信息科学与技术丛书 程序设计系列

刘文涛 编著

网络安全编程技术与实例

- 网络安全扫描编程
- 网络协议分析编程
- 网络数据包生成编程
- 入侵检测编程

机械工业出版社
CHINA MACHINE PRESS

信息科学与技术丛书·程序设计系列

网络安全编程技术与实例

刘文涛　编著

机械工业出版社

本书详细讲述了重要的网络安全技术原理，并进行了编程实现，涉及的技术有网络安全扫描、网络协议分析、网络数据包生成、网络入侵检测。全书使用 Visual C++编程，程序实例丰富，讲解透彻，源代码注释清晰，容易理解。读者可在 www.cmpbook.com 下载源代码。

本书供网络安全研究和开发人员以及网络安全爱好者阅读，也可以作为计算机网络和网络安全专业方面的教学参考书。

图书在版编目（CIP）数据

网络安全编程技术与实例/刘文涛编著．—北京：机械工业出版社，2008.7
（信息科学与技术丛书·程序设计系列）
ISBN 978-7-111-24616-9

Ⅰ．网… Ⅱ．刘… Ⅲ．计算机网络－安全技术－程序设计 Ⅳ．TP393.0

中国版本图书馆 CIP 数据核字（2008）第 101231 号

机械工业出版社（北京市百万庄大街 22 号 邮政编码 100037）
策划编辑：丁 诚
责任编辑：车 忱
责任印制：洪汉军

北京振兴源印务有限公司印刷厂印刷
2008 年 8 月·第 1 版第 1 次印刷
184mm×260mm·25 印张·616 千字
0001—5000 册
标准书号：ISBN 978-7-111-24616-9
定价：42.00 元

凡购本书，如有缺页、倒页、脱页，由本社发行部调换
销售服务热线电话：（010）68326294
购书热线电话：（010）88379639 88379641 88379643
编辑热线电话：（010）88379753 88379739
封面无防伪标均为盗版

出版说明

随着信息科学与技术的迅速发展，人类每时每刻都会面对层出不穷的新技术、新概念。毫无疑问，在节奏越来越快的工作和生活中，人们需要通过阅读和学习大量信息丰富、具备实践指导意义的图书，来获取新知识和新技能，从而不断提高自身素质，紧跟信息化时代发展的步伐。

众所周知，在计算机硬件方面，高性价比的解决方案和新型技术的应用一直备受青睐；在软件技术方面，随着计算机软件的规模和复杂性与日俱增，软件技术受到不断挑战，人们一直在为寻求更先进的软件技术而奋斗不止。目前，计算机在社会生活中日益普及，随着因特网延伸到人类世界的层层面面，掌握计算机网络技术和理论已成为大众的文化需求。由于信息科学与技术在电工、电子、通信、工业控制、智能建筑、工业产品设计与制造等专业领域中已经得到充分、广泛的应用，所以这些专业领域中的研究人员和工程技术人员越来越迫切需要汲取自身领域信息化所带来的新理念和新方法。

针对人们对了解和掌握新知识、新技能的热切期待，以及由此促成的人们对语言简洁、内容充实、融合实践经验的图书迫切需要的现状，机械工业出版社适时推出了“信息科学与技术丛书”。这套丛书涉及计算机软件、硬件、网络、工程应用等内容，注重理论与实践相结合，内容实用，层次分明，语言流畅，是信息科学与技术领域专业人员不可或缺的图书。

现今，信息科学与技术的发展可谓一日千里，机械工业出版社欢迎从事信息技术方面工作的科研人员、工程技术人员积极参与我们的工作，为推进我国的信息化建设作出贡献。

机械工业出版社

前 言

随着计算机网络的飞速发展，安全问题日益突出。为了保护网络安全，一些网络安全技术应运而生，对网络安全技术的研究也变得至关重要。网络安全是一门实践性很强的学科。理论联系实际，实践出真知，本书就是在这个背景下产生的，以实例为指导，以编程为中心，旨在让读者对网络安全相关技术有更深的理解。

