每时每课 给你新机会

课工场 kgc.cn

云计算工程师系列

北京课工场教育科技有限公司 出品

◉ 视频课程 ◉ 案例素材 ◉ 交流社区 ◉ QQ讨论组

云计算与网络安全

主 编 肖 睿 徐文义
副主编 刘方涛 付 伟 王树军

中国水利水电出版社
www.waterpub.com.cn

云计算与网络安全

主　编　肖　睿　徐文义

副主编　刘方涛　付　伟　王树军

中国水利水电出版社
www.waterpub.com.cn

·北京·

内 容 提 要

云计算已经成为未来发展的趋势，虽然云计算带来了很多好处，但也同时带来了安全隐患。本书针对具备云计算基础的人群，首先介绍了网络信息安全体系、病毒木马、密码学、信息安全管理体系、局域网安全防御、VPN、防火墙、网站安全技术等传统的安全内容，然后介绍了与云计算相关的安全内容，既有理论又有实战，使读者对云计算安全有一个全面的认识。

本书通过通俗易懂的原理及深入浅出的案例，并配以完善的学习资源和支持服务，为读者带来全方位的学习体验，包括视频教程、案例素材下载、学习交流社区、讨论组等终身学习内容，更多技术支持请访问课工场 www.kgc.cn。

图书在版编目（CIP）数据

云计算与网络安全 / 肖睿，徐文义主编. -- 北京 : 中国水利水电出版社，2017.5
（云计算工程师系列）
ISBN 978-7-5170-5401-6

Ⅰ. ①云… Ⅱ. ①肖… ②徐… Ⅲ. ①云计算②计算机网络－网络安全 Ⅳ. ①TP393.027②TP393.08

中国版本图书馆CIP数据核字(2017)第107507号

策划编辑：祝智敏　责任编辑：李　炎　加工编辑：封　裕　封面设计：梁　燕

书　　名	云计算工程师系列 云计算与网络安全 YUNJISUAN YU WANGLUO ANQUAN
作　　者	主　编　肖　睿　徐文义 副主编　刘方涛　付　伟　王树军
出版发行	中国水利水电出版社 （北京市海淀区玉渊潭南路 1 号 D 座 100038） 网　址：www.waterpub.com.cn E-mail：mchannel@263.net（万水） sales@waterpub.com.cn 电　话：（010）68367658（营销中心）、82562819（万水）
经　　售	全国各地新华书店和相关出版物销售网点
排　　版	北京万水电子信息有限公司
印　　刷	北京泽宇印刷有限公司
规　　格	184mm × 260mm　16 开本　11 印张　242 千字
版　　次	2017 年 5 月第 1 版　2017 年 5 月第 1 次印刷
印　　数	0001—3000 册
定　　价	35.00 元

丛书编委会

前　言

在“互联网 + 人工智能”时代，新技术的发展可谓是一日千里，云计算、大数据、物联网、区块链、虚拟现实、机器学习、深度学习等，已经形成一波新的科技浪潮。以云计算为例，国内云计算市场的蛋糕正变得越来越诱人，以下列举了 2016 年以来发生的部分大事。

