第5章 chapter 5

网络安全基础

互联网犹如为电子商务铺设了四通八达的道路，但是在这些道路上并不是很安全的，而是危机四伏，险象环生。当然，我们不能因为路上不太安全，就不从事电子商务活动了。而应该权衡利弊，评估风险，以适当的方法和代价，建立起适合电子商务的安全网络，争取在电子商务活动中获得较高的收益。

本章将从网络协议和网络体系结构上分析网络安全，指出常见的几种网络安全威胁方式。由于计算机病毒也可以威胁网络安全，本章还将讨论计算机病毒。

5.1 网络安全体系模型

Internet 是以 TCP/IP 协议为基础构建的，然而在 ISO/OSI 体系结构和 TCP/IP 协议创建之初，并没有适当地考虑安全的需要，因而存在着许多安全漏洞和根本性的缺陷，给攻击者留下了可乘之机。网络安全在体系结构上的脆弱性表现在以下几个方面。

(1) 很容易被窃听和欺骗。数据包在互联网上传输的时候，往往要经过很多个节点的重发。而在局域网内，通常采用的以太网或令牌网技术都是广播类型的网络，这使得窃听者可以轻而易举地得到发往其他主机的数据包。如果这些数据包没有强有力的加密措施，就等于把信息拱手送给了窃听者。比较陈旧的 DNS 服务软件易受虚假的 IP 地址信息的欺骗。另外一种 IP 地址的欺骗方式是在阻塞了受害的某台主机后再用受害者的 IP 地址在网络上冒充行骗。

(2) 脆弱的 TCP/IP 服务。基于 TCP/IP 协议的服务很多，最常用的有 WWW、FTP (File Transfer Protocol)、E-mail，此外还有 TFTP(Trivial FTP)、NFS(Network File System)、Finger 等，它们都存在着各种各样的安全问题。WWW 服务所使用的 CGI 程序、Java Applet 小程序和 SSI 都有可能成为黑客的得力工具。FTP 的匿名服务有可能浪费甚至耗尽系统的资源。TFTP 则无安全性可言，它常被用来窃取口令文件。E-mail 的安全漏洞曾经导致蠕虫在互联网上的蔓延。

(3) 配置的错误和疏忽。由于网络系统本身的复杂性，配置防火墙是一件相当复杂的事情。在没有更好的辅助工具出现之前，缺乏训练的网络管理员很有可能发生配置错误，给黑客留下可乘之机。在系统配置时过于宽容，或者由于对某些服务的安全性了解不够而没有限制或禁止这些不安全的服务，或者对于某些节点的访问要求给予太多的权

力，都会给安全带来危害。

5.1.1 网络体系结构及其安全缺陷

1. OSI 模型与 TCP/IP 模型的关系

OSI（Open System Interconnect）模型是 1977 年国际标准化组织（International Standard Organized，ISO）开发的开放系统互联参考模型，OSI 模型是用来作为开发网络通信协议的一个工业参考标准。根据 OSI 模型，计算机网络按功能分为 7 层，它们是物理层、数据链路层、网络层、传输层、会话层、表示层和应用层。OSI 模型只是个理论上的模型，它的缺陷在于所划分的层太多，其中会话层和表示层基本上没有使用价值。于是在 OSI 模型的基础上，又开发了一个重要的网络模型——TCP/IP 协议。

TCP/IP 协议是一个四层结构的网络通信协议组，包括：应用层、传输层、网络层及链路层。TCP/IP 协议与 ISO/OSI 模型的各层之间存在一定的对应关系，如图 5.1 所示。