本书主要对网络安全方面的一些技术进行了案例分析，通过编程实现了一些常用的网络安全技术，包括网络安全扫描、网络协议分析、网络数据包生成和网络入侵检测。

本书不是讲解网络安全理论的书籍，关于网络安全理论的书籍市面上很多，读者可以参考很多经典作品。本书主要讲解关于网络安全的编程技术，对常用网络安全技术进行了编程实现。由于网络安全涉及的内容很多，本书主要对网络安全扫描、网络协议分析、网络数据包生成和网络入侵检测进行了编程实现。其他的网络安全内容，限于篇幅没有涉及。

第 1 章介绍了一些网络安全方面的基本知识。

第 2 章主要介绍了一些基本的网络安全编程，包括 Winsock 套接字编程，还涉及进程、计时器以及注册表编程等。在 Winsock 套接字编程中主要介绍了套接字编程的基本原理，以及基于流式套接字和基于数据报套接字的编程方法。重点介绍了原始套接字的基本原理，对其发送数据包和接收数据包的过程进行了分析。在本章还介绍了获取网络接口的编程方法，此功能在网络安全编程中经常要用到。

第 3 章对网络安全扫描进行了编程实现，首先简单阐述了一些网络安全扫描的知识，其中包括各种端口扫描、隐秘扫描、漏洞扫描、远程操作系统识别、服务器扫描、木马扫描等技术。然后通过实例程序对每种网络安全扫描技术进行了编程实现，其中涉及 Winsock 原始套接字编程技术以及多线程技术等。在端口扫描中实现了 TCP 扫描，包括 TCP 连接扫描、TCP SYN 扫描以及 TCP FIN 扫描等。还实现了 ICMP 扫描、UDP 扫描、多线程扫描技术等。对服务器扫描实现了 Web 服务器扫描、FTP 服务器扫描以及 Email 服务器扫描。

第 4 章讲述网络协议分析系统的实现过程，使用编程工具 Visual C++ 6.0 介绍了多种协议分析实现方法，包括使用 Winsock 原始套接字方法以及 WinPcap 方法。本章详细阐述了网络协议分析系统的实现原理，包括数据包捕获技术、协议分析技术。介绍了利用 Winsock 原始套接字捕获网络数据包的过程，列举了利用 Winsock 原始套接字方法对 IP 协议分析、TCP 协议分析、UDP 协议分析以及 ICMP 协议分析的编程案例。最后利用 WinPcap 方法实现了一个基于 MFC 的协议分析系统，实现了对以太网、ARP、IP、TCP、UDP、ICMP 协议的分析功能，是一个内容比较综合的网络协议分析系统实例。

第 5 章介绍网络数据包生成编程技术，阐述了几种生成网络数据包的方法，包括 Winsock 原始套接字方法，WinPcap 生成数据包的方法以及使用 Libnet 生成数据包的方法。介绍了使用这些方法生成数据包的基本过程以及它们的区别，并且列举了利用这些方法分别实现常用协议数据包的生成实例，具体包括以太网数据包生产、ARP 数据包生成、IP 数据包生成、UDP 数据包生成、TCP 数据包生成和 ICMP 数据包生成。

第 6 章介绍了网络入侵检测系统的编程技术，在本章设计和实现了一个简单的基于 Windows 的入侵检测系统，本系统是在第 4 章的协议分析系统基础上实现的，添加了入侵检测功能部分。在本章对基本的模式匹配入侵检测技术和基于协议分析的入侵检测技术进行了简单实现。

本书设计和实现的所有案例短小精悍，以阐述和实现网络安全原理为目的。侧重于网络安全的编程实践，而不是纯理论的介绍。在书中，对每个程序都有比较详尽的解释，每个程序实例力求完整、简洁、清晰，以说明问题为主，不增加过多的次要功能。

书中所有实例都是用 Visual C++ 6.0 编写而成的。

如果读者想要理解这些网络安全技术，又想通过编程实现这些技术，本书是一个很好的参考样本。本书可供网络安全研究和开发人员以及网络安全爱好者参考也可以作为计算机网络和网络安全专业的教学参考书，还可以作为课程设计参考书。随书的代码可在 http://www.cmpbook.com 下载。