（1）中国联通发布云计算策略，并同步成立“中国联通沃云 + 云生态联盟”，全面开启云服务新时代。

（2）内蒙古斥资 500 亿元欲打造亚洲最大云计算数据中心。

（3）腾讯云升级为平台级战略，旨在探索云上生态，实现全面开放，构建可信赖的云生态体系。

（4）百度正式发布“云计算 + 大数据 + 人工智能”三位一体的云战略。

（5）亚马逊 AWS 和北京光环新网科技股份有限公司联合宣布：由光环新网负责运营的 AWS 中国（北京）区域在中国正式商用。

（6）来自 Forrester 公司的报告认为，AWS 和 OpenStack 是公有云和私有云事实上的标准。

（7）网易正式推出“网易云”。网易将先行投入数十亿人民币，发力云计算领域。

（8）金山云重磅发布“大米”云主机，这是一款专为创业者而生的性能王云主机，采用自建 11 线 BGP 全覆盖以及 VPC 私有网络，全方位保障数据安全。

在 DT 时代，企业对传统 IT 架构的需求减弱，不少传统 IT 企业的技术人员面临失业风险。全球最知名的职业社交平台 LinkedIn 发布报告，最受雇主青睐的十大职业技能中“云计算”名列前茅。2016 年，中国企业云服务整体市场规模超 500 亿元，预计未来几年仍将保持约 30% 的年复合增长率。未来 5 年，整个社会对云计算人才的需求缺口将高达 130 万。从传统的 IT 工程师转型为云计算与大数据专家，已经成为一种趋势。

基于云计算这样的大环境，课工场（kgc.cn）的教研团队几年前开始策划的“云计算工程师系列”教材应运而生，它旨在帮助读者朋友快速成长为符合企业需求的、优秀的云计算工程师。这套教材是目前业界最全面、最专业的云计算课程体系，能够满足企业对高级复合型人才的要求。参与本书编写的院校老师有徐文义、刘方涛、付伟、王树军。

课工场是北京大学下属企业北京课工场教育科技有限公司推出的互联网教育平台，专注于互联网企业各岗位人才的培养。平台汇聚了数百位来自知名培训机构、高校的顶级名师和互联网企业的行业专家，面向大学生以及需要“充电”的在职人员，针对与互联网相关的产品设计、开发、运维、推广和运营等岗位，提供在线的直播和录播课程，并通过遍及全国的几十家线下服务中心提供现场面授以及多种形式的教学服务，并同步研发出版最新的课程教材。

除了教材之外，课工场还提供各种学习资源和支持，包括：

- 现场面授课程
- 在线直播课程
- 录播视频课程
- 授课 PPT 课件
- 案例素材下载
- 扩展资料提供
- 学习交流社区
- QQ 讨论组（技术、就业、生活）

以上资源请访问课工场网站 www.kgc.cn。

本套教材特点

（1）科学的训练模式

- 科学的课程体系。
- 创新的教学模式。
- 技能人脉，实现多方位就业。
- 随需而变，支持终身学习。

（2）企业实战项目驱动

- 覆盖企业各项业务所需的 IT 技能。
- 几十个实训项目，快速积累一线实践经验。

（3）便捷的学习体验

- 提供二维码扫描、观看相关视频讲解和扩展资料等知识服务。
- 课工场开辟教材配套板块，提供素材下载、学习社区等丰富的在线学习资源。

读者对象

（1）初学者：本套教材将帮助读者快速进入云计算及运维开发行业，从零开始逐步成长为专业的云计算及运维开发工程师。

（2）初中级运维及运维开发者：本套教材将带读者进行全面、系统的云计算及运维开发学习，使其逐步成长为高级云计算及运维开发工程师。

课工场出品（kgc.cn）

课程设计说明

课程目标

读者学完本书后，能够理解网络安全及云计算安全的原理，同时具备一定的实际操作能力。

训练技能

- 能够通过模拟理解病毒、木马与后门技术的原理。
- 理解密码技术理论，并能够应用加密解密技术。
- 能够使用安全评估工具评估系统安全、Web 安全、网络安全。
- 掌握端口安全、DHCP 监听，了解入侵检测与防御系统。
- 理解 IPSec VPN 原理并掌握其应用。
- 理解防火墙原理，能够配置 H3C 路由交换及防火墙设备。
- 理解网站安全技术，包括缓冲区溢出、Hash 注入、SQL 注入、Cookie 欺骗、CSRF 攻击、维持访问技术、社会工程学等。
- 理解云计算的安全及防护。

设计思路

有关安全的很多内容不适合在教材中提供，请读者访问课工场网站来获取。

教材分为 9 个章节、2 个阶段来设计学习，即传统的网络安全、云计算安全，具体安排如下：

- 第 1 章～第 8 章介绍传统的网络安全，包括网络信息安全体系、病毒、木马与后门技术、密码技术、局域网安全防御、IPSec VPN 原理与配置、H3C 防火墙应用、网站安全技术等内容。
- 第 9 章介绍云计算的潜在利好和安全隐患，以及 IaaS 层面的安全风险等内容。