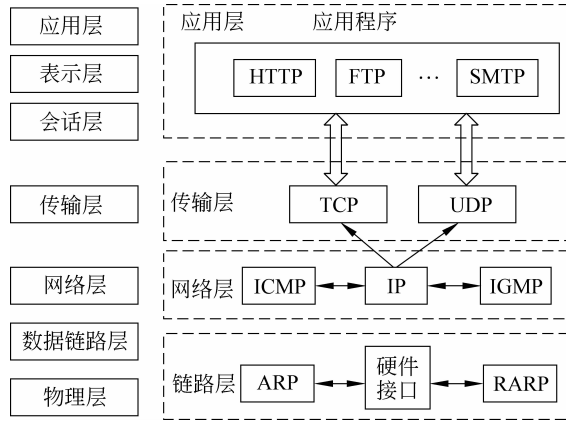

图 5.1 OSI 模型与 TCP/IP 协议组

目前，TCP/IP 协议已成为计算机网络事实上的工业标准，因为无论是局域网还是 Internet 上的计算机，在联网时都需要配置 IP 地址。

2. 网络层地址和传输层地址的关系

在基于 TCP/IP 协议的网络环境中，一台计算机（具有一个 IP 地址）可以提供多种服务，如文件传输服务 FTP、远程登录 Telnet、Email 等。为了使各种服务协调运行，TCP/IP 协议为每种服务设定了一个端口，称为 TCP 协议端口。每个端口都拥有一个 16b 的端口号（显然，对于一台主机，可以定义 65536 个端口）。用户自己提供的服务可以使用自由的端口号，不过，一般系统使用的端口号为 0～1024。用户自定义的端口从 1024 开始。

TCP/IP 的服务一般是通过 IP 地址加一个端口号（Port）来决定的。这是因为，IP 地址是网络层的地址，它只能唯一地标识网络上的一台主机，如 59.51.24.38 就是一个 IP

地址。也就是说 IP 地址对应一台主机，但目前的计算机是多进程设备，一台主机上可以同时运行多个应用程序，为了确定数据包是传给主机上哪个应用程序的，必须采用“IP 地址＋端口号”的形式（即每种应用程序对应一个 TCP 端口号）。因此，两台主机上的某个应用程序之间要进行通信的话就要使用“IP 地址＋端口号”作为标识，如图 5.2 所示。

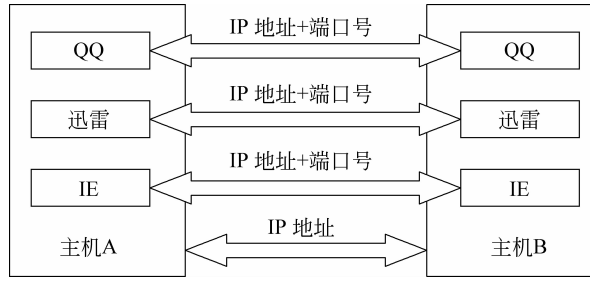

图 5.2 IP 地址和端口号的作用

对于一些常见的程序，它们使用的 TCP 端口号一般是固定的（有些程序需要占用几个端口，当然也可以更改这些程序默认的端口号）。常见应用程序的端口号如表 5.1 所示。因此，通过端口号还能辨别目标主机上正在运行哪些程序。使用“netstat -an”命令可以查看本机上活动的连接和开放的端口，是网络管理员查看网络是否被入侵的最简单方法。

表 5.1 常用的网络协议/应用程序端口号

协 议	端 口	协 议	端 口	应用程序	端 口
FTP	TCP/UDP 21	SMTP	TCP/UDP 25	QQ	UDP 4000 开始
HTTP	TCP 80	HTTPS	TCP 443	远程桌面	TCP 3389
Telnet	TCP/UDP 23	DNS	TCP/UDP 53	SSH	TCP 22

