“十三五”国家重点出版物出版规划项目

高等教育网络空间安全规划教材

网络攻防原理与技术

第2版

吴礼发 洪 征 李华波 编著

提供电子教案

http://www.cmpedu.com

机械工业出版社
CHINA MACHINE PRESS

“十三五”国家重点出版物出版规划项目
高等教育网络空间安全规划教材

网络攻防原理与技术

第2版

吴礼发　洪　征　李华波　编著

机械工业出版社

本书着重阐述网络攻防技术原理及应用，内容包括：网络攻防概论、密码学基础知识、网络侦察技术、网络扫描技术、拒绝服务攻击、特洛伊木马、口令攻击技术、网络监听技术、缓冲区溢出攻击、Web 网站攻击技术、认证技术、访问控制技术、网络防火墙技术和入侵检测技术。各章均附有习题及实验项目。

本书可作为网络工程、信息安全和计算机等专业的教材，也可作为相关领域的研究人员和工程技术人员的参考书。

本书配有电子课件，需要的教师可登录 www. cmpedu. com 免费注册，审核通过后下载，或联系编辑索取（QQ：2850823885，电话：010－88379739）。

图书在版编目（CIP）数据

网络攻防原理与技术/吴礼发，洪征，李华波编著．—2 版．—北京：机械工业出版社，2016. 12

高等教育网络空间安全规划教材

ISBN 978-7-111-55201-7

Ⅰ．①网… Ⅱ．①吴… ②洪… ③李… 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（2016）第 249375 号

机械工业出版社（北京市百万庄大街 22 号 邮政编码 100037）

责任编辑：郝建伟 责任校对：张艳霞

责任印制：李 洋

中教科（保定）印刷股份有限公司印刷

2017 年 1 月第 2 版·第 1 次印刷

184mm×260mm·20. 25 印张·487 千字

0001－3000 册

标准书号：ISBN 978-7-111-55201-7

定价：49. 00 元

凡购本书，如有缺页、倒页、脱页，由本社发行部调换

电话服务

服务咨询热线：(010)88379833

读者购书热线：(010)88379649

网络服务

机 工 官 网：www. cmpbook. com

机 工 官 博：weibo. com/cmp1952

教育服务网：www. cmpedu. com

金 书 网：www. golden－book. com

高等教育网络空间安全规划教材
编委会成员名单

前　言

本书的第1版于2012年4月出版，至今已4年有余。在这期间，国内外安全形势发生了很大变化，包括中国在内的多数国家都已将网络空间安全上升到国家安全的战略高度，进而大大推动了网络攻防技术的快速发展。因此，第1版中介绍的部分内容已显得陈旧了。另一方面，经过几年的教学实践，对教材相关章节的安排及内容有了新的认识，也希望通过新版教材来体现。

编写教材最难处理的是内容的取舍，特别是网络攻防技术，内容繁多，实践性强。在有限的篇幅中，应当将哪些最重要的内容教给学生呢？经验表明，基本原理是核心。掌握了基本原理以后，既可以为自己编写攻防工具打下坚实的理论基础，也可以更快地掌握、更合理地使用已有的攻防工具和技术。因此，第2版遵循的原则仍然是阐述攻防技术的基本原理。尽管网络攻防领域特别强调实践能力，但本书并不希望将教材写成使用手册。每天都有大量新的攻防工具问世，我们希望给读者介绍这些工具背后所蕴含的关键技术的基本思想。当然，要想真正掌握一门网络攻防技术，只靠学习本书中的材料是远远不够的，还需要读者利用课程实验、大量的课外阅读和实践活动来实现。

与第1版相比，本书的章节修订简要说明如下。

第1章是绪论。本次修订重写了本章。2015年底，国务院学位委员会、教育部批准增设了“网络空间安全”一级学科。本章从网络空间安全一级学科的角度，全面介绍了网络空间安全发展历程和知识体系。目的是使读者在一级学科知识体系的大框架下，对网络攻防技术有一个总体的了解，为后续章节的学习打下基础。

第2章介绍密码学基础知识。考虑到学完如何加密的内容后，再来探讨破解密码的问题更符合认识规律，本次修订将有关密码分析的内容从2.1节“密码学概述”部分独立出来，放在本章的最后，同时增加了密码旁路分析技术、密码算法和协议的工程实现分析技术。

