“十二五”江苏省高等学校重点教材

21世纪高等学校网络空间安全专业规划教材

网络攻击与防御技术

王群 编著

电子课件

教学大纲

上机实训

工具软件

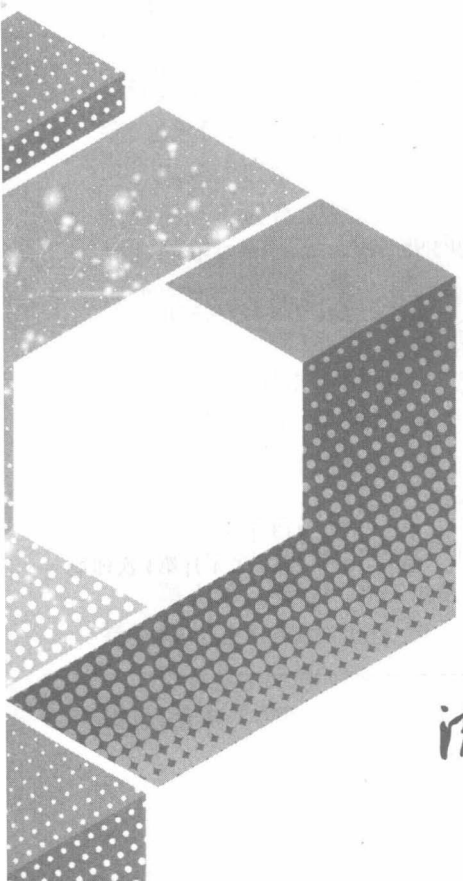
清華大學出版社

“十二五”江苏省高等学校重点教材

21世纪高等学校网络空间安全专业规划教材

网络攻击与防御技术

◎ 王群 编著



清華大學出版社

北京

内 容 简 介

本书从攻击与防御两个层面，通过网络攻防技术概述、Windows 操作系统的攻防、Linux 操作系统的攻防、恶意代码的攻防、Web 服务器的攻防、Web 浏览器的攻防、移动互联网应用的攻防共 7 章内容，系统介绍网络攻防的基本原理和技术方法，力求通过有限的篇幅和内容安排来提高读者的攻防技能。

本书可作为高等院校信息安全、网络空间安全相关专业本科生和研究生的教材，也可作为从事网络与系统管理相关方向技术人员及理工科学生学习网络攻防技术的参考用书。

图书在版编目(CIP)数据

网络攻击与防御技术/王群编著. —北京：清华大学出版社，2019
(21 世纪高等学校网络空间安全专业规划教材)
ISBN 978-7-302-51832-7

Ⅰ. ①网… Ⅱ. ①王… Ⅲ. ①计算机网络－安全技术－高等学校－教材 Ⅳ. ①TP393.08

中国版本图书馆 CIP 数据核字(2018)第 284313 号

策划编辑：魏江江
责任编辑：王冰飞
封面设计：刘　键
责任校对：梁　毅
责任印制：沈　露

出版发行：清华大学出版社
网　　址：http://www.tup.com.cn，http://www.wqbook.com
地　　址：北京清华大学学研大厦 A 座　　**邮　　编**：100084
社 总 机：010-62770175　　**邮　　购**：010-62786544
投稿与读者服务：010-62776969，c-service@tup.tsinghua.edu.cn
质量反馈：010-62772015，zhiliang@tup.tsinghua.edu.cn
课件下载：http://www.tup.com.cn,010-62795954
印 装 者：三河市龙大印装有限公司
经　　销：全国新华书店
开　　本：185mm×260mm　　**印　　张**：16.75　　**字　　数**：413 千字
版　　次：2019 年 4 月第 1 版　　**印　　次**：2019 年 4 月第1次印刷
印　　数：1～1500
定　　价：49.50 元

产品编号：081641-01

前　言

网络攻防表面上是一种攻守双方的技术对抗，其实质则是攻击者与防守者之间的力量较量，是人与人之间的智力博弈。近年来，随着人们对网络的依赖性越来越强，功能各异的操作系统和应用软件在丰富了网络应用的同时，其自身存在的漏洞也成为网络攻击者不断挖掘和利用的资源。网络攻防是一种矛与盾的关系，防守者总希望能够通过获取并分析攻击者的痕迹来溯源攻击行为，并制定或修改防御策略。

本书（包括配套的《网络攻击与防御实训》）是江苏省高等学校重点教材，从立项之初到最后成书，期间曾多易其稿，甚至将第一稿的全部内容推翻进行重写。在写作过程中克服了许多困难。

