况。因此，可以在 IP 包的源地址和目标地址字段中放入任意的 IP 地址，也就是说，提供虚假的 IP 地址。

TCP 层在 IP 层的基础上提供面向连接的可靠传输。可靠性是由数据包中的多位控制字来提供的，其中最重要的是数据序号和数据确认，分别用 SYN 和 ACK 来表示。在源地址和目标地址之间数据传送过程中，TCP 为每一个数据字节分配一个序列号，确认已成功接收从源地址发送的数据包。ACK 在确认的同时，还携带了下一个期望获得的数据序列号。显然，相对于 IP 来说，TCP 提供的这种可靠性使得攻击者在 TCP 连接中插入数据包的难度加大，如图 1-1 所示。

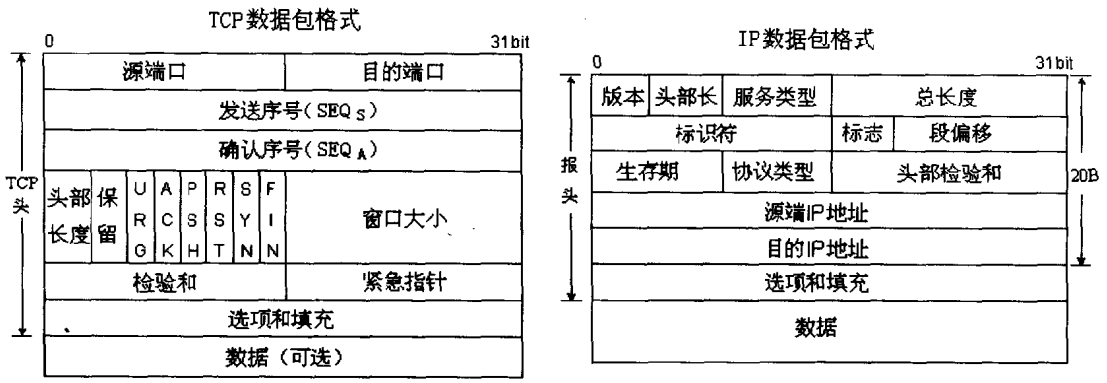


图 1-1　TCP 包和 IP 包格式

由于 TCP 要保证端到端的可靠传输，它具有处理数据包丢失、重复或乱序等异常情况的机制。发送方对它所传送出的所有数据字节分配序列编号，接收方收至数据后向发送方提供确认，TCP 就能保证可靠的传送。接收端利用序列号确定数据的先后顺序，并丢弃重复的数据包。TCP 序列编号在 TCP 数据包中占 32 位，范围为从 0 至 $2^{32}-1$。在 TCP 数据包的序列号(SYN)表示本数据包发送的数据在整个数据序列中的位置。确认号(ACK)表示接收方准备接收的数据序列号，同时表示该序列号之前的所有数据都已经收到。

TCP 通过滑动窗口的概念来进行流量控制。设想在发送端发送数据的速度很快而接收端接收速度却很慢的情况下，为了保证数据不丢失，显然需要通知发送端减慢发送速度。所谓滑动窗口，可以理解成接收端所能提供的缓冲区大小。TCP 利用一个滑动的窗口来告

诉发送端对它所发送的数据能提供多大的缓冲区。接收端最大能提供 65535 个字节的缓冲(窗口字段在 TCP 头中占 16 位)。由此，可以利用窗口大小(Window 字段)和确认序列号(ACK 字段)计算出最大可接收的数据序列号。

TCP 头中的其他字段包括 RST(连接复位，Reset the connection)、PSH(压入/推功能，Push function)和 FIN(发送者无数据，No more data from sender)。如果收到 RST，TCP 连接将立即断开。通常在接收端接收到一个与当前连接不相关的数据包时向发送端发送 RST。TCP 头部的 PSH 迫使 TCP 模块立即发送数据，即使数据没有充满一个发送数据包。

最早是由 Morris 发现并利用 TCP 序列号预测这一安全漏洞的。利用这个漏洞，即使是没有从服务器得到任何响应，也可以产生一个 TCP 包序列来和服务器进行通信。