第3章介绍网络侦察技术。本次修订主要增加了近几年发展较快的以因特网上的设备为搜索对象的搜索引擎——Shodan的介绍。

第4章介绍网络扫描技术，主要对原有内容进行了更新与补充。

第5章介绍拒绝服务攻击。本章进行了比较大的修订，主要加强了近几年流行的反射式拒绝服务攻击方法和新型拒绝服务攻击防御技术的介绍，缩减了已较少使用的拒绝服务攻击方式的篇幅。

第6章介绍特洛伊木马。近年来，木马取代了传统的计算机病毒成为恶意代码的主要形式，是黑客最常利用的攻击手段。同时，木马、病毒和蠕虫等恶意代码之间的界限逐渐模糊，采用的技术和方法也呈多样化、集成化。因此，本次修订将第1版的第6章“计算机病毒”和第7章“特洛伊木马”合并为一章，以介绍木马为主，同时对木马涉及的相关技术进行了修订，以体现最新的技术状态。

第7章介绍口令攻击技术。操作系统、网络应用等的用户口令破解与防御是网络攻防对抗中的重要一环，因此，此次修订增加了口令攻击技术，主要介绍口令认证概述、操作系统口令破解、网络应用口令破解、常用文档口令破解和口令防御技术。

第8章介绍网络监听技术。此次修订重写了本章。首先按网络监听涉及的两个步骤（流量劫持、数据采集与分析）对第1版的章节安排进行了调整，其次增加了一些新的流量劫持技术、数据采集与解析技术原理的介绍。

第9章介绍缓冲区溢出攻击，第10章介绍Web网站攻击技术。此次修订主要对这两章的相关内容进行了更新，以反映最新的技术现状。

从第11章开始主要介绍典型的网络防护技术。第11章介绍信息认证技术，第12章介绍访问控制技术，第13章介绍防火墙的基本概念、工作原理、体系结构、评价标准和使用方法等，第14章介绍入侵检测技术。在此次修订中，对这些章节的相关内容进行了增加、删除或相应的改动。

最后，此次修订在每章（第1章除外）增加了与章节内容相匹配的实验项目，给出了每个实验的实验目的、实验内容及要求、实验环境等基本要素，供授课教师布置实验时参考。

本书可作为网络工程、信息安全及计算机等专业的教材，参考理论时数为40～50学时，实验时数为20～30学时。学习本门课程之前，读者最好已了解或掌握了有关计算机网络、操作系统或C程序设计等课程的内容。因此，建议在大学四年级或研究生阶段开设本课程。本书也可作为相关领域的研究人员、工程技术人员，以及广大网络攻防技术爱好者的参考书。

本书在编写过程中得到了作者所在课程建设小组其他成员（刘军教授、赖海光副教授、周海刚副教授、黄康宇讲师、周振吉博士）的大力支持，这里表示诚挚的感谢。

由于网络攻防涉及的内容广、更新快，加之作者水平有限，书中难免存在各种缺点和错误，敬请广大读者批评指正。

编　者

目　录

第1章 绪 论

本章从网络空间安全的角度，全面介绍了网络空间安全的发展历程、知识体系、安全防护技术概览和攻击技术概览。目的是使读者在网络空间安全学科知识体系的大框架下，对网络攻防技术有一个总体了解，为后续章节的学习打下基础。

1.1 网络空间安全概述

近年来，新服务的发展、通信量的上升和信息技术的进步这三股来自不同维度的力量不断推动着计算机网络向前发展。日益增长的网络应用需求催生了各种各样的新型网络服务，而新服务的实现对网络技术提出了新的要求。为了应对日益增长的网络流量，特别是多媒体流量的快速增长，各种新的网络传输技术相继出现，进一步促进了网络技术，尤其是移动传输技术的飞速发展。而信息技术的发展，特别是计算机技术和通信技术的发展，更是对网络的发展起到了非常大的促进作用。技术的发展进一步促进了网络在世界范围内的广泛应用，如同水电一样，网络已成为人们的日常生活不可或缺的部分。