一是内容确定。武汉大学张焕国教授曾经用“信息安全是信息的影子”来比喻信息与信息安全之间的关系，非常确切。今天，当人们随时随地、无时无刻地享受着即时通信、撰写博客、点评美食、网络约车等信息技术带来的便捷时，银行账号信息窃取、电信诈骗、地理位置信息泄露等信息安全问题也如影相随。那么，作为一本课时量受限的教材来说，又该如何在有限的时间内为学生系统介绍信息安全领域有关攻击与防范的知识呢？本书立足作者多年来从事信息安全实践与教学科研的经验，最后确定将操作系统、恶意代码、Web 服务与应用和移动互联网应用等方面的攻防作为重点进行介绍。

二是内容组织。从攻防的角度来讲，本书的每一章都可以单独编成一本厚厚的书，很显然这不适合于教学。本套书将理论和实践分开，本书重点介绍攻击与防御中涉及的基础知识和基本理论，而配套的《网络攻击与防御实训》主要提供具体的攻防训练，通过实训加深对基础知识的理解，并培养实践动手能力。

三是知识融合。就攻击和防御来说，虽然针对每一个具体案例在知识结构上具有相对独立性，但不同案例所涉及的知识点和实践能力的培养具有交叉性，这就涉及不同章节及同一章节不同知识点之间的融合。融合不仅仅是内容上的有效组织，更是培养目标的确定，以及培养过程的遵循。只有在内容上注重相互间的关联，在教学过程中关注理论与实践之间的结合，才能最后实现在知识上融会贯通的人才培养目标。

本书共 7 章，具体内容简述如下。

第 1 章：网络攻防技术概述。本章较为系统地介绍网络攻防的基础知识，主要包括网络攻击的类型、方法、实施过程及发展趋势。

第 2 章：Windows 操作系统的攻防。本章在介绍 Windows 操作系统安全机制的基础上，重点从数据、进程与服务、日志、系统漏洞、注册表等方面分别介绍攻防的实现方法。

第 3 章：Linux 操作系统的攻防。本章在介绍 Linux 操作系统工作机制和安全机制的基础上，分别介绍用户和组、身份认证、访问控制、日志等的安全机制，并对 Linux 操作系统的远程攻防技术和用户提取方法进行介绍。

第 4 章：恶意代码的攻防。恶意代码包括的内容较多，而且相关内容的发展较快。本章重点对计算机病毒、蠕虫、木马、后门、僵尸网络和 Rootkit 等典型恶意代码从攻击与防范两个层面进行较为系统的介绍。

第 5 章：Web 服务器的攻防。本章在对比分析了 C/S 结构和 B/S 结构及安全机制的基础上，从 Web 服务器的组成出发，重点介绍 Web 服务器信息的收集方法、Web 数据的攻防、Web 应用程序的攻防及 Web 服务器软件的攻防等内容。

第 6 章：Web 浏览器的攻防。本章与第 5 章的内容相互照应，但重点不同。本章主要从 Web 浏览器安全应用出发，从浏览器插件和脚本、Cookie、网页木马、网络钓鱼、黑链攻击等方面，介绍针对 Web 浏览器的攻击与防范方法。

第 7 章：移动互联网应用的攻防。作为近年来发展迅速的移动互联网应用及存在的主要安全问题，本章立足于应用安全，通过大量的案例介绍，从技术和非技术两个层面介绍相关的安全问题，并提出相应的安全防范方法。

本书在编写过程中得到了许多同事和同行的无私帮助和支持，在项目申请和出版过程中得到了清华大学出版社编辑老师的关心和帮助，我的同事倪雪莉老师和刘家银老师对全书的文字进行了校对。同时，本书的编写参考了大量的文献资料，尤其是国内外著名安全企业的技术手册，有些未能在参考文献中标明。在此一并表示衷心的感谢！

由于作者水平有限，书中难免有不足之处，敬请读者提出宝贵意见。

作　者

2019 年于南京

目　录

第1章　网络攻防技术概述

近年来，世界各国对网络空间的争夺日益激烈，针对网络空间的控制信息权和话语权成为新的战略制高点；现实空间的渗透和恐怖袭击正与网络空间的渗透和恐怖袭击紧密地结合在一起，成为人类社会面临的新威胁；不断增长和扩散的计算机病毒（如木马、蠕虫）、黑客攻击等大量信息时代的“衍生物”，正在对信息化程度较高的金融、交通、商业、医疗、通信、电力等重要国家基础设施造成严重的破坏，成为影响国家安全的新威胁。保护网络空间安全作为重大挑战之一，已与防止核恐怖事件、利用核聚变能量等一起被列为21世纪亟待解决的难题。本章立足网络空间安全，介绍网络攻防的基本概念和相关技术。