在本书编写过程中李元香帮助查阅资料，在此表示感谢。还要感谢我的同事和朋友，以及不断支持我的家人。

由于作者水平有限，书中难免有不妥和疏漏之处，欢迎指正。

本书联系 Email：liuwentao268@163.com

刘文涛

武汉工业学院

目　录

第1章 网络安全概述

1.1 网络安全原理

1.1.1 信息安全

根据国际标准化委员会的定义，计算机信息安全是指“为数据处理系统采取的技术和管理的安全保护，保护计算机硬件、软件、数据不因偶然的或恶意的原因而遭到破坏、更改、显露”。信息安全要保证信息的保密性、完整性、可用性和可控性。保密性是指保证信息不被非授权用户使用。完整性是指保障信息的准确性和完全性，保证信息在存储或传输过程中不被篡改。可用性是指确保信息为授权用户所正常使用，信息能够按照某种权限按需存取。可控性是指使用的信息能够被监控，对信息的传输及内容具有控制能力。由于信息具有抽象性和可变性等特征，使得它在处理、存储和传输的过程中很容易被干扰、滥用和泄露，甚至被窃取、篡改和破坏，所以在实际使用中，信息经常处在不安全的状态。信息系统不安全的因素主要有物理因素、网络因素、系统因素、应用因素和管理因素等。

1.1.2 网络安全

网络安全是指利用相应的安全技术使网络系统的硬件设备和软件系统以及网络中的相关数据得到保护，避免其因为某种原因而受到破坏、更改和泄露，保证系统连续、可靠、正常地运行，网络服务不中断。它是信息安全的重要内容。其主要目的就是保护网络上的重要信息不受破坏，要保证网络信息的可用性，保证网络对象的可靠性，包括硬件、软件、环境等可靠性。信息的操作和存储需要计算机，而信息的传输需要网络系统，所以保障信息的安全离不开保护计算机的安全和网络安全。

破坏和影响网络安全的因素和技术有很多，下面对其进行归纳总结。

1. 拒绝服务

拒绝服务是指由于某些行为导致合法用户不能正常访问网络，不能够得到应有服务的状态。一些非法用户使用某种攻击技术浪费网络带宽，侵占网络资源，而正常的用户却不能够得到应有的服务，这样就导致了拒绝服务。这些攻击技术一般称为拒绝服务攻击，它们的种类繁多，只要是能导致拒绝服务的攻击技术都可以称为拒绝服务攻击。此类攻击就是利用合理的服务请求来占用过多的服务资源，致使系统超载，无法响应其他的请求。这些服务资源包括网络带宽、文件系统空间容量、开放的进程或者向内的连接，这种攻击会导致资源的匮乏。现在，已经出现了分布式拒绝服务攻击方式，攻击者利用大量的中间主机来攻击目标主机，这些中间主机俗称“僵尸主机”，而由僵尸主机组成的网络俗称“僵尸网络”，它们是由攻击者控制的主机，执行攻击者的口令，完成直接的攻击行为。其原理是攻击者通过指令控

制中间机器发送大量的网络数据包给目标主机，导致目标主机的资源被大量占用，而正常的用户却无法获取。有时候会导致网络阻塞，或者网络设备瘫痪，或者服务器资源耗尽而停机。常用的拒绝服务攻击技术有 ICMP Flood、SYN Flood、ACK Flood 等等。从拒绝服务攻击的表现来看，可以分为针对流量攻击和针对资源攻击两大类：流量攻击通过生成大量的网络数据包，造成庞大的网络流量，使网络产生拥挤，浪费网络带宽；资源攻击则针对一些主机，导致其 CPU 资源被侵占，或者内存被耗尽，或者提供的服务被占用，从而导致应用程序无法启动，正常用户无法获得服务。