人们在享受网络带来的种种好处时，也不得不面对它所带来的问题。长久以来，网络攻击一直呈指数级增长，成千上万的网络安全事件每天都在发生，小到普通民众、商业公司，大到军队、国家，无一例外均受到了不同程度的影响。网络安全在国家安全中的地位越来越重要，国家政治、经济、文化和军事等领域受网络的影响日益增强，世界各国纷纷将网络安全提升到国家安全的战略高度。

同时，随着信息时代的到来，战争的形式也在发生着深刻的变化，现代战争已成为信息的战争。信息是战略资源、决策资源，毫不夸张地说，它就是武器系统的核心，更是战场的灵魂。而网络作为敌对双方借以获取信息优势的制高点，与之相关的攻击与防护已成为军队作战的新模式，随着世界各国相继建立并大力发展网络战部队，网络战时代已经到来。

网络战是为干扰、破坏敌方网络信息系统并保证己方网络信息系统正常运行而采取的一系列网络攻防行动。网络战正在成为高技术战争的一种日益重要的作战样式，它能够破坏敌方的指挥控制、情报信息和防空等军用网络系统，甚至可以悄无声息地破坏、瘫痪和控制敌方的商务、政务等民用网络系统，不战而屈人之兵。

网络战的出现意味着国家级力量开始大力介入网络安全领域，也将网络攻防对抗提升到了一个新的高度，对抗的层次、水平和影响力均已远远超越以前的黑客攻击。例如，2010年9月发生的震网病毒攻击伊朗核电站事件，2013年斯诺登曝光的美国系列网络监控丑闻等，都对世界各国的网络安全领域带来了深远的影响。

网络安全形势千变万化，网络安全的内涵和外延随着技术的进步也在不断地丰富和拓展。

在计算机产生之前，网络安全主要是指通信安全，重点关注的是信息加密（信息的保密性）。计算机产生后，需要考虑计算机系统的安全，如保障计算机系统自身的完整性。计

算机网络产生后，“网络安全”中的“网络”主要是指计算机网络，包括计算机网络系统的硬件、软件，以及在网络中存储、传输和处理的数据。网络安全是指保护计算机网络不因偶然或恶意因素的影响而遭到破坏、更改或泄露，系统连续、可靠、正常地运行，网络服务不中断。

随着网络和通信技术的进一步发展，传统的以语音业务为主的“电信网络”，以及以视频业务为主的“有线电视网络”，在消除了政策上的障碍后，实现了基于 IP 的深度融合，即所谓的“三网融合”。网络安全领域也从计算机网络延伸到了电信网络和有线电视网络。

近几年来，网络安全进一步向物理世界和虚拟世界延伸，包括与国家基础设施密切相关的工业控制网络或系统（如电力网络、交通控制网络、城市供水网络、石油天然气网络和核电控制系统等）、虚拟的社交网络等，网络安全上升到了“网络空间安全”。目前，“网络空间”这一术语被广泛用于中、美等多国战略报告、论文和媒体报道中。网络空间也被称为与海、陆、空、太空并列的第五空间。

时至今日，国内外有关“网络空间”的定义还不统一，其内涵也在发展的过程中不断完善，下面对此做一个简要介绍。

美国最早使用 Cyberspace[㊀]一词来描述与信息和网络有关的物理和虚拟空间。国内对 Cyberspace 的翻译很多，比较典型的有：电磁空间、电子空间、网络空间、网际空间、虚拟空间、控域、网络电磁空间和赛博空间等，对其内涵的解读在学术界和工业界也呈百家争鸣的状态。接受度比较广的两种译法是“网络空间”和“赛博空间”，其中后者是音译。2015 年 6 月国务院学位办批准设立“网络空间安全”一级学科，采用的是“网络空间”这一名词。因而本书也采用“网络空间”的译法。

美国国家安全部门和美军对 Cyberspace 的理解也不完全一致，并且随着时间的推移，对其内涵的解读也在不断变化。据不完全统计，Cyberspace 有近 30 种正式定义，此外还有各种各样的个人解释。自 2004 年以来，美国政府先后推出了 4 种不同的官方定义。这些定义的基本思路相同，但侧重点略有区别。

2001 年初，美国国防部的“官方词典”——联合出版物 JP1 - 02 将 Cyberspace 定义为数字化信息在计算机网络中通信时的一种抽象（notional）环境。这个定义虽很简洁，但比较模糊，看不出确切的含义。