1.1　黑客、红客及红黑对抗

计算机的出现使程序的自动运行变成了现实，而网络技术的应用使信息成为物质和能量以外维护人类社会的第三资源。随着计算机应用的普及、Internet的飞速发展和黑客、红客等概念出现，涉及黑客与红客之间博弈的红黑对抗越来越引起社会的关注。

1.1.1　黑客与红客

1. 黑客

黑客（hacker）原是正面形象，特指那些技术高超、爱好钻研计算机技术，能够洞察到各类计算机安全问题并加以解决的技术人员。在这一定义中，黑客不具有恶意破坏计算机系统和扰乱网络正常运行秩序的特征，而是安全的守护者和捍卫者。其中，将挖掘并公开漏洞的黑客称为白帽，而白帽网站（如乌云网）则是一个供白帽、安全厂商和安全研究者对安全漏洞等问题进行公开和反馈的网络平台，也是互联网安全研究者学习交流和研究的平台。

今天的黑客又称为“骇客”（cracker），描述为熟悉计算机操作系统的原理且能够及时发现和利用操作系统存在的安全漏洞，借此实施非法入侵、窃取、破坏等行为的计算机捣乱分子或计算机犯罪分子。

黑客和骇客之间的差异性主要表现在以下几个方面。

（1）黑客是系统安全的守卫者，所从事的工作是建设性的；而骇客则是系统安全的破坏者，所从事的是破坏行为。

（2）虽然黑客和骇客都是利用自己掌握的计算机技术，设法在未经授权的情况下访问计算机文件或网络，是计算机系统和网络的入侵者。但黑客在成功入侵后进行的操作不是恶意破坏性的，而是有建设性的，而骇客则不然。

（3）由于运行程序是计算机的唯一功能，所以黑客需要掌握计算机编程能力，而骇客一般不具有此能力，通常只掌握一些入侵和扫描工具的使用方法，并利用这些工具入侵他人系统进行不法行为。

20世纪90年代，Internet在中国快速发展，国内一批计算机技术爱好者开始研究安全漏洞，并通过网络分享自己的研究成果，成为第一批黑客群体。之后，随着越来越多的安全漏洞被发现，一些人意识到了其利用价值，买卖漏洞、恶意代码的现象开始在黑客中出现，黑客群体开始向两极分化。以赢利为目的的网络攻击行为促使了黑色产业链的产生和迅猛发展，而崇尚分享、自由、开放的最为纯正的黑客精神逐渐走向消亡。

现在的黑客特指假借名义控制他人计算机的特殊人群，可以称为通过使用已有工具软件对计算机系统进行攻击和控制的软件黑客(software cracker)或脚本小子(script kids)。软件黑客和脚本小子继承了骇客的破坏性特征，而缺乏原本黑客应有的高深技术。在现实网络空间中，真正对网络进行破坏的，往往不是那些挖掘并研究漏洞的黑客，而是软件黑客或脚本小子。如不做特殊说明，本书中所讲的黑客一般是指软件黑客。

2. 红客

红客(honker)是信息安全的守卫者，除在技术上具备传统黑客的能力外，还需要具有“正义感”，能够有效阻止计算机系统和网络的破坏行为，确保用户能够按既定的秩序在系统中提供或获得服务。红客的本意是维护系统的秩序，减少系统的不安全因素。

黑客在某种意义上代表着“邪恶”，因此黑客的行为都是在隐蔽环境下进行的。而红客代表的是“正义”，所以红客的行动一般都是公开的，可以充分运用技术和非技术(如法律、法规、管理制度等)手段来捍卫系统的安全。在中国，红色代表着正义、进步和强大，红客除蕴含着技术能力外，还映射着一种正能量和正面精神，即具有正义感、爱国情怀和进取精神的从事网络安全的黑客。

1.1.2 红黑对抗

网络空间是继陆、海、空、天领域之后的第五维空间，它是以自然存在的电磁能为载体，人工网络为平台，信息控制为目的的空间。网络空间包括电子系统、计算机、通信网络和其他信息基础设施，通过对信息的采集、存储、修改、交换、分析和利用，实现对物理实体的实时控制，影响人的认知活动和社会行为。网络空间已经成为当前国家最重要的基础设施之一，网络空间安全对抗也成为捍卫国家安全的重要使命。

