网络空间安全系列规划教材
普通高等教育“十三五”规划教材

网络与信息安全基础

（第2版）

◎ 王 颖　蔡 毅　主编　　◎ 周继军　夏华胜　彭松宇　副主编

中国工信出版集团
電子工業出版社
PUBLISHING HOUSE OF ELECTRONICS INDUSTRY
http://www.phei.com.cn

网络空间安全系列规划教材

普通高等教育“十三五”规划教材

网络与信息安全基础

（第2版）

王　颖　蔡　毅　主　编

周继军　夏华胜　彭松宇　副主编

電子工業出版社

Publishing House of Electronics Industry

北京 · BEIJING

内 容 简 介

本书全面介绍计算机网络安全的总体情况和发展趋势。本书共 14 章，内容包括网络安全概述、网络安全与信息加密、数字签名和认证、信息隐藏、计算机病毒及防范、远程访问、数据库安全、ASP.NET 安全、电子邮件安全、入侵检测系统、网络协议的缺陷与安全、网络隔离、虚拟专用网络、无线网络安全等若干关键课题内容。本书概念准确、内容新颖、图文并茂，既重视基础原理和基本概念的阐述，又紧密联系当前一些前沿科技知识，注重理论与实践的有机统一。

本书既适合网络空间安全、计算机相关专业的本科生和专科生学习，又可作为网络安全技术开发人员的工具书，对相关企事业单位的信息主管及普通工作人员具有一定的参考价值。

图书在版编目（CIP）数据

网络与信息安全基础 / 王颖，蔡毅主编. —2 版. —北京：电子工业出版社，2019.9
ISBN 978-7-121-36690-1

Ⅰ. ①网… Ⅱ. ①王… ②蔡… Ⅲ. ①计算机网络－信息安全－高等学校－教材 Ⅳ. ①TP393.08

中国版本图书馆 CIP 数据核字（2019）第 103082 号

策划编辑：戴晨辰
责任编辑：韩玉宏
印　　刷：北京捷迅佳彩印刷有限公司
装　　订：北京捷迅佳彩印刷有限公司
出版发行：电子工业出版社
　　北京市海淀区万寿路 173 信箱　　邮编：100036
开　　本：787×1 092　1/16　印张：23.75　字数：718.2 千字
版　　次：2008 年 8 月第 1 版
　　2019 年 9 月第 2 版
印　　次：2019 年 9 月第 1 次印刷
定　　价：69.00 元

凡所购买电子工业出版社图书有缺损问题，请向购买书店调换。若书店售缺，请与本社发行部联系，联系及邮购电话：（010）88254888，88258888。

质量投诉请发邮件至 zlts@phei.com.cn，盗版侵权举报请发邮件至 dbqq@phei.com.cn。

本书咨询联系方式：dcc@phei.com.cn。

前言

Preface

“得人者兴，失人者崩。”网络空间的竞争，归根结底是人才竞争。建设网络强国，没有一支优秀的人才队伍，没有人才创造力迸发、活力涌流，是难以成功的。2016 年 4 月 19 日，习近平总书记主持召开网络安全和信息化工作座谈会，做出了“培养网信人才，要下大功夫、下大本钱，请优秀的老师，编优秀的教材，招优秀的学生，建一流的网络空间安全学院”的重要指示。

本书的第 1 版是普通高等教育“十一五”国家级规划教材，自出版以来被多所高校选为教材，读者反响良好。为贯彻落实中央关于加强网络安全人才培养，特别是教材体系建设的精神，我们决定对本书的第 1 版进行修订。

本书根据第 1 版在使用时广大读者的反馈意见重新梳理，删减了原理性较强的知识点，总结性地介绍了关键理论，并把容易混淆的知识点进行了比较，同时大幅增加了实验截图和操作步骤，以便读者在学完基础理论后，通过动手实验来加深对知识的理解。本书介绍了关键的网络安全技术，使用 Windows Server 2016、IIS 10.0、Microsoft SQL Server 2008、Office 2016 等新版本软件进行实验和演示，以提高学生的动手实践能力。

本书内容系统、全面，更注重理论与实际的结合，每章内容编写力求讲清安全概念、安全理论、安全策略、安全实践和安全评估。每章都配有课后习题，帮助读者复习和巩固所学内容，并启发读者思考。

本书包含 PPT、源代码、工具包等配套教学资源，读者可登录华信教育资源网（www.hxedu.com.cn），注册后免费下载。

本书由王颖、蔡毅担任主编，由周继军、夏华胜、彭松宇担任副主编。本书的编写得到了北京亿中邮信息技术有限公司白玥、高塚工程师的大力支持，华为 3Com 技术有限公司季勇军、陈旭工程师，华为技术有限公司田野工程师，北京联信永益科技股份有限公司沈虹工程师，深信服科技股份有限公司官俊东工程师为本书提供了很多有价值的建议，王善强、何培培、吴博文为本书内容编写提供了方便的测试环境，在此一并对他们表示诚挚的谢意！