在客户 C 和服务器 S 之间，建立 TCP 连接需要经过三次握手。客户选择和传输一个初始的序列号 ISN_C(ISN=Initial Sequence Number)，并设置标志位 SYN=1，告诉服务器它需要建立连接。服务器确认这个传输，并发送它本身的序列号 ISN_S，并设置标志位 ACK，同时告知下一个期待获得的数据序列号是 ISN_C+1。客户再确认它。在这三次确认后，开始传输数据，整个过程如图 1-2 所示。

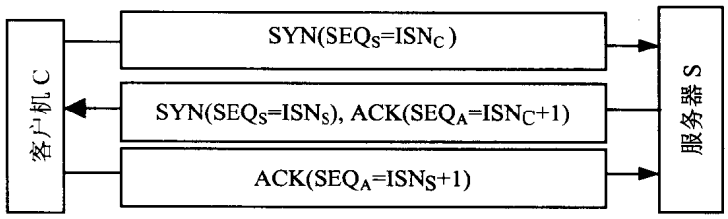


图 1-2　TCP 三次握手

简单表示为：

C→S: SYN(ISN_C)

S→C: SYN(ISN_S)，ACK(ISN_C+1)

C→S: ACK(ISN_S+1)

也就是说对一个 TCP 连接，客户必须得到 ISN_S 确认。ISN_S 可能是一个随机数。

了解服务器如何选择初始序列号和如何根据时间变化是很重要的。按照一般推测，当主机启动后序列号初始化为 1，但实际上并非如此。初始序列号是由 tcp_init 函数确定的。以 BSD 4.2 为例，ISN 每秒增加 128000，如果有连接出现，每次连接将把计数器的数值增加 64000。序列号用 32 位表示，在没有连接的情况下，序列号每 9.32 小时复位一次。因此，可最大限度地避免减少序列号的重复。如果初始序列号是随意选择的，那么不能保证现有序列号是不同于先前的。假设有这样一种情况，在一个路由回路中的数据包最终跳出了循环，回到了“旧有”的连接，显然会发生对现有连接的干扰。

T 被 S 所信任，入侵者 X 冒充 T 和 S 进行通信。如果入侵者 X 能预测出 ISN_S，就可以用下面的连接过程来欺骗 S，使服务器 S 相信 X 就是 T。

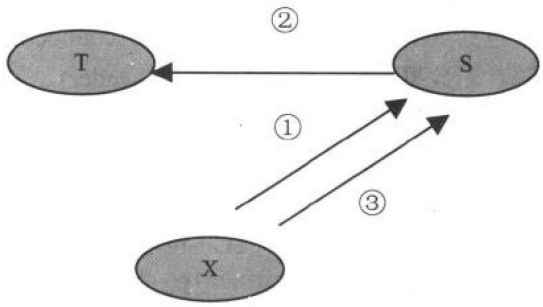


图 1-3　欺骗攻击示意

其过程为：

① X→S: SYN(ISN_X)，SRC = T

② S→T: SYN(ISN_S)，ACK(ISN_X+1)

③ X→S: ACK(ISN_S+1)，SRC = T

尽管在第②步数据包 S→T 并不经由 X，但是 X 能预测出 ISN_S，因此能在第 3 步发送数据包给 S 作为应答。在建立这个连接后，服务器 S 以为是在 T 通信，攻击者 X 就可以通过这个连接在目标主机 S 上执行一些命令。

如果主机 T 能正常工作，它能收到第②步数据包，认为是一个非法数据包，终止连接，而使得欺骗者 X 的目的落空。欺骗者 X 可以通过 DoS 攻击使主机 T 丧失处理能力。

1.1.2　IP 欺骗

IP 欺骗由若干步骤组成。做如下假定：首先，目标主机 S 已经选定。其次，信任模式已被发现，并找到了一个被目标主机信任的主机 T。为了进行 IP 欺骗，使被信任的主机 T 丧失工作能力，同时采样目标主机 S 发出的 TCP 序列号，猜测出它的数据序列号。然后，伪装成被信任的主机 T，同时建立起与目标主机 S 基于地址验证的应用连接。如果成功，可以通过这个连接在目标主机 S 上执行一些命令，比如置入一个后门程序，获取口令文件等等。