网络攻防的实质是网络空间中人与人之间的智力博弈，其表现形式为红客与黑客之间的对抗，即“红黑对抗”。互联网本身是不健壮的，但在设计之初被认为是安全的。红黑对抗是一种正义与非正义之间的斗争。在网络空间中，攻击者与防卫者就是一种矛与盾的关系，矛希望能够刺穿盾，盾则希望能够阻挡矛。信息安全领域中的红黑对抗就是这样一个互相抗衡、此消彼长的动态过程。红客和黑客连续不断的网络攻防对抗，导致了网络秩序失去平衡。红黑对抗是伴随着信息技术的发展而不断演进的。

在教学环节中，网络攻防可通过配置虚拟网络实验环境，在虚拟的、高实时、强交互、网络拓扑结构处于高度不稳定状态的网络中，对基于过程的网络行为分析、网络跟踪、网络主动防御等技术进行研究。通过网络攻击和防御技术的模拟，再现攻击和防御的博弈过程。网络攻防不仅是一种攻击和防御的实施方法，而且可以为网络的可恢复性、灵活性和安全性评估提供技术指导。

作为应用数学分支之一的博弈论是一套研究智能的理性决策者之间冲突与合作的策略选择理论，而网络空间中的攻防本身就是一种冲突，攻击与防御在方法和技术上的较量归根

到底就是攻防双方在决策上的博弈。模型创建是网络攻防的基础，通过建立和分析网络攻防博弈模型，可以评测攻防双方的既定策略，并基于攻防双方的驱动与能力，获得纵深的策略集合甚至是攻防均衡点，使防御方能够基于最小的代价获得最大的安全收益，为网络攻防提供理论依据。

1.2　网络攻击的类型

网络攻击是指任何非授权而进入或试图进入他人计算机网络的行为，是入侵者实现入侵目的所采取的技术手段和方法。这种行为包括对整个网络的攻击，也包括对网络中的服务器、防火墙、路由器等单个节点的攻击，还包括对节点上运行的某一个应用系统或应用软件的攻击。根据攻击实现方法的不同，可以分为主动攻击和被动攻击两种类型。

1.2.1　主动攻击

主动攻击是指攻击者为了实现攻击目的，主动对需要访问的信息进行非授权的访问行为。例如，通过远程登录服务器的 TCP 25 号端口搜索正在运行的服务器的信息，在 TCP 连接建立时通过伪造无效 IP 地址耗尽目的主机的资源等。主动攻击的实现方法较多，针对信息安全的可用性、完整性和真实性，主动攻击一般可以分为中断、篡改和伪造 3 种类型。

1. 中断

中断主要针对的是信息安全中的可用性。可用性(availability)是指授权实体按需对信息的取得能力，强调的是信息系统的稳定性，只有系统运行稳定，才能确保授权实体对信息的随时访问和操作。可用性同时强调的是一种持续服务能力，这种能力的实现需要立足系统的整体架构来解决可能存在的安全问题，降低安全风险。中断是针对系统可用性的攻击，主要通过破坏计算机硬件、网络和文件管理系统来实现。拒绝服务是最常见的中断攻击方式，除此之外，针对身份识别、访问控制、审计跟踪等应用的攻击也属于中断。

2. 篡改

篡改针对的是信息安全中的完整性。完整性(integrity)是指防止信息在未经授权的情况下被篡改，强调保持信息的原始性和真实性，防止信息被蓄意地修改、插入、删除、伪造、乱序和重放，以致形成虚假信息。在计算机系统和网络环境中，信息所具有的数字化特征，致使信息被篡改的可能性和可操作性要比传统纸介质简单得多，为此篡改也成为了网络攻击过程中较常使用的一种危害性较大的攻击类型。

完整性要求保持信息的原始性，即信息的正确生成、存储和传输。在网络环境中，信息的完整性一般通过协议、纠错编码、数字签名、校验等方式来实现。针对这些实现方法，篡改攻击则会利用存在的漏洞破坏原有的机制，达到攻击目的。例如，通过安全协议可以有效地检测出信息存储和传输过程中出现的全部或部分被复制、删除、失效等行为，但攻击者也可以破坏或扰乱相关安全协议的执行，进而使安全协议丧失应有的功能。