2．病毒

计算机病毒其实是一种程序，是指在计算机程序中插入的破坏计算机功能或者毁坏数据、影响计算机使用并能自我复制的一组计算机指令或者程序代码。病毒运行后能够损坏文件、使系统瘫痪，从而造成各种难以预料的后果。它具有传染性、隐蔽性、破坏性等特征。计算机病毒可以通过网络传播，还可以通过其他存储设备传播，例如光盘。病毒如果按照传染方式进行分类有引导型、文件型和混合型病毒，如果按照实现方法来分有木马病毒、蠕虫病毒、宏病毒、电子邮件病毒、U 盘病毒等。

3．木马

木马是一种特殊的程序，它专门收集一些敏感信息，监视和控制用户的机器，可以把它当作一种计算机病毒。网络木马具有远程控制功能，攻击者可以利用木马完全控制受害者主机，执行攻击者指令，完成一些破坏行为。利用木马可以窃取用户的秘密数据和个人资料，删除文件，放置后门，因此木马的危害是巨大的。木马一般具有客户端和服务器端两个部分，有时候它们相互转换，具有双重功能。客户端是攻击者控制端，用来完成与远程服务器的连接并发送相应的指令。而服务器端是放置在目标主机上的，用来执行特殊任务，完成攻击者指定的操作。现在破坏比较严重的是盗取密码的木马，它们可以盗取各种应用程序的用户名和密码，例如网络银行、即时通信、电子邮件、网络游戏等。现在的木马种类繁多，许多新技术也应用到木马上，包括病毒技术，产生了一些智能病毒木马，具有更强的病毒特征。它们通常具有自启动功能，隐藏在一些正常的进程之中，用户很难察觉，具有很强的隐蔽性。有时候木马会把自己加载为服务项，作为机器的一项服务被启动。有些木马具有绕过防火墙的功能，隐藏自己的服务器端口，把自己捆绑到正常的服务之上，使一些安全软件不易发觉。先进的木马具有自我保护功能，通常进行备份处理，被删除后，其备份的程序能重新启动。

4．系统漏洞

系统漏洞是指系统中存在的一些 bug，攻击者可以利用 bug 进行破坏活动。系统漏洞是大部分安全问题的根源，是影响网络安全的最重要的因素。特别是一些重要的系统软件，如果出现漏洞则会产生严重危险。操作系统、服务器软件尤其如此。很多安全问题就是因为有了漏洞才产生的，一些计算机病毒都是根据漏洞而写出来的。系统存在 bug 是在所难免的，不可能完全消除，只有在设计开发的时候更加认真和规范，进行足够的测试，才能将 bug 的危害降至最低。如果系统发现了漏洞，要及时打好补丁，这是解决由于系统漏洞造成安全威胁的最好办法。用户要培养定期更新系统的习惯。有时候也可以借助漏洞扫描软件来辅助检测。

5．网络欺骗

网络欺骗是指利用一些欺骗技术达到攻击目的。它包括 IP 欺骗、TCP 劫持、ARP 欺骗、

DNS 欺骗等类型。IP 欺骗可以用在各种网络攻击技术中，例如在 TCP SYN Flood 攻击中可以构造虚假的 IP 地址，让被攻击的目标无法检测正确的攻击源，这样攻击者可以很好地伪装和保护自己，以免被发觉。TCP 会话劫持则利用欺骗技术让目标主机相信攻击者是一个合法的主机。ARP 欺骗技术是将 ARP 应答数据包发送给目标主机，让目标主机认为某个特定 IP 地址的 MAC 是应答数据包中包含的 MAC 地址，其实这个 MAC 地址是攻击者的 MAC 地址，结果所有发送这个特定 IP 地址的数据包都发送到攻击者主机，这个时候攻击者就可以监听所有发送给这个 IP 地址的网络数据包。同样也可以发送 ARP 欺骗数据包给这个特定的 IP 主机，让它相信目标主机的 MAC 地址是攻击者地址，这样攻击者就可以截获目标主机和这个特定 IP 主机之间的网络通信了。一个完整的 ARP 欺骗其实是双向欺骗的，让两者都相信攻击者 MAC 是对方的 MAC 地址，这样攻击者就可以监听两者的通信。DNS 欺骗会造成域名和 IP 地址的实际不对应，让用户在访问一个域名的时候，并没有转向真正的 IP 地址，而是转向一个攻击者设定的 IP 地址，攻击者可在此地址挂载木马或者病毒，让用户自动下载而被感染。