章节导读

- 技能目标：学习本章所要达到的技能，可以作为检验学习效果的标准。
- 本章导读：学习本章内容的原因和对本章内容的概述。
- 知识服务：提供二维码，内容可随时更新，更好地服务于读者。
- 内容讲解：对本章涉及的技能内容进行分析并展开讲解。
- 操作案例：对所学内容的实操训练。

- 本章总结：针对本章内容的概括和总结。
- 本章作业：针对本章内容的补充练习，用于加强对技能的理解和运用。

学习资源

- 学习交流社区（课工场）
- 案例素材下载
- 相关视频教程

更多内容详见课工场 www.kgc.cn。

课工场介绍

课工场是专注互联网教育的生态平台，汇聚了中国和北美数百位来自知名互联网企业的行业大咖，向寻求就业和技术提升的人群提供直播、录播、面授等多模式教学场景，并通过遍布全国的线下服务中心提供成熟的学习服务，形成完善的“互联网 + 教育”解决方案。同时，课工场也为高校、企业、行业提供教育技术赋能，依托 Transform 智能教育生态平台，打造智慧校园、企业大学、行业培训的教育场景，提供一站式教育解决方案。

课工场于 2016 年荣膺新浪网“2016 中国影响力科技创新教育机构”，腾讯网“2016 中国影响力教育品牌”，网易“2016 年度最受信赖教育机构”，小米“2016 教育行业突出贡献奖”。

扫一扫关注课工场公众号

关注微信 立送20K币
可购买收费课程

课工场APP客户端下载

产品/设计/开发/运维/运营
随时随地随心学

课工场岗位课程

- 大数据开发工程师
- 前端开发工程师
- Android 开发工程师
- PHP 开发工程师
- 新媒体运营师
- 互联网营销师
- 电子商务师
- 移动端 UI 设计师
- 网页 UI 设计师
- 互联网 UI 设计师
- 动漫设计师
- Python 开发工程师
- 云计算工程师
- VR 游戏设计师
- VR 游戏开发工程师
- VR 商用开发工程师
- 人工智能工程师

更多课程请访问 kgc.cn

联系我们

北京课工场教育科技有限公司

网址：kgc.cn

Q Q：800161516

邮箱：ke@kgc.cn

电话：010-88550007

地址：北京市海淀区成府路 207 号 B 座一层

目　录

第1章

计算机网络安全

技能目标

- 了解操作系统安全
- 掌握应用程序和服务安全
- 理解企业网络安全的基本架构
- 了解企业网络所面临的安全威胁
- 掌握网络攻击的常见方法
- 了解网络安全解决方案

本章导读

随着计算机与网络技术的飞速发展，信息安全的重要性也日益突显。在高度信息化的应用环境中，企业和个人的各种数据、服务器系统、应用服务乃至各种硬件设备，或多或少都面临着不同程度的安全风险。若要提高我们的安全加固和防御能力，建立起全面的安全意识是非常必要的。

企业局域网接入 Internet 后，一方面拉近了企业用户与世界的距离，企业用户可以与世界各地的人进行沟通，进行信息交换。另一方面也带来了很多风险。例如，企业要提供自己的网站供 Internet 上的用户访问，可能会有恶意用户篡改网站主页或者渗透到内部主机上窃取企业机密数据。还有，如果开放了 FTP 服务供 Internet 用户交互，可能会因为黑客的攻击而发生服务器拒绝对外提供服务的问题。

本章将学习计算机安全的基础知识，包括处理操作系统面临的常见风险、了解操作系统的安全级别、服务的安全、数据文件的保护，以及如何防范有害程序等。

知识服务

1.1 计算机面临的主要风险

计算机在家庭和企事业单位中得到了空前规模的应用，人们越来越依赖计算机帮助他们处理各种繁杂的数据。在实现资源共享、提升效率的同时，也发生了大量的重要数据丢失、密码泄露等黑客攻击事件，给企业和个人造成了严重的损失。世界上最著名的黑客 Kevin Mutnik，从 15 岁开始，陆续成功入侵过北美空中防护指挥系统、联邦调查局、太平洋电话公司等网络系统。现在，黑客的攻击手段层出不穷，根据攻击对象、安全弱点的不同，攻击者所采用的方法也千变万化。了解常见的一些攻击方法，将有助于大家及时采取有效的防护措施，制定更有针对性的安全策略。