3. 网络层的安全缺陷

网络层的 IP 协议在设计时主要用于寻址和路由。对 IP 协议的攻击，是目前 Internet 上最主要的攻击。IP 协议存在的主要缺陷包括：①IP 通信不需要进行身份认证，无法保证数据源的真实性；②IP 数据包在传输时没有加密，无法保证数据传输过程中的保密性、完整性；③IP 的分组和重组机制不完善，无法保证数据源的正确性；④IP 地址的表示不需要真实及确认，无法通过 IP 验证对方的身份等。像常见的网络攻击如 IP 碎片攻击、源路由攻击、IP 欺骗、IP 伪造、Smurf 攻击、Ping Flooding 等都是利用 IP 协议的缺陷，而针对 IP 协议进行攻击的。

4. 传输层的安全缺陷

传输层包括 TCP 协议和 UDP 协议，对 TCP 协议的攻击，主要利用 TCP 建立连接时 3 次握手机制的缺陷，像 SYN Flooding 等拒绝服务攻击等都是针对该缺陷的。对 UDP 协议的攻击，主要是进行流量攻击，强化 UDP 通信的不可靠性，以达到拒绝服务的目的。

5. 应用层的安全缺陷

对应用层的攻击包括的面非常广，如对应用协议漏洞的攻击，对应用数据的攻击，对应用操作系统平台的攻击等。对应用层攻击包括：未经审查的 Web 方式的信息录入、应用权限的访问控制被攻破、身份认证和会话管理被攻破、跨站点的执行代码漏洞、缓存溢出漏洞等。

5.1.2 ISO/OSI 安全体系结构

计算机网络和 Internet 协议的制定者后来也逐步意识到了网络安全的脆弱性。1988 年，为了在开放系统互联参考模型(OSI/RM)环境下实现信息安全，ISO/TC97 技术委员会制定了 ISO 7498-2 国际标准“信息处理系统→开放系统互连→基本参考模型→第 2 部分：安全体系结构”，为网络安全的研究奠定了基础。这些标准给出了 OSI 参考模型的 7 层协议之上的信息安全体系结构，这是一个普遍适用的安全体系结构，对具体网络环境的信息安全体系结构具有重要的指导意义，其核心内容是保证异构计算机进程与进程之间远距离交换信息的安全。

这个标准确立了与安全体系结构有关的一般要素。在参考模型的框架内，还构建了一些指导原则与约束条件，从而提供了解决开放系统互联中安全问题的一致性方法。

1. OSI 定义的 5 种安全服务

OSI 安全体系结构定义了安全服务、安全机制、安全管理的功能，并给出了 OSI 网络层次、安全服务和安全机制之间的逻辑关系。OSI 规定了 5 种标准的安全服务。