本书第 1 版在使用中收到了很多专家、高校教师、学生反馈的意见和建议，这些意见和建议对本书的修订帮助甚大，在此对他们表示谢意！ 同时，希望有更多读者能够对本书提出意见和建议，这将有助我们在今后继续更新、完善本书，编者邮箱为 caiyi@travelsky.com。

编　者

目录

Contents

第1章　网络安全概述

本章要点

随着计算机网络的发展，网络安全及其相关技术得到了前所未有的重视。本章的讲解将对本书后面章节的学习起到提纲挈领的作用。

本章的主要内容如下。

- 网络安全的现状。
- 针对校园网的攻击与防护。
- 校园网的安全管理。

1.1　为什么要重视网络安全

1.1.1　网络安全的现状

随着我国教育信息化的飞速发展，城域网和校园网的建设与应用得到了广泛的普及。然而，网络的信息安全问题不容乐观。我国校园网安全问题已经成为教育主管部门和各地学校管理者关心和研究的重要课题。

1．安全事件的发生呈上升趋势

据工业和信息化部网站统计，2018 年第一季度共监测网络安全威胁约 4541 万个，其中电信主管部门收集约 216 万个，基础电信企业监测约 1168 万个，网络安全专业机构监测约 6 万个，重点互联网企业和网络安全企业监测约 3151 万个。教育行业虽然不具有较高的商业价值，也不是网络攻击的主要目标，但是庞大的普通用户数量和相对较弱的安全防护意识，也导致了校园网内信息安全事件的频繁发生。

截至 2018 年上半年，各种网络钓鱼攻击增加了 74%，勒索软件攻击事件和商业电子邮件入侵（Business E-mail Compromise，BEC）事件也在逐步增多，这些都成为互联网安全的主要威胁，各种恶意软件通常在用户不知情的情况下把截获的用户信息发送给“信息收集者”，如盗取用户网络游戏的账号，并变卖玩家的装备，甚至是商业信息，这些都严重损害了使用者的利益。

各地中小型校园网虽然都会有一定的安全防护，但是学生的接入设备、共享 Wi-Fi 接入等终端并不在安全控制范围内，导致蠕虫病毒、间谍软件、网络钓鱼等各种恶意代码充斥在校园网中，严重影响了校园网的正常运行。

2．安全标准引用不及时

根据 BSI（British Standards Institution，英国标准协会）的统计，我国通过国际安全认证的企业和政府信息化职能部门相对较少，而引入某个管理标准进行管理的校园网就更少了。目前，校园网的网络结构没有统一的样式，安全产品和邮件服务器也应用着不同厂商的产品，网络管理员的维护技术和厂家的支持技术良莠不齐。

1.1.2　加强青少年的网络安全意识

有些青少年为了满足自己的好奇心，利用从网络上学来的入侵手段，非法获取别人的信息，恶意修改团体、学校甚至政府机关的网站，这些都触犯了我国的法律。需要指出的是，这类攻击

者号称黑客，其实他们只是网络攻击工具的使用者，简称 Tools User。

因此，我们应加强计算机安全教育，包括提高各级网络管理人员对网络重要性的认识和安全措施的掌握水平，向社会宣传计算机网络入侵的破坏性，尤其要加强拥有 Internet 访问能力的青少年的网络安全法律观念。

具体措施包括：以公益广告的形式向社会宣传计算机网络安全的重要性和法律含义；在校园网的主页以醒目的方式告诫有入侵倾向的网络用户；在注册校园网用户时，要求实名制；网络管理员在发现不明身份的用户时，应立即确定其身份，并对其发出警告，提前制止可能的网络犯罪；应该有专门的网络安全管理人员对校园网进行时段监控，并定期进行安全检查，同时应在网络中配置相关的安全检测工具。

切实加强网络的安全配置和管理，做到防患于未然，可以有效降低计算机网络受到攻击的频率，减少因受到攻击而产生的损失，增强校园网的安全性。

1.2 什么是攻击

仅在入侵行为已经完成，且入侵者已进入目标网络内的行为称为攻击。但关于攻击的定义更为积极的观点是，所有可能使一个网络受到破坏的行为都称为攻击，即从一个入侵者开始寻找目标机的那个时刻起，攻击就开始了。