1.1.1 利用漏洞

通过特定的操作，或使用专门的漏洞攻击程序，利用操作系统、应用软件中的漏洞，可入侵系统或获取特殊权限。

溢出攻击也是利用漏洞的一种攻击方法，它通过向程序提交超长的数据，结合特定的攻击编码，可以导致系统崩溃，或者执行非授权的指令，获取系统特权等，从而产生更大的危害。

SQL 注入是一种典型的网页代码漏洞利用。大量的动态网站页面中的信息，都需要与数据库进行交互，若缺少有效的合法性验证，则攻击者可以通过网页表单提交特定的 SQL 语句，从而查看未授权的信息，获取数据操作权限等。

1.1.2　暴力破解

暴力破解多用于密码攻击领域，即使用各种不同的密码组合反复进行验证，直到找出正确的密码。这种方式也称为“密码穷举”，用来尝试的所有密码集合称为“密码字典”。从理论上来说，任何密码都可以使用这种方法来破解，只不过越复杂的密码需要的破解时间也越长。例如，破解 WiFi 密码、压缩文件密码、Office 文件密码等大都使用此方法。

1.1.3　木马植入

通过向受害者系统中植入并启用木马程序，在用户不知情的情况下窃取敏感信息（如 QQ 密码、银行账号、机密文件），甚至于夺取计算机的控制权。当访问一些恶意网页、聊天工具中的不明链接，或者使用一些破解版软件，单击未知类型的电子邮件附件，甚至打开网友发来的所谓的照片、视频等文件时，都有可能被悄悄地植入木马。

木马程序好比潜伏在计算机中的电子间谍，通常伪装成合法的系统文件，具有较强的隐蔽性、欺骗性，基本都具有键盘记录甚至截图功能，收集的信息将会自动发送给攻击者。图 1.1 所示就是 QQ 粘虫弹出的假冒登录窗口，黑客借此得到用户输入的账号和密码。