3. 伪造

伪造针对的是信息安全中的真实性。真实性(validity)是指某个实体(人或系统)冒充

成其他实体，发出含有其他实体身份信息的数据信息，从而以欺骗方式获取一些合法用户的权利和特权。伪造主要用于对身份认证和资源授权的攻击，攻击者在获得合法用户的用户名和密码等账户信息后，假冒成合法用户非法访问授权资源或进行非法操作。例如，当攻击者冒充为系统管理员后，可拥有对系统的最高权限，进而对系统进行任意的参数修改、功能设置、账户管理等操作，对系统安全产生严重威胁。

在一个授权访问系统中，认证系统的功能是使信息接收者相信所接收到的信息确实是由该信息声称的发送者发出的，即信息发送者的身份是可信赖的。另外，认证系统或协议需要保证通信双方的通信连接不能被第三方介入，防止攻击者假冒其中的一方进行数据的非法接收或传输。

1.2.2 被动攻击

被动攻击是利用网络存在的漏洞和安全缺陷对网络系统的硬件、软件及系统中的数据进行的攻击。被动攻击一般不会对数据进行篡改，而是利用截取或窃听等方式在未经用户授权的情况下对消息内容进行获取，或者对业务数据流进行分析。被动攻击主要分为窃听和流量分析两种方式。

1. 窃听

窃听原本指偷听别人之间的谈话，随着通信技术的应用和发展，窃听的含义早已超出了偷听和搭线截听电话的概念，开始借助于技术手段窃取网络中的信息，既包括以明文形式保存和传输的信息，也包括通过数据加密技术处理后的密文信息。

一些窃听的实现需要打破原有的工作机制，如对加密后密文的窃听需要对获取的密文进行破解后才能得到明文信息。而有些窃听的实现则利用了网络已有的工作机制，如目前广泛使用的以太网是一种广播类型的分组网络，任何一台接入以太网的计算机都可以接收到本网段中的广播分组，当网卡设置为混杂模式时可以接收到本网段中的所有分组，若网络通信没有采用加密机制，便可以通过协议分析获知全部的报文信息。例如，无线局域网(Wireless Local Area Networks，WLAN)目前采用 2.4GHz 和 5.0GHz 两个微波频段通信，由于微波信号以电磁波的形式在开放空间中传输，所以任何一台工作在该频段的设备在信号传输的有效范围内都可以接收到承载着各类信息的信号，然后通过信号分析便可以恢复得到原始信号。

2. 流量分析

数据在网络中传输时都以流量进行描述，流量分析建立在数据拦截的基础上，对截获的数据根据需要进行定向分析。Internet 中，流量在节点之间传输时都需要遵循 TCP/IP 体系结构所确定的协议，在分层模型中每一层对网络流量的格式定义称为协议数据单元(Protocol Data Unit，PDU)。其中，物理层的 PDU 称为数据位(bit)，数据链路层的 PDU 称为数据帧(frame)，网络层的 PDU 称为分组(packet)，传输层的 PDU 称为数据段(segment)，应用层的 PDU 统一称为报文(message)。

流量分析攻击可以针对分层结构的每一层，最直接的是通过对应用层报文的攻击直接获得用户的数据。对于传输层及其以下层的 PDU 虽然无法直接获得具体的信息，但攻击者通过对获取的 PDU 的分析，便可以确定通信双方的 MAC 地址、IP 地址、通信时长等，进

而确定通信双方所在位置、传输的数据类型、通信的频度等，这些信息为进一步实施后续的攻击提供了重要依据。例如，通过对通信双方所占用带宽和通信时长的分析，便可以知道双方信息交换的信息类型；通过对流量的协议分析，便可以推断出用户数据的类型；通过对异常流量的分析，可以判定网络是否存在攻击等。

1.3　网络攻击的属性

网络攻击的实施是一个系列过程，同时涉及技术和非技术因素。对于任何一个攻击来说其实施过程都不是单一的，而是由一个或多个不同阶段组成的，其中不同的阶段体现出不同的攻击特点。研究网络攻击的目的是通过掌握攻击的实施过程来确定对应的防御方法。攻击涉及安全，而安全具有相对性，所以在具体的研究过程中，受研究条件、研究环境、把控能力等因素的影响，人们对各种网络攻击的理解不尽相同，进而对网络攻击的判定和特征的提取方法也不相同，对网络攻击及其造成危害或威胁的认识程序也不一致，从而对网络的防御带来了一定的困难。为便于对攻击过程的理解，本节选择从攻击中抽取属性的方法，将攻击分为权限、转换方法和动作 3 种类型。