2003 年 2 月，布什政府发布了《保卫 Cyberspace 的国家安全战略》，其中将 Cyberspace 比喻为“国家中枢神经系统”，由成千上万的计算机、服务器、路由器和交换机用光纤互联在一起，支持关键的基础设施运行。这个定义除具体地列举了网络空间的组成外，还指出了计算机网络在国家、社会、政治、经济和军事上举足轻重的作用。

2006 年 12 月，美国参联会主席签署了《Cyberspace 行动的国家军事战略》，并将 Cyberspace 定义为“域”（domain），其特征是：使用电子技术和电磁频谱存储、修改和交换信

㊀ 科幻小说作家威廉·吉布森（William Gibson）在 1981 年出版的小说《Burning Chrome》（“整垮苛萝米”或“燃烧的铬”）中首次使用 Cyberspace 一词，表示由计算机创建的虚拟信息空间。当时 Cyberspace 与计算机网络还没有发生直接关联。大约到了 21 世纪初，Cyberspace 才被人们赋予更多的计算机网络内涵。在许多场合下，Cyberspace 可简称为 Cyber。例如，美军网络战司令部的名称为“Cyber 司令部”，其任务主要是保卫美国军用计算机网络，以防遭到Cyber 攻击。

息，并通过网络化的信息系统和物理基础设施达到此目的。该定义主要强调支撑 Cyberspace 的技术基础：电子技术和电磁频谱。

2008 年 1 月，布什签署了两份与网络安全（cyber security）相关的文件：第 54 号国家安全政策指令和第 23 号国土安全总统指令（NSPD－54/HSPD23），其中对 Cyberspace 的定义是："网络空间是由众多相互依赖的信息技术（IT）基础设施网络组成，包括因特网、电信网、计算机系统和用于关键工业部门的嵌入式处理器、控制器。还涉及人与人之间相互影响的虚拟信息环境"。这个定义首次明确指出 Cyberspace 的范围不限于因特网或计算机网络，还包括各种军事网络和工业网络。

2008 年 5 月，美国防部常务副部长戈登签署了一份备忘录，对上述的 Cyberspace 定义作了一些修订，删去了"关键工业部门"等字样，认为 Cyberspace 是全球信息环境中的一个领域，它由众多相互依存的 IT 基础设施网络组成，包括因特网、电信网、计算机网和嵌入式处理器、控制器。考虑到信息领域快速演变的特点，Cyberspace 的定义有可能会被进一步修订，备忘录建议在未得到进一步的通知之前，军方沿用这一定义。到目前为止，美国国防部或参联会没有发布新的定义。

2009 年 4 月，美国国防大学根据美国国防部负责政策的副部长的指示，组织专家学者编写出版《Cyberpower 和国家安全》一书，书中对 Cyberspace 的定义做了全面的解读：①它是一个可运作的（operational）空间领域，虽然是人造的，但不是某一个组织或个人所能控制的，在这个空间中有全人类的宝贵战略资源，不仅仅是用于作战，还可用于政治、经济和外交等活动，例如在这个空间中虽然没有一枚硬币流动，但每天都有成千上万美元的交易；②与陆、海、空、天等物理空间相比，人类依赖电子技术和电磁频谱等手段才能进入 Cyberspace，才能更好地开发和利用该空间资源，正如人类需要借助车、船、飞机或飞船才能进入陆、海、空、天物理空间一样；③开发 Cyberspace 的目的是创建、存储、修改、交换和利用信息，Cyberspace 中如果没有信息的流通，就好比电网中没有电流，公路网上没有汽车一样，虽然信息的流动是不可见的，但信息交换的效果是不言自明的；④构建 Cyberspace 的物质基础是网络化的、基于信息通信技术（ICT）的基础设施，包括联网的各种信息系统和信息设备，所以网络化是 Cyberspace 的基本特征和必要前提。