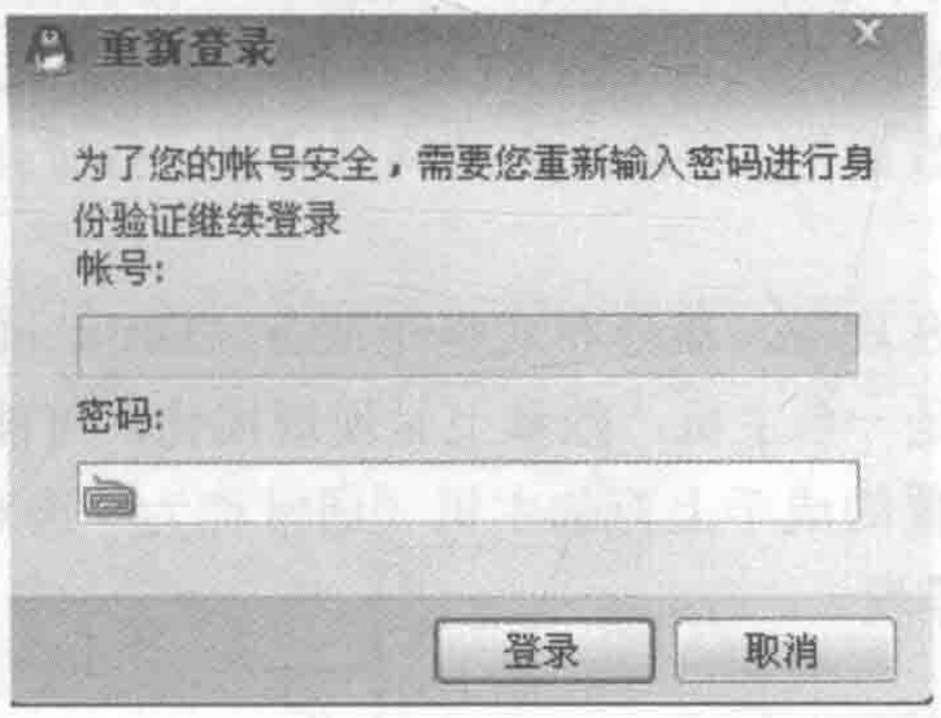

图 1.1　QQ 粘虫木马

1.1.4　病毒 / 恶意程序

与木马程序不同的是，计算机病毒（Virus）、恶意程序的主要目的是破坏（如删除文件、拖慢网速、使主机崩溃、破坏分区等），而不是窃取信息。其中病毒程序具有自我复制和传染能力，可以通过电子邮件、图片和视频、下载的软件、光盘等途径进行传播；而恶意程序一般不具有自我复制、感染能力等病毒特征。

病毒或恶意程序就好比进入计算机中的电子流氓，其明目张胆的破坏能力极具危害性，如臭名昭著的 CIH 病毒、千年虫、冲击波、红色代码、熊猫烧香等病毒。

1.1.5 系统扫描

实际上扫描还不算是真正的攻击，而更像是攻击的前奏，指的是利用工具软件来探测目标网络或主机的过程。通过扫描过程，可以获取目标的系统类型、软件版本、端口开放情况，发现已知或潜在的漏洞。

攻击者可以根据扫描结果来决定下一步的行动，如选择哪种攻击方法、使用哪种软件等；防护者可以根据扫描结果采取相应的安全策略，封堵系统漏洞、加固系统和完善访问控制等。

1.1.6 DoS

DoS（拒绝服务）全称为 Denial of Service，顾名思义，指的是无论通过何种方式，最终导致目标系统崩溃、失去响应，从而无法正常提供服务或资源访问的情况。导致拒绝服务的手段可以有很多种，包括物理破坏、资源抢占等。

DoS 攻击中比较常见的是洪水方式，如 SYN Flood、Ping Flood。SYN Flood 攻击利用 TCP 协议三次握手的原理，发送大量伪造源 IP 地址的 SYN，服务器每收到一个 SYN 就要为这个连接信息分配核心内存并放入半连接队列，然后向源地址返回 SYN+ACK，并等待源端返回 ACK。由于源地址是伪造的，所以源端永远都不会返回 ACK。如果短时间内接收到的 SYN 太多，半连接队列就会溢出，操作系统就会丢弃一些连接信息。这样客户发送的正常的 SYN 请求连接也会被服务器丢弃。Ping Flood 通过向目标发送大量的数据包，导致对方的网络堵塞、带宽耗尽，从而无法提供正常的服务。

威力更大的是 DDoS 攻击，即分布式拒绝服务（Distributed Denial of Service）。这种方式的攻击方不再是一台主机，数量上呈现规模化，可能是被发起者所控制的分布在不同网络、不同位置的成千上万的主机（通常称为“肉鸡”）。DDoS 攻击的发起或防御，都有较大的难度。

1.1.7 网络钓鱼

通过论坛、QQ、电子邮件、短信、弹出广告等途径发送声称来自某银行、某购物网站或其他知名机构（如网监、公安等）的欺骗信息，引诱受害者访问伪造的网站，以便收集用户名、密码、信用卡资料等敏感信息。

对于缺少安全经验的网民来说，钓鱼攻击很容易让人中招。从外观上看，攻击者伪造的网站与真正的网站几乎一模一样，网站域名也比较相似。例如，招商银行的真正网址为 www.cmbchina.com，攻击者可伪造一个外观相仿的 www.cmdchina.com 站点，并向受害者发送譬如“您的网银账号于 × 月 × 日登录失败，为了提高账号安全性，建议登录 http://www.cmdchina.com/ 重置密码……”的电子邮件，从而诱使其访问伪造站点以盗取其网上银行账号和密码等信息。