(1) 对象认证安全服务。通信双方对各自通信对象的合法性、真实性进行确认，以防假冒。

(2) 访问控制服务。用于防止非授权用户非法使用系统资源。

(3) 数据保密服务。用于防止信息被截获或被非法存取而泄密。

(4) 数据完整性服务。用于阻止非法实体对交换数据的修改、插入、删除及防止数据丢失。

(5) 抗抵赖服务。用于证实已发生过的操作，防止对发生的行为进行抵赖。

2. OSI 定义的 8 种安全机制

为了提供上述安全服务。OSI 安全体系结构定义了 8 种安全机制。

(1) 加密机制。加密是提供数据保密的最常用方法，而且还能部分或全部用于实现其他安全机制。在哪一层进行加密取决于以下几个因素。

① 如果要求全通信业务流的机密性，那么将选取物理层加密或传输安全手段。

② 如果要求细粒度的保护(例如对每个应用提供不同的密钥)和抗抵赖或选择字段的保护，那么将选择表示层加密。

③ 如果要求端到端通信的机密性保护，或者希望有一个外部的加密设备，那么将选取网络层加密。这样能够提供机密性和不带恢复的完整性。

④ 如果要求带恢复的完整性，同时又具有细粒度保护，那么将选取传输层加密。这能提供机密性、带恢复的完整性或不带恢复的完整性。

（2）数字签名机制。数字签名用来解决通信双方发生争执时可能产生的否认、伪造、冒充和篡改等安全问题。

（3）访问控制机制。访问控制机制被用来实施对资源访问或操作加以限制的策略。

（4）数据完整性机制。数据完整性机制防止数据被假冒、丢失、重放、插入或修改。它包括两种形式：一种是数据单元的完整性，另一种是数据单元序列的完整性。

（5）认证交换机制。认证交换是以交换信息的方式来确认实体身份的机制。

（6）业务流填充机制。这种机制是对抗非法者在线路上监听数据并对其进行流量和流向分析。采用的对抗方法一般由保密装置在无信息传输时，连续发出随机序列，使得攻击者无法分辨哪些是有用信息，哪些是无用信息。

（7）路由控制机制。在一个大型网络中，从源节点到目的节点可能有多条线路，有些线路可能是安全的，而另一些线路是不安全的。路由控制机制可使信息发送者选择特殊的路由，以保证数据安全。

（8）公证机制。在一个大型网络中，由于用户或系统的原因，可能会引起很多责任问题，这时就需要一个各方都信任的实体——公证机构，来提供公证服务，仲裁出现的问题。

OSI 安全体系结构中安全机制与安全服务的关系如表 5.2 所示。

表 5.2 OSI 安全机制与安全服务的关系

安全服务 / 安全机制	对等实体鉴别	访问控制	数据保密	数据完整性	抗抵赖
加密机制	√		√	√	
数字签名机制	√	√		√	√
访问控制机制		√			
数据完整性机制				√	√
认证交换机制	√				
业务流填充机制			√		
路由控制机制			√		
公证机制					√

注：表中√表示该机制可以提供此安全服务，或与其他机制结合提供安全服务。

为了实现电子商务的这些安全要求，就必须使用各种技术手段，电子商务的安全技术与安全需求的对应关系如表 5.3 所示。

3. TCP/IP 协议的安全服务及实现机制

TCP/IP 协议是一个 4 层结构的网络通信协议组，包括：应用层、传输层、网络层及链路层。由于 TCP/IP 协议与 ISO/OSI 模型的各层之间存在一定的对应关系，因而可以根据 OSI 的安全体系结构框架，将各种安全机制和安全服务映射到 TCP/IP 的协议集中，从而形成一个基于 TCP/IP 协议层的网络安全体系结构，如表 5.4 所示。

表 5.3 安全技术与电子商务系统的安全需求的关系

安全要求 \ 安全技术	加密	口令	数字签名	数字证书	访问控制	防火墙	防病毒	认证	安全监控
完整性	√		√				√		√
保密性	√				√			√	
真实性	√	√	√	√				√	
不可抵赖性			√					√	
抵抗攻击					√	√	√		√
系统可用性					√				√

表 5.4 TCP/IP 协议的安全服务与安全机制

安全服务	安全机制
对等实体鉴别服务	由基于加密技术的 TCP 3 次握手交换鉴别机制支持
数据源鉴别服务	由加密机制和数据完整性机制支持
面向连接的数据机密性服务	由 TCP 保密连接机制和加密机制支持
面向连接可恢复的数据完整性服务	由加密机制、数据完整性机制、TCP 报文确认重发机制和保密连接交换鉴别机制支持
访问控制	由 TCP 保密连接机制和访问控制机制支持
数据源和目的的不可否认服务	由加密机制和数字签名机制支持

5.1.3 网络安全的分层配置

为了实现 Internet 的安全性，从原理上说安全服务可以在 TCP/IP 协议的任何一层实现。但通常都是在应用层、传输层或网络层上配置安全服务，如图 5.3 所示。在不同层级实现安全服务有着不同的特点。