1.3.1　权限

网络中的权限用于确定谁能够访问某一系统及能够访问这一系统上的哪些资源。对于任何一个授权访问系统来说，权限管理对其安全性是非常重要的。以 Windows Server 操作系统来说，用户被分成多个组，每个组设置了不同的权限，组与组之间的权限不同。其中，Administrators(管理员组)默认具有最高的权限，位于该组中的用户可以对计算机或域进行任意权限的操作；Power Users(高级用户组)中的用户可以执行除了为 Administrators 组保留的任务外的其他任何操作系统任务，其权限仅次于 Administrators；Users(普通用户组)中的用户可以运行经过验证的应用程序，但无法修改操作系统的设置或用户信息。通过对不同类型的用户设置不同的权限，可以加强对用户的分类管理，以提高系统的安全性。

根据访问方式的不同，权限又分为远程网络访问、本地网络访问、用户访问、超级网络管理员访问和对主机的物理访问等类型。任意一种访问如果被恶意利用，便构成了针对该访问方式的攻击。

1. 远程网络访问攻击

远程网络访问攻击属于一种外部攻击方式，它是通过各种手段，从被攻击者所在网络外发起的攻击行为。

2. 本地网络访问攻击

本地网络访问攻击属于一种内部攻击方式，攻击者和被攻击者属于同一个网络(多为内部局域网)，也可能是攻击者为了隐藏自己的真实身份，从本网络获取了被攻击者的必要信息后，从外部发起攻击，造成外部入侵的假象。

3. 用户访问攻击

用户访问攻击属于利用账户的攻击方式，攻击者在非法获得了合法用户账户信息后，冒

充合法用户访问系统或资源。

4. 超级网络管理访问攻击

超级网络管理访问攻击属于利用账户的攻击方式，攻击者在非法获得了系统管理员的账户信息后，冒充系统管理员对系统进行非法的操作。

5. 对主机的物理访问攻击

作为内部攻击方式时，攻击者通常获得能够直接接触被攻击主机的机会，对主机进行物理破坏；作为外部攻击方式时，攻击者在入侵被攻击对象后通过植入木马或病毒对内存或硬盘等主机的硬件进行破坏。

1.3.2 转换方法

转换方法是指攻击者对已有漏洞的利用。攻击过程的实施需要借助通信机制，通过对已有机制存在的漏洞的利用来实现。转换方法主要包括以下几种。

1. 伪装

伪装就是将攻击者的秘密信息隐藏于正常的非秘密文件中，常见的有图像、声音、视频等多媒体数字文件。伪装技术不同于传统的加密技术，加密操作仅仅隐藏了信息的内容，而信息伪装不但隐藏了信息的内容而且隐藏了信息的存在。伪装攻击最大特点是具有隐蔽性，不易被发现。

2. 滥用

滥用主要是指针对系统功能和权限的非法利用。例如，针对权限的滥用多是指服务端开放的功能超出了实际的需求，或者服务端开放的权限对具体需求的限制不严格，导致攻击者可以通过直接或间接调用的方式达到攻击效果。

3. 执行缺陷

缺陷(Bug)是指系统或程序中隐藏着的一些未被发现的错误或不足，程序设计中存在的缺陷会导致功能不正常或运行不稳定。执行缺陷是指攻击者对系统或程序中缺陷的发现和利用。

4. 系统误设

用户需求的多元化导致了应用系统功能的多样性，但对于某一个具体的应用来说其功能需求是确定的。然而，在系统部署过程中，受技术熟练程度、需求掌握情况及安全意识等方面的限制，对系统功能的设置往往没有做到与具体功能的对应，出现了超出预定需求甚至是错误的设置。错误设置尤其是安全功能的错误设置一旦被攻击者利用，就会对安全造成威胁。

5. 社会工程学

社会工程学被认为是反映当代社会现象发展复杂性程度的一门综合性的社会科学，其目标是对各种社会问题进行实例分析和解决。它并不是将人文科学、社会科学、自然科学的知识与技术简单相加，而是根据计划、政策的概念，在重构这些知识和技术的基础上，进行新的探索和整合。社会工程学攻击是一种针对受害者本能反应、好奇心、信任、贪婪等心理陷阱采取诸如欺骗、伤害等危害手段，获得自身利益的手法。传统的计算机攻击者在系统入侵