以上是美国政府安全部门和军队对 Cyberspace 的理解，美国民间对 Cyberspace 的理解也不尽相同。有人认为它是由计算机网、信息系统和电信基础设施共同构建的、无时空连续特征的信息环境；有人认为它是因特网和万维网（WWW）的代名词；但更多的人认为 Cyberspace 不限于计算机网络，还应包括蜂窝移动通信、天基信息系统等。有人认为 Cyberspace 是一种隐喻（metaphor），是概念上的虚拟信息空间；有人认为这个空间是社会交互作用的产物，包括从认知到信息再到物理设施三个层次。还有人强调 Cyberspace 和陆、海、空、天等物理空间的根本区别是：前者是非动力学（non－kinetic）系统，而后者是动力学（kinetic）系统。

牛津字典对"网络空间"的定义是：网络空间是通过计算机和全球因特网进行通信、控制和信息交换的虚拟空间。

国内对网络空间的定义也没有完全统一。著名网络安全专家方滨兴院士给出的定义是："网络空间是人运用信息通信技术系统进行数据交互的虚拟空间。其中，"信息通信技术系统"包括各类因特网、电信网、广电网、物联网、在线社交网络、计算系统、通信系统和

控制系统等电磁或数字信息处理设施；“数据交互”是指网民运用电磁或数字信息等形式所进行的信息通信技术活动”。它包含三个要素。

（1）载体：信息通信系统（包括各类因特网、电信网、广电网、物联网、在线社交网络、计算系统、通信系统和控制系统等，以及电子或数字信息处理设备等）。

（2）主体：网民、用户。

（3）规则：构造一个集合，用规则管理起来，称为“网络空间”。

上文介绍了“网络空间”这一重要概念，下面来讨论“网络空间安全（Cyberspace Security，简称 Cybersecurty）”。

网络空间安全涉及网络空间中电磁设备、电子信息系统、运行数据和系统应用中所存在的安全问题，既要防止、保护并处置“信息通信技术系统”及其所承载的数据受到损害，也要应对这些信息通信技术系统所引发的政治安全、经济安全、文化安全、社会安全与国防安全。针对上述风险，需要采取法律、管理、技术和自律等综合手段来应对，确保机密性、可用性、可控性得到保障。

网络空间安全主要研究网络空间中的安全威胁和防护问题，包括基础设施、信息系统的安全和可信，以及相关信息的保密性、完整性、可用性、真实性和可控性等相关理论和技术。从层次角度来看，网络空间安全主要包含四个层次的安全，从低到高分别如下。

（1）设备层安全：在网络空间中信息系统设备所面对的安全问题，主要包括：物理安全、辐射泄密、电子对抗、移动终端安全和硬件可靠等。

（2）系统层安全：在网络空间中信息系统自身所面对的安全问题，主要包括：运行安全、网络窃密、网络对抗、计算安全、传输安全、无线信道安全和软件安全等。

（3）数据层安全：在网络空间中处理数据时所带来的安全问题，主要包括：数据安全、密码破解、情报对抗、数据可信、数据保护和数据通信安全等。

（4）应用层安全：在信息应用过程中出现的安全问题，主要包括：内容安全、信息发掘、传播对抗、隐私保护、控制安全和身份安全等。

网络空间安全涉及的理论与技术众多，2015 年教育部“网络安全一级学科论证工作组”给出的网络空间安全知识体系主要包括网络空间安全基础理论、密码学基础知识、系统安全理论与技术、网络安全理论与技术，以及应用安全技术等五大类，如图 1-1 所示。

网络空间安全基础理论是支撑网络空间安全一级学科的基础，为网络空间安全其他研究方向提供理论基础、技术架构和方法学指导。主要内容包括：网络空间安全数学理论、网络空间安全体系结构、网络空间安全博弈理论、网络空间安全治理与策略、网络空间安全标准与评测，以及网络空间中人的安全行为与管理。

密码学基础主要研究在有敌手的环境下，如何实现计算、通信和网络的信息编码和分析。密码学为系统、网络及应用安全提供密码机制。主要内容包括：对称密码设计与分析、公钥密码设计与分析、安全协议设计与分析、侧信道分析与防护，以及量子密码和新型密码。

系统安全理论与技术主要研究网络空间环境下计算单元（端系统）的安全，是网络空间安全的基础单元。主要研究内容包括：芯片安全、系统硬件与物理环境安全、系统软件安全、恶意代码分析与防护、可信计算，以及先进计算安全等。

网络安全理论与技术是网络空间可靠、通信安全的保障。主要内容包括：通信基础设施