HZ BOOKS
华章教育

Pearson

网络空间安全学科规划教材

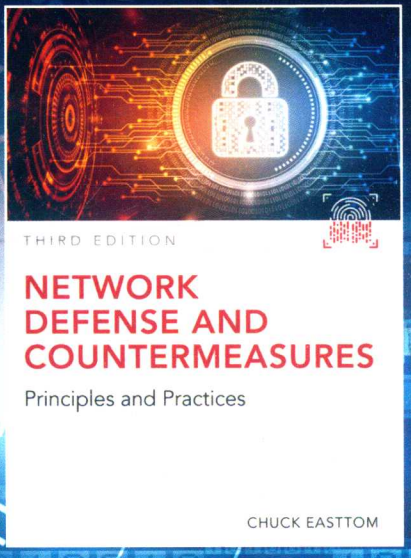
（原书第3版）

网络防御与安全对策
原理与实践

[美] 查克·伊斯特姆 （Chuck Easttom）◎著
刘海燕◎等译

Network Defense and Countermeasures

Principles and Practices
Third Edition



机械工业出版社
China Machine Press

网络空间安全学科规划教材

（原书第3版）

网络防御与安全对策
原理与实践

Network Defense and Countermeasures

Principles and Practices
Third Edition

[美] 查克·伊斯特姆 （Chuck Easttom）◎著

刘海燕◎等译

机械工业出版社
China Machine Press

图书在版编目（CIP）数据

网络防御与安全对策：原理与实践（原书第3版）/（美）查克·伊斯特姆（Chuck Easttom）著；刘海燕等译．—北京：机械工业出版社，2019.5
（网络空间安全学科规划教材）
书名原文：Network Defense and Countermeasures: Principles and Practices, Third Edition

ISBN 978-7-111-62685-5

I. 网… II. ① 查… ② 刘… III. 计算机网络－网络安全－教材 IV. TP393.08

中国版本图书馆CIP数据核字（2019）第083511号

本书版权登记号：图字 01-2018-3139

本书全面介绍了网络防御和保护网络的方法，内容包括网络安全的基本知识、虚拟专用网、物理安全和灾备、恶意软件防范、防火墙和入侵检测系统、加密的基础知识、用于确保安全的设备和技术、安全策略的概貌、基于计算机的取证等。每一章的结尾都给出了自测题帮助读者巩固所学知识。

本书不仅适合作为本科生或研究生学习网络安全知识的基本教材，还可以作为网络管理人员、安全专业人员、安全审计人员、网络犯罪调查人员等的随身参考书籍。

出版发行：机械工业出版社（北京市西城区百万庄大街22号 邮政编码：100037）

责任编辑：陈佳媛	责任校对：殷 虹
印 刷：三河市宏图印务有限公司	版 次：2019年6月第1版第1次印刷
开 本：185mm×260mm 1/16	印 张：22.75
书 号：ISBN 978-7-111-62685-5	定 价：119.00元

凡购本书，如有缺页、倒页、脱页，由本社发行部调换
客服热线：（010）88378991 88379833
购书热线：（010）68326294
投稿热线：（010）88379604
读者信箱：hzjsj@hzbook.com

译者序

网络安全近年来一直是最活跃的信息技术领域之一，在政治、经济、军事和社会发展中占据着越来越重要的地位。网络安全知识涉及面广，不仅包括概念、原理和技术，还涉及法律法规以及标准规范。网络安全领域的发展十分迅速，攻防双方的思想、方法和技术在激烈的对抗中不断地创新和突破。信息化要进一步普及和深化，保证网络安全是必备的基础。

许多国家都已认识到网络安全的重要性，不仅高度重视自身网络安全技术的研究和相关法律法规、标准规范的制定，尤其重视网络安全人才的培养以及网络安全知识的普及。合理的教学体系、合适的教材对网络安全人才的培养至关重要。无论从学习网络安全知识，锻炼网络安全技能，还是从培养网络安全意识的角度看，学习本书都是一个不错的选择。在翻译本书的过程中我们深刻体会到，作为一本网络安全知识的教材和参考书，本书内容广博、对关键内容解析透彻，作者根据自身经验对知识点、案例和习题都进行了精心的选择和设计。本书在结构和内容上具有如下特点：