1．使被信任主机丧失工作能力

一旦发现被信任的主机，为了伪装成它，必须使其丧失工作能力。由于攻击者将要代

替真正的被信任主机，必须确保真正被信任的主机不能接收到任何有效的网络数据，否则将会被揭穿。有许多方法可以做到这些。其中的一种被称为“TCP SYN 淹没”。

建立 TCP 连接的第一步就是客户端向服务器发送 SYN 请求。第二步，服务器将向客户端发送 SYN/ACK 消息。这里客户端是由 IP 地址确定的。第三步，客户端随后向服务器发送 ACK，然后就可以进行数据传输了。然而，TCP 处理模块有一个处理并行 SYN 请求的最上限，它可以看作是服务器能同时处理的连接数目。其中，包括了那些正在进行三步握手(而没有最终完成)的连接，也包括了那些已成功完成握手但还没有被应用程序所调用的连接。如果达到队列的最上限，TCP 将拒绝所有连接请求，直至队列中的连接被释放，或者其中的某些连接达到超时时间。

攻击者 X 向被进攻目标 T 的 TCP 端口发送大量 SYN 请求，这些请求的源地址是合法的但是虚假的 IP 地址(Z，例如该合法 IP 地址的主机没有开机)。而受攻击的主机 T 会向该 IP 地址发送响应的，但得不到确认(第三步不能完成)。与此同时，第二步发出的 IP 包不能送达，因此网络会通知 T：目标不可到达，但主机 T 的 TCP 会认为是一种暂时网络故障，并继续重试，直至达到超时次数为止。当然，主机 T 的处理过程需要大量的时间。值得注意的是，攻击者是不会使用那些正在工作的 IP 地址的，因为这样一来，真正 IP 持有者会收到 SYN/ACK 响应，而随之发送 RST 给受攻击主机 T，从而使主机 T 断开连接。向主机 T 发送虚假 TCP 连接的过程可以表示为如下模式：

① $X \rightarrow T$: $SYN(ISN_X)$，$SRC = Z$

② $T \rightarrow Z$: $SYN(ISN_T)$，$ACK(ISN_S+1)$

③ $T \rightarrow Z$: RST

在时刻 1，攻击主机 X 把大批 SYN 请求发送到受攻击目标 T，使其 TCP 队列充满。在时刻 2 时，受攻击目标向虚假的 IP 地址 Z 作出 SYN/ACK 反应。在这一期间，受攻击主机的 TCP 模块会对所有新的连接请求予以忽视。在时刻 3，T 会因为超时而终止连接，将连接从连接队列中清除，可以接受新的连接请求。不同系统的 TCP 保持连接队列的长度可能不同。BSD 一般是 5，Linux 一般是 6。

使被信任主机 T 失去处理新连接的能力，所赢得的宝贵空隙时间(时刻 2 和时刻 3 之间的间隙)就是黑客进行攻击目标主机 S 的时间，这使其伪装成被信任主机 T 成为可能。

2．序列号取样和推测

要对目标主机 S 进行攻击，必须知道目标主机使用的数据包序列号(ISN_S)。可以与被攻击主机的一个端口(SMTP 是一个很好的选择)建立起正常的连接，然后再断开。这个过程被重复若干次，以采样到目标主机为最后一次连接设定的 ISN。还需要估计他的主机与被信任主机之间的 RTT 时间(往返时间)，这个 RTT 时间是通过多次统计平均求出的。RTT

对于推测下一个 ISN 是非常重要的。ISN 的大小是 128000 乘以 RTT 的一半，如果此时目标主机刚刚建立过一个连接，那么再加上 64000。在估计出 ISN 后，立即就开始进行攻击。

伪装成 T 向目标 S 发动攻击的过程为：

① X→S: SYN (ISN_X)，SRC = T

② S→T: SYN (ISN_S)，ACK(ISN_X+1)