6．Zero-Day 攻击

Zero-Day 攻击也称为“0-day”攻击，是指攻击者利用刚刚发现的系统漏洞尚未被修补上的间隔而发起的攻击行为。当系统被发现存在漏洞，但是还没有补丁能够下载安装，那么在这个间隔期间，攻击者可以利用此漏洞进行攻击。有时候，这个系统的漏洞被某些人发现，但是没有公布于众，则攻击者可以贩卖此漏洞而从中牟利。还有大多数的用户，虽然系统漏洞的补丁已经发布，但是没有及时进行升级安装，或者由于某些原因不知道补丁已经发布，此时 Zero-Day 攻击也会延续下去。

7．网络钓鱼

网络钓鱼是指攻击者利用伪造的信息来骗取用户的敏感数据。攻击者可以伪造邮件，或伪装成各种 Web 站点甚至银行机构来发布消息，诱使用户以为是正规的信息而填写一些个人数据，攻击者趁机窃取用户的数据。例如，攻击者伪造一个银行的 Web 站点，跟正常的银行站点几乎一样，用户如果不仔细辨别很难分清，于是用户有可能使数据泄密。有时攻击者利用系统漏洞，在网站上挂载一些恶意代码，伪装成正常的服务，骗取用户密码。

1.1.3　网络安全模型

比较实用的网络安全模型为 P2DR 模型，P2 表示策略（Policy）和保护（Protection），D 表示检测（Detection），R 表示响应（Response）。制定周全的策略是首要的内容，然后是综合运用一切网络安全技术来保护和检测网络，例如防火墙、病毒检测、入侵检测、安全扫描等。当发现有危险状态发生时或者出现入侵行为则要及时进行响应，把危险降到最低。保护、检测、响应和恢复涵盖了对现代信息系统的安全防护的各个方面，构成了一个完整的体系，使网络安全建筑在一个更加坚实的基础之上。

有时候根据网络协议层次对网络安全也进行分层考虑，根据协议的分层也有每个层的安全内容。在网络层，有代表性的是 IpSec 安全协议，传输层有 SSL 和 TLS，应用层有 SSH、SHTTP、S/MIME 等。其中 IpSec 由协议 AH 和 ESP 组成，包括传输和隧道两种模式，一个密钥交换管理协议 IKE 以及两个数据库（安全策略数据库 SPD 和安全关联数据库 SAD）。IPSec 的主要特征是可以支持 IP 及所有流量的加密和认证，因此可以增强分布式应用的安全性。AH 协议为 IP 数据包提供完整性和鉴别功能，AH 提供的服务包括数据源认证，无连接

的完整性，可选的抗重放服务。ESP 提供保密功能，包括报文内容的机密性，可以提供鉴别服务。IP 层安全性的主要优点是它具有透明性，安全服务的提供不需要特定的应用程序以及其他通信层次的任何修改。其主要缺点是网络层一般对属于不同进程和相应程序的数据包不作区别，对所有同一地址的数据包，它将按照同样的加密密钥和访问控制策略来处理，这样就导致了性能的下降。IP 层非常适合提供基于主机对主机的安全服务，相应的安全协议可以用来在网络上建立安全的 IP 通道和虚拟私有网 VPN。传输层安全（TLS，Transport Layer Security）是 SSL3.0 的后续版，在传输层上，在源和目的实体间建立一条安全通道，提供基于证书的认证和信息完整性以及数据保密性服务。SHTTP（Secure Hyper Text Transfer Protocol）是 Web 上使用的超文本传输协议的安全增强版本，提供了文件级的安全机制，用作加密及签名的算法可以由参与通信的收发双方协商，提供了多种单向散列函数的支持，如 MD5、SHA 等，也提供多种单钥体制的支持，如 DES、3DES、RC4 等，还提供了对数字签名体制的支持，如 RSA、DSS 等。S/MIME 是在多功能电子邮件扩展报文基础上添加数字签名和加密的一种协议，MIME 是正式的电子邮件扩充标准格式，但它未提供任何安全服务功能。