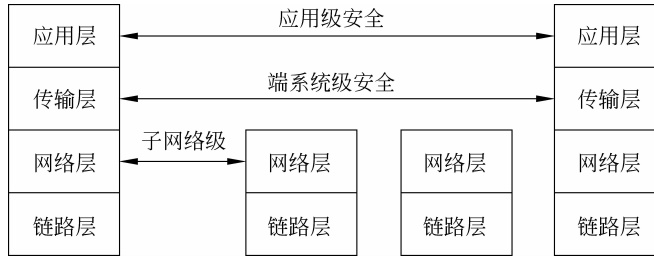

图 5.3 3 个基本的安全结构层

(1) 应用级安全。必须在终端主机上实施，以用户为背景执行，便于实施强大的基于用户的身份认证和访问控制。应用层的数据加密后，数据在链路、路由器和网关中都是密文状态，只有到用户的主机上才能恢复成明文，减少数据受到威胁的机会。使用应用层的安全服务实际上是最灵活的处理单个文件安全性的手段，缺点是必须针对每个应用设计一套安全机制。应用层安全协议有 SET、S/MIME、PGP、PEM、SSH 等。

(2) 端系统级安全。在传输层实现的安全机制,不会强制要求每个应用都在安全方面做出相应改进,缺点是为了提供由具体用户决定的服务,通常假定只有一名用户使用系统,与应用级安全类似,只能在终端系统实现,应用程序仍需要修改,才能要求传输层提供安全服务。传输层的安全协议有 SSL/TLS。

(3) 子网络级安全。网络层安全的优点是密钥协商的开销被大大削减了,因为只需要在网络节点之间协商密钥,其上的多种传输协议和应用程序可共享网络层提供的密钥管理架构,对应用程序的改动要少得多,能很容易地构建 VPN。缺点是因为缺乏用户参与背景,很难解决"抗抵赖"之类的需求。网络层的安全协议有 IPSec。子网络级安全和端系统级安全的区别是:前者只对所经过的一个或多个特定子网络提供保护。

5.1.4 网络安全的加密方式

在计算机网络中,加密可分为通信加密(即信息传输过程中的数据加密)和文件加密(即存储数据的加密)。通信加密又可分为链路-链路加密、节点加密、端-端加密等方式,如图 5.4 所示。

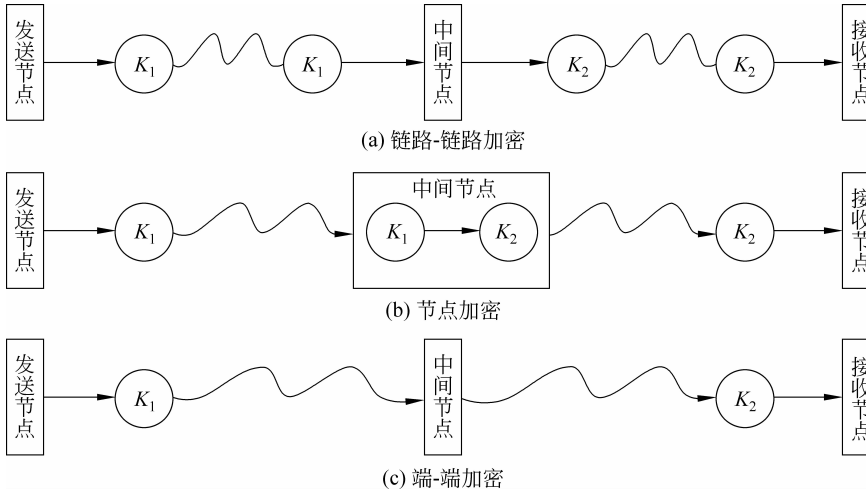

图 5.4 网络安全的 3 种加密方式

1. 链路-链路加密

链路-链路加密又称为在线加密,它对相邻节点间链路上传输的数据进行加密,如图 5.4 (a)所示。对于链路加密,所有数据在传输之前已经进行加密,各个节点对接收到的数据进行解密,然后使用下一个链路的密钥对数据进行加密,再进行传输。在到达目的地之前,一条消息可能要经过许多通信链路的传输,但是只对通信链路中的数据进行加密,而不对网络节点内的数据加密。它是一种链式连接的加密方式,每一链路被独立地加密。由于链路加密可以在物理层和数据链路层实施,因此它不仅对数据进行加密,还对报头进行了加密。