通常，在正式攻击之前，攻击者先进行试探性攻击，目的是获取系统有用的信息，此时的攻击手段包括 Ping 扫描、端口扫描、账户扫描、DNS 转换、恶性的 IP Sniffer（通过技术手段非法获取 IP 包，以获得系统的重要信息）及特洛伊木马程序等。

1.2.1 收集信息的主要方式

经常使用的信息收集软件包括 NSS、Strobe、Netscan、SATAN（Security Administrator's Tool for Auditing Network）、Jakal、FTPScan 及各种 Sniffer 软件。从广义上讲，特洛伊木马（Trojan）程序是收集信息攻击的重要手段。收集信息攻击有时是其他攻击手段的前奏。对于简单的端口扫描，敏锐的网络安全管理员往往可以从异常的日志记录中发现攻击者的企图。但是对隐秘的 Sniffer 软件和特洛伊木马程序来说，检测它们的存在是一件高级和困难的任务。

1. Sniffer

Sniffer 本来是用来诊断网络连接情况的，是带有很强 DeBug 功能的常用网络分析器，所以黑客利用它来截获用户口令等敏感信息，甚至还可以用它来攻击相邻的网络。

检测 Sniffer 的存在是一个非常困难的任务，因为 Sniffer 本身只是被动地接收数据，而不发送任何数据包。

一般来讲，真正需要保密的只是一些关键数据，如用户名和口令等。因此，可以使用 IP 包级的加密技术，这样即使 Sniffer 得到数据包，也很难得到真正的数据信息。这样的工具包括 Secure Shell（SSH）及 F-SSH，尤其是 F-SSH 针对一般利用 TCP/IP 进行通信的公共传输提供了非常强大的、多级别的加密算法。另外，采用网络分段技术、减少信任关系等手段可以将 Sniffer 的危害控制在较小范围内。

2. 特洛伊木马

RFC 1244 中给出了特洛伊木马程序的经典定义："它提供了一些有用的或仅仅是有意思的功能。但是特洛伊木马程序通常会做一些用户不希望发生的事，诸如在用户不了解的情况下复制文件或窃取用户的密码、直接将重要资料转送出去和破坏系统等行为。"

很多情况下，特洛伊木马程序是在二进制代码中被发现的，它们大多无法直接阅读，并且可

以应用在很多系统平台上，它的传播方式和计算机病毒非常相似。从 Internet 上下载的软件（尤其是免费软件和共享软件）及从匿名服务器或 USERNET 新闻组中获得的程序等都有可能捆绑了特洛伊木马程序。因此，经常上网的用户自觉做到不轻易安装或使用来路不明的软件是十分必要的。2018 年 4 月份出现的木马病毒有 Ransom.Zenis 和 Backdoor.Teawhy 等。

检测一个特洛伊木马程序，需要深入了解有关操作系统的知识。用户可以通过检查文件的更改时间、文件长度、校验和等来判断文件是否进行过非预期的操作。另外，文件加密也是有效的检查特洛伊木马程序的方法。

1.2.2 攻击的主要手段

1. 口令入侵

口令入侵包括两个层次的行为：一种是破解使用加密口令加密了的用户文件，对于这种破解，攻击者可以很轻松地完成任务，因为目标文件通常已经下载到攻击者本地的计算机上，受害者对此已经无能为力；另一种是破解目标计算机的系统口令，对于这种破解，攻击者需要小心处理，以免触动目标计算机的报警系统，因为通常情况下，在系统账号登录失败达到一定次数后，计算机通常会自动锁死，并触发一定的日志记录功能或进行报警（包括向系统管理员发送电子邮件进行通知）。

2. 后门软件攻击

后门软件攻击是互联网上用得比较多的一种攻击手法。早期的 Back Orifice 2000、冰河等都是比较著名的后门软件，它们可以非法地取得用户计算机的超级管理员权限，并完全控制用户的计算机。这些后门软件一般分为服务器端和用户端两个部分，黑客进行攻击时，会使用用户端程序登录已安装好服务器端程序的计算机，这些服务器端程序都比较小，一般会被捆绑在某些软件上。另外，大部分后门软件的重生能力比较强，给用户的清理工作造成一定的困难。

目前最流行的是反弹端口的后门程序，这类后门程序不再区分客户端软件和服务器端软件，只需要安装在目标计算机上，使用的端口也是随机的，这对利用端口进行查毒的防护软件来说是一个很大的威胁。