1.1.4 安全策略

针对纷繁的网络安全问题制定相应的安全策略是至关重要的。为了提高网络安全意识，加强网络安全管理，制定有效而合理的安全策略，对于保护整个网络安全是事半功倍的。安全策略简单地说，就是对于某个特定的网络环境，按照特定的安全要求，制定一整套安全措施和规则，以保证这个特定的网络处于安全状态。

针对不同的策略对象，应实施相应的安全策略。一般有：① 物理安全策略，用来保护网络设备特别是重要的网络服务器设备以及网络路由和通信设备，它们的操作和管理都必须设置相应的权限，有严格的控制规则。② 访问控制策略，它的应用非常广泛，可以具体到某一个简单的系统，也可以是一个非常复杂的网络系统，其主要目的就是保证被保护的对象不被非授权用户访问，一般有基于角色的访问控制策略以及基于身份的访问控制策略。③ 加密策略，数据加密是一种普遍采用的安全措施，在网络上传输的数据可以通过加密进行保护。对于数据的加密也要制定相应的策略规则。例如根据加密层次的不同有链路层加密、传输层加密以及端到端加密等，根据加密方法的不同有公钥加密和私钥加密等。

1.1.5 安全管理

一个大型的网络系统需要专门的部门进行管理，而安全管理是其重要内容之一。网络安全最重要的是在思想上高度重视，网站或局域网内部的安全需要用完备的安全制度来保障。建立和实施严密的计算机网络安全制度与策略是真正实现网络安全的基础。

具体地说，网络安全管理应包括对授权机制的管理、对访问控制策略的管理、对加密和密钥的管理、对安全日志的管理。要制定周密的管理措施，包括设立安全机制、发布安全信息以及解决安全事件等内容。网络安全管理的目的主要包括：确保网络数据的私有性，不被非授权用户随意获取；授权访问，即不可抵赖性，发送的数据要能够识别是谁发送的；信息的访问控制，对敏感的数据要分级，资源不能越权访问。

1.2　网络安全的组成

网络安全是一个非常全面而复杂的课题，它包括的内容极其庞大。在这里把网络分成三个组成部分，分别是客户端、服务器和网络设施，从这三个方面来考虑网络安全的问题。

1.2.1　客户端安全

在客户端部分主要涉及具体用户使用网络的安全问题，例如个人数据的安全性。用户把计算机联入网络之后，其就是一个客户端。要保证个人数据的安全，需要建立良好的使用网络的习惯。例如包括定时杀毒，安装个人防火墙，不打开可疑邮件，不随便安装来路不明的软件。对个人的敏感信息要进行加密处理，放在一个安全的地方，对重要的数据要进行备份，以免硬件损坏而丢失数据。要及时升级操作系统，安装各种补丁程序，或者下载新的软件应对安全问题。在客户端的一些常用软件最易受到安全威胁，例如网络浏览器，由于经常使用这类软件，其安全性能备受关注，而安全问题也是最多的。还有一些比较常用的软件，例如文字处理软件、媒体播放器软件、电子邮件接收和阅读软件等，也容易受到威胁。

1.2.2　服务器安全

服务器方面的安全性也至关重要，很多重要的数据都放在服务器里面。对于重要数据的保护则需要更加强大的安全措施，例如使用专业的防火墙设备、入侵检测系统、安全扫描系统、针对特定服务器的保护系统。

在使用服务器的服务软件时，软件的合理配置也很重要，对于不需要开放的服务尽量不要开放，对于开放的服务要有足够的安全措施，例如设置安全权限以及密钥。

最常用的客户端和服务器系统是 Web 浏览器和 Web 服务器系统，它们的安全性在网络安全内容中占据着重要的地位。针对 Web 浏览器和 Web 服务器的攻击数量庞大，种类繁多，危害性也很大。针对 Web 安全提出了很多技术，例如安全套接层（SSL，Secure Sockets Layer）、TLS、SHTTP 等。SSL 使用 TCP 提供一个可靠的端到端安全服务，为两个通信个体之间提供保密性和完整性。SSL 包括 SSL 握手协议和 SSL 记录协议两个部分；SSL 记录协议建立在可靠的传输协议基础上，提供连接的保密性和完整性，用来封装高层的协议；SSL 握手协议完成客户端和服务器端之间的安全鉴别，协商加密算法和密钥，提供身份鉴别和可靠协商的功能。