链路-链路加密的优缺点如下。

(1) 加密对用户是透明的,通过链路发送的任何信息在发送前都先被加密。

(2) 每个链路两端节点需要一个共用密钥。

(3) 攻击者无法获得链路上的任何报文结构的信息,因此可称之为提供了信号流安全。

(4) 缺点是数据在中间节点以明文形式出现,维护节点安全性的代价较高。

2. 节点加密

为了解决采用链接加密方式时,在中间节点上的数据报文是以明文形式出现的缺点。节点加密在每个中间节点里装上一个用于加、解密的安全模块,如图 5.4(b)所示。由它对信息先进行解密,然后进行加密,从而完成一个密钥向另一个密钥的转换。这样,节点中的数据不会出现明文。但由于每个节点要加装安全单元或保护装置,因此需要公共网络提供配合。

节点加密仅对报文加密,而不对报头加密,以方便路由的选择。

3. 端-端加密

端-端加密方式是建立在 OSI 模型的网络层、传输层或应用层,这种方式要求传送的数据从源端到目的端一直保持密文状态,数据在发送端被加密,在接收端解密,中间节点数据不会以明文的形式出现(图 5.4 (c))。用户或主机都可独自采用这种加密技术而不会影响其他的用户或主机。如果加密在应用层或表示层进行,那么加密可以不依赖于所有通信网的类型。

端-端加密方法将网络看成是一种介质,数据能安全地从源端到达目的端。这种加密在 OSI 模型的高三层进行,在源端进行数据加密,在目的端进行数据解密,而在中间节点及其线路上一直以密文形式出现。除报头外的报文均以密文的形式贯穿于全部传输过程,只是在发送端和接收端才有加、解密设备,而在中间任何节点报文均不解密,因此,不需要有密码设备。因此端-端加密和链路加密相比,可减少密码设备的数量。

然而,由于端-端加密只加密报文,报头以明文形式传送,因此它无法对抗业务流分析攻击。另外,端-端加密需要的密钥量大于链路加密需要的密钥数量,因此对端-端加密而言,如何对密钥进行管理是一个问题。

5.2 网络安全的常见威胁

通常,网络受到的安全威胁有以下几种,黑客正是利用其中一种或几种对网络进行攻击的。

5.2.1 漏洞扫描

攻击者在采取攻击行动之前需要了解攻击目标的相关信息,因此信息收集是攻击网络系统的第一步。信息收集主要包括获取 IP 地址信息和端口及漏洞扫描(扫描目标主

机上开放的端口和漏洞)。漏洞扫描主要使用漏洞扫描程序或 Windows 下的网络扫描命令。

漏洞源自“Vulnerability”(脆弱性),一般认为,漏洞是指软件或策略设置上存在的安全缺陷,从而使攻击者有机会在未授权的情况下访问和控制系统。漏洞对系统的威胁体现在恶意攻击行为对系统的威胁。操作系统和应用软件的漏洞最容易被黑客利用,从而进行木马、病毒等恶意代码攻击。近年来利用漏洞进行网络攻击的事件日益增多,给网络安全造成了严重威胁。

漏洞扫描程序(如 X-Scan)是一个可自动检测并初步分析远程或本地主机安全性弱点的程序。如一个 TCP 端口扫描器可以向某些 TCP/IP 端口和服务发出请求,然后记录这些目标的响应消息,从而收集目标主机的有用信息。通过使用扫描器,攻击者可以不留痕迹地发现目标主机的操作系统信息、端口的分配及提供的服务和它们的软件版本。例如检测主机是否支持匿名登录、是否开启了 Telnet 服务等。因此攻击者通过扫描器软件可以发现目标主机类型以及相应漏洞,并可能利用这些已知漏洞入侵目标主机。当然,系统管理员也可以使用扫描程序发现系统漏洞,并在攻击者攻击之前修补漏洞,从而提高了网络系统的安全性。