3. 监听法

这一部分的内容请参阅 1.2.1 节的“Sniffer”部分。

4. 电子邮件技术

电子邮件（E-mail）是互联网上运用得十分广泛的一种通信方式。黑客可以使用一些电子邮件炸弹软件或 CGI 程序向目的电子邮箱发送大量内容重复、无用的垃圾电子邮件，使目的电子邮箱容量被占满，从而达到让其无法使用的目的。当垃圾电子邮件的发送流量特别大时，还有可能造成电子邮件系统对于正常的工作反应缓慢，甚至瘫痪的情况出现，这一点和本书后面要讲到的拒绝服务攻击（DDoS）比较相似。

电子邮件炸弹是一种简单有效的侵扰工具。它反复发送给目标接收者相同的信息，用这些垃圾信息填满用户的电子邮箱空间，如 bomb02.zip（Mail Bomber）软件（运行在 Windows 平台）和 EmailBomb 软件（运行在 UNIX 平台），它们的使用都非常简单。

同时，攻击者可以利用电子邮件列表，把攻击目标以电子邮件列表的方式注册到用户服务器的电子邮件列表中，或者直接通过用户的电子邮件列表发送垃圾电子邮件或带有计算机病毒的电子邮件。

对于遭受此类攻击的用户电子邮箱，可以使用一些垃圾电子邮件清除软件来解决，其中常见的有 Spam Eater、Spamkiller 等。Outlook 等软件也提供过滤功能，发现此类攻击后，将源目标地址放入拒绝接收列表中即可。

5．电子欺骗

电子欺骗（Spoofing Attack）包括两种攻击形式：一种是针对 HTTP、FTP、DNS 等协议的攻击，这种攻击可以窃取普通用户甚至超级用户的权限，任意修改信息内容，造成巨大危害；另一种攻击是 IP 欺骗，即攻击者伪造他人的 IP 地址，本质上就是让一台计算机来扮演另一台计算机，借以达到蒙混过关的目的。

几乎所有的电子欺骗都依赖目标网络的信任关系（计算机之间的互相信任）。入侵者可以使用扫描程序来判断远程计算机之间的信任关系。这种技术欺骗成功的案例较少，要求入侵者具备特殊的工具和技术（并且对非 UNIX 系统不起作用）。

6．拒绝服务

从网络攻击的各种方法和所产生的破坏情况来看，拒绝服务（Denial of Service，DoS）算是一种很简单但又很有效的进攻方式。它的目的是降低或中断用户服务器提供的访问能力，破坏组织的正常运行，最终它会使用户的 Internet 连接和网络系统部分或全部失效。DoS 的攻击方式有很多种，最基本的 DoS 攻击就是利用合理的服务请求来占用过多的服务资源，从而使合法用户无法得到服务。

1.2.3 入侵的常用策略

1．利用系统文件攻击

这里以攻击 UNIX 系统为例，黑客可以通过 Telnet 指令操作得知 Sendmail 的版本号，从而结合已公布的资料了解操作系统会有哪些安全漏洞。禁止对可执行文件的访问虽不能防止黑客对它们的攻击，但至少可以使这种攻击变得更困难。

2．伪造信息攻击

黑客可以通过发送伪造的路由信息，构造系统源主机和目标主机的虚假路径，从而使流向目标主机的数据包均经过攻击者的系统主机。这样攻击者就有可能获得用户密码等敏感信息。

3．利用协议弱点攻击

IP 地址的源路径选项允许 IP 数据包选择一条捷径通往系统目的主机。假设攻击者试图连接到防火墙后面的主机 A 上，攻击者只需要在送出的请求报文中设置 IP 源路径选项，使报文有一个目的地址指向防火墙，而最终地址是主机 A。当报文到达防火墙时被允许通过，因为它指向防火墙而不是主机 A。防火墙的 IP 层处理该报文的源路径被改变，并被发送到内部网上，报文就这样到达了主机 A。

4．网络钓鱼

在被攻击主机上启动一个可执行程序或打开一个链接，该程序或链接显示一个伪造的登录界面。当用户在这个伪装的界面上输入登录信息（用户名、密码等）后，该程序将用户输入的信息传送到攻击者主机，然后关闭界面给出提示信息“系统故障”，要求用户重新登录或跳转到一个真实的界面上，此后才会出现真正的登录界面。

5．利用系统管理员失误的攻击

网络安全的重要因素之一就是人。网络安全中常说的一句话就是：“堡垒最容易从内部攻破。”人为的失误包括 Web 服务器系统的配置差错、普通用户使用权限扩大等，这些给黑客造成了可乘之机。黑客常利用系统管理员的失误收集用于攻击的信息。

6．利用 ICMP 报文攻击

黑客利用 ICMP 报文的重定向消息可以改变路由列表，路由器可以根据这些消息建议主机走另一条更好的路径。攻击者可以有效地利用重定向消息把连接转向一个不可信的主机或路径，或者使所有报文通过一个不可信主机来转发。