1.2.3　网络设施安全

网络设施的安全是要保护重要的网络设备，例如路由器和交换机等重要设备，防止由于故障例如停电以及其他自然灾害造成系统瘫痪。电源故障会造成设备断电，导致操作系统引导失败或数据库信息丢失等。

1.3　研究网络安全的必要性

1.3.1　技术层面

信息的保密性、完整性和可用性对用户和单位至关重要，但信息系统和网络会受到来自

四面八方的各种威胁。计算机网络面临的安全性威胁主要包括：数据截获，攻击者从网络上窃听他人的通信内容；通信中断，攻击者有意中断他人在网络上的通信；数据篡改，入侵者故意篡改网络上传送的报文；数据伪造，攻击者伪造信息在网络上传送。

现在出现了许多网络破坏技术，例如：计算机病毒，现在的病毒更加具有智能化和网络化等特征；恶意代码，包括木马、逻辑炸弹等。还有各种具有迷惑性的网络攻击行为，例如网络钓鱼。网络钓鱼是指入侵者利用欺骗性的电子邮件和伪造的 Web 站点来进行诈骗活动，受骗者会暴露自己的敏感数据，例如个人的真实信息、银行卡号、账户以及密码等。随着网络技术的发展，入侵者可以很快掌握入侵技术，使破坏网络安全的行为变得越来越容易。同时，很多人的安全意识比较薄弱，所以网络安全问题变得越来越突出。

1.3.2 社会层面

网络安全是一个关系到国家安全和社会稳定的重要问题。其重要性正随着全球信息化的步伐与日俱增。网络安全是一门涉及计算机科学、网络技术、加密技术、信息安全技术、应用数学、数论和信息论等多种学科的综合性科学。随着网络飞速发展，计算机网络得到了广泛应用，但随着网络之间的信息传输量的急剧增长，一些机构和部门在得益于网络加快业务运作的同时，其上网的数据也遭到了不同程度的攻击和破坏。入侵者可以利用网络技术窃取网络上传输的敏感信息，例如用户的口令，还可以篡改数据库内容，设计虚假的用户身份，窃取核心数据。有时，入侵者会删除数据库内容，破坏网络信息系统，放置一些木马后门和病毒程序。这些行为都导致数据的安全性和机构的利益受到了非常严重的破坏。随着信息的膨胀和网络的飞速发展，信息网络的安全防护技术已逐渐成为一个新兴的重要技术领域，并且受到政府、军队和全社会的高度重视。随着我国政府和金融等重要领域都建设了信息网络平台，国家的信息网络已成为重要的安全领域，逐渐成为国家安全的最高价值目标之一，可以说信息网络的安全与国家安全密切相关。

社会的基础设施现在都基于网络环境，特别是一些重要的单位部门，例如政府部门、电力系统、电子商务系统等。它们的安全性至关重要，如果出现问题，其损失是非常重大的。随着网络时代的到来，整个国家的许多重要方面都要依赖于网络，例如军事、经济、文化、商业等，它们都有相应的网络系统。这些网络存在的安全隐患越来越多。据统计，全世界由于信息系统的脆弱性而导致的经济损失每年可达数百亿美元。信息安全防护能力是综合国力的体现，是国际竞争力的主要成分。如果信息安全得不到保证，则社会的各个方面都会受到威胁，国家在当今的信息战中也会处于不利地位。

1.4 网络安全技术

1.4.1 网络安全扫描

所有软件系统几乎都有漏洞存在，其安全性问题由于漏洞的存在而大大提高。安全检测主要是试图发现系统的漏洞，对目标进行安全检测，找出可疑点，把检测结果报告给管理员，然后进行分析以便及时进行补救，是网络安全的一项重要技术。