常见的漏洞扫描工具有 X-Scan。它是国内最著名的综合扫描器,其软件界面如图 5.5 所示。它采用多线程方式对指定 IP 地址段(或单机)进行安全漏洞检测,支持插件功能,提供了图形界面和命令行两种操作方式。扫描的项目很多,并且可以在如图 5.6 所示的界面中选择,使用方法很简单,首先设置检测范围,可设置一个有效的 IP 地址,然后可以在扫描模块中设置需要扫描的项目。

图 5.5 漏洞扫描软件 X-Scan 的主界面

设置完毕后,单击“开始”按钮,X-Scan 就开始扫描,可以查看具体的扫描过程。扫描完成后,X-Scan 会自动生成 html 格式的相关漏洞检测报告。

5.2.2 Windows 网络检测和管理命令

黑客在进行网络攻击的初期,通常没有权限在目标主机的桌面进行操作,他们一般

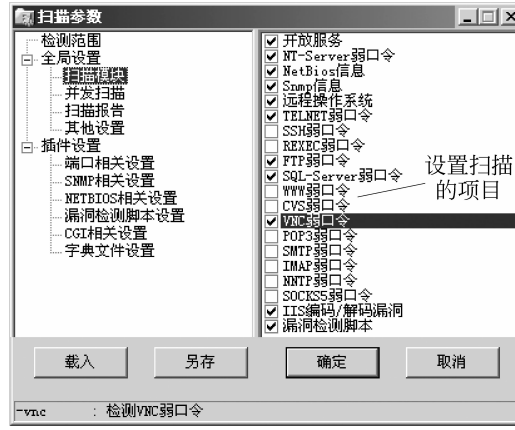

图 5.6 设置 X-Scan 的扫描参数和扫描项目

是使用 Windows 网络命令，因此掌握一些基本的 Windows 命令是进行网络攻防和网络安全检测的前提。

1. ping 命令

ping 命令可以检测网络目标主机存在与否以及网络是否正常(能否通达)。ping 的原理是向目标主机传送一个小数据包，目标主机接收到后将该包返送回来，如果返回的数据包与发送的数据包一致，就说明 ping 成功了。通过返回的数据、响应时间和数据丢失率，就能判断与对方的连接成功与否，连接效果、速度如何。

ping 命令可接域名、IP 地址或主机名，如 ping www.163.com，ping 59.51.78.210/t。ping 命令还可以带参数，其中“/t”表示不停地 ping 对方主机，直到用户按 Ctrl+C 键；“/a”会将对方 IP 地址转换成主机名。

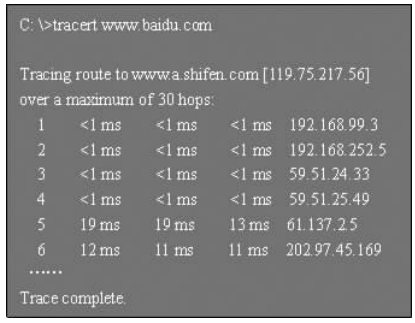

图 5.7 tracert 命令的执行结果

2. tracert 命令

tracert 是一个探测路由的命令，用来跟踪一个报文从一台主机到另一台主机所经过的所有网络节点路径。图 5.7 是“tracert www.baidu.com”的执行结果。

通过该命令可以知道数据包从发出后经过了哪些网关、路由器等设备再到达目的地址的。攻击者可以据此知道路由器和防火墙等设备的 IP 地址。

3. netstat 命令

netstat 命令用于显示网络连接、路由表和网络端口信息，可以让用户知道目前有哪些网络连接正在运行。如：netstat -an，查看目前活动连接和开放的端口，如图 5.8 所示。