③ X→S: ACK (ISN_S+1)，SRC = T

④ X→S: PSH，SRC = T

攻击者伪装成被信任主机 T 的 IP 地址，此时，该主机仍然处在停顿状态(因 TCP 连接队列满而失去处理能力)，攻击者向目标主机 S 的 513 端口(rlogin 的端口号)发送连接请求，如时刻 1 所示。在时刻 2，目标主机 S 对连接请求作出反应，发送 SYN/ACK 数据包给被信任主机 T(如果被信任主机处于正常工作状态，那么会认为是错误并立即向目标主机返回 RST 数据包，但此时它处于停顿状态)。在时刻 3，攻击者向目标主机 S 发送 ACK 数据包，该 ACK 使用前面估计的序列号加 1(因为是在确认)。如果攻击者估计正确的话，目标主机将会接收该 ACK。至此，连接正式建立起来了。在时刻 4，将开始数据传输。因为此时已建立了 rlogin 连接，攻击者发送的数据被主机 S 认为是从 T 上发送来的，而以 rlogin 的方式执行。

当然，如果能够使用 Sniffer 等工具获得目标主机在时刻 2 的应答，则可直接获得目标主机 T 的 ISN。不必使用 ISN 预测法就可以发送时刻 3 所需的 ACK 确认包。

1.1.3　防范 IP 欺骗

防范的要点在于，增加生成 ISN 算法的复杂性。这种攻击之所以能够成功是因为操作系统采用了相对简单的初始序列号计算方法，使得从一个已知的 ISN 序列号能够容易地推测到目标主机的下一个 ISN 序列号。

另一种方法就是不使用以 IP 地址为基础的验证。不允许 r*类远程调用命令的使用；删除.rhosts 文件；清空/etc/hosts.equiv 文件。这将迫使所有用户使用其他远程通信手段，如 telnet、ssh、skey 等等。

如果网络是通过路由器或防火墙接入 Internet 的，那么可以利用它们来进行包过滤。确信只有内部 LAN 可以使用信任关系，而拒绝内部 LAN 外上的主机对 513 端口(rlogin 的端口号)的访问。

在通信时要求加密传输和验证也可以防止 IP 欺骗，如使用 IPsec 协议。

1.2　嗅探器 Sniffer

Sniffer 攻击是通过捕获网络上传送的数据包来收集敏感数据，这些数据可能是用户的账号和密码，或者一些机密数据等等。嗅探器是一种网络管理工具，能够分析网络协议及定位网络故障，在形式上可固化成为硬件产品或直接作为软件程序运行，Sniffer 的拓扑结构如图 1-4 所示。

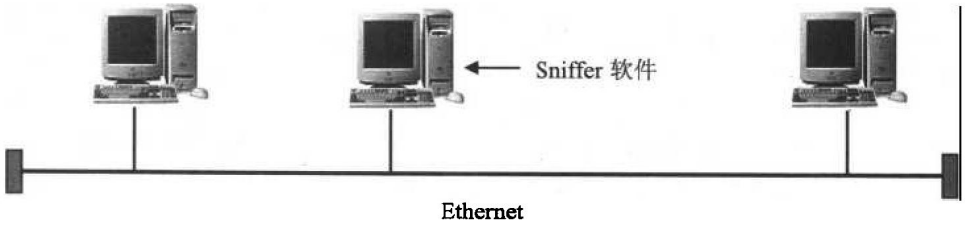


图 1-4　Sniffer 的拓扑结构

1.2.1　以太网偷听

在以太网上，任意两台主机的所有网络数据包都在总线上进行传送，而总线上的任何一台主机都能够侦听到这些数据包。攻击者可利用 Sniffer 对以太网上传送的数据包进行侦听，以发现敏感数据。可以自动地将符合条件的包存到一个 log 文件中供分析。例如，包含字符串"username"或"password"的包。

将网卡设置为杂凑(Promiscuous)模式后，该网卡能够接收网络上的所有数据包，不论这些数据包的目的地如何。在以太网中，任何两个主机之间传送的数据包都能被 Sniffer 监听到。

通常是攻击者已经进入了目标系统，然后在某个主机上运行 Sniffer，或者在路由器(以及有路由功能的主机)上运行，这样就获得网络中传送的大量数据。

在各种操作系统上都有 Sniffer 程序。如 Linux 的 tcpdump、NT 的 Network Monitor、Solaris 的 Snoop 等工具。

通常 Sniffer 程序只检查一个数据包的前 200~300 个字节的数据，就能发现诸如口令和用户名之类的敏感信息。

以 Solaris 下的 Snoop 为例，它随操作系统一起提供，在网络接口上监听并记录所有收到的数据包，并可以设置一些过滤条件。Snoop 的使用方法：