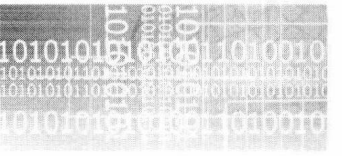
- **内容广博，对于全方位了解网络安全技术大有裨益**。全书共17章，不仅包括网络面临的安全威胁、网络安全防护技术及应用、网络调查取证等网络安全基本概念、原理和技术，还包括安全策略、安全评估、安全标准、网络恐怖主义等宏观的深层次问题。
- **内容深浅适度，线索清晰**。网络安全涉及的每项技术都有深刻的背景知识，要在有限的章节中介绍一个专题，必须在内容上精心选择，并在深度上进行权衡。本书在概念的解释说明、示例的选择、解决方案的选取以及习题的选择上都进行了精心设计，不仅讲解清楚，而且条理清晰、逻辑严密，便于读者把握章节的主题和内涵。
- **内容新颖及时，反映了网络攻击和防御方面的最新进展**。网络攻击和防御技术在双方的对抗中一直在不断发展和提高，新的思想、方法和技术不断出现，作者将新的概念、原理和技术及时引入教材，为处理新问题提供相应的解决方案。
- **内容实用性强，不仅有助于培养工程实践能力，而且能直接指导应用**。本书除了介绍基本的概念、原理、技术外，针对每类技术，还提供了行业内流行的解决方案。不仅夯实了理论知识，而且能对读者运用相关技术解决实际问题提供直接帮助。
- **习题丰富，便于加深对理论知识的理解，检验学习效果**。书中每章后面都提供了大量的自测题。其中，多项选择题主要是对已学概念、原理等知识进行检查；练习题主要是对一些方法和工具进行实践和操作；项目题主要是针对一个具体问题，让读者运用所学知识尝试求解。

内容广博、深浅适度、新颖及时、实用性强、习题丰富，这些特点使得本书不仅适合作为本科生或研究生学习网络安全知识的教材，还可以作为网络管理、安全开发、安全审计、网络犯罪调查等专业人员的参考书籍。对那些想初步了解网络安全知识的人员来说，本书也是不错的参考。

在翻译本书的过程中，项目组成员不仅对书中涉及的内容进行了深入研究，而且参考了国内外大量的相关资料。我们的原则是力图在遵从网络安全行业习惯称谓的基础上，用平实的语言反映作者的真实意图。对书中所涉及的专业术语、系统命令、软件工具等，译文参考了国内同行的习惯用法；对一些可能存在不同理解的问题，译文中增加了部分译者注，我们希望这些注释能减少可能存在的歧义，保持概念的清晰和准确。

本书内容涉及面广，参加翻译人员较多，译者之间反复多次互相审稿。参加本书翻译工作的人员包括：刘海燕、陈颖颖、李冠男、曹洁、武卉明、常成、张国辉、尚世峰、李红领、杨健康、张增等。刘海燕对全书进行了统稿和审校。鉴于译者水平有限，书中难免有错误和疏漏之处，敬请读者批评指正。

前言



当今 IT 行业最热门的话题是计算机安全。我们经常能看到关于黑客攻击、病毒以及身份窃取的新闻，安全已变得越来越重要。安全的基础是网络防御。本书全面介绍了网络防御知识，向学生介绍网络安全的威胁以及防护网络的方法。其中，有三章内容致力于介绍防火墙和入侵检测系统，还有一章详细介绍了加密技术。本书将网络的威胁信息、保护安全的设备和技术以及诸如加密这样的概念结合起来，为学生提供了一个坚实的、宽基础的网络防御方法知识框架。

本书融合了理论基础和实践应用。每章结尾都给出多项选择题和练习题，多数章节还给出了项目题。阅读全书后，学生应该会对网络安全有深刻的理解。此外，书中不断指导学生了解额外的资源，以便丰富相应章节中呈现的内容。

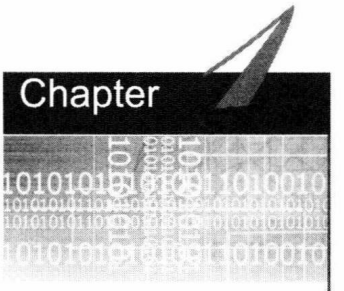
本书读者

本书主要是为那些基本理解网络运行机制（包括基本术语、协议和设备）的学生设计的。学生不需要拥有广泛的数学背景或高深的计算机知识。

本书内容

本书将带领读者全面了解防御网络攻击的复杂手段。第 1 章简要介绍网络安全领域。第 2 章解释网络的安全威胁，包括拒绝服务攻击、缓冲区溢出攻击和病毒等。第 3～5 章和第 7 章详细介绍各项网络安全技术，包括防火墙、入侵检测系统以及 VPN。这些技术是网络安全的核心内容，因此本书花很大篇幅来保证读者全面理解它们的基本概念和实际应用。每部分都给出为特定网络选择合适技术的实用性指导。第 6 章详细介绍加密技术。这个主题非常重要，因为计算机系统终究只是一个存储、传输和处理数据的简单设备。无论网络多么安全，如果它传输的数据不安全，那么就有重大危险。第 8 章指导如何增强操作系统的安全。第 9 章和第 10 章告诉读者防范网络上常见危险的具体防御策略和技术。第 11 章向读者介绍安全策略的内容。第 12 章教读者如何评估网络的安全性，其中包括审查安全策略的原则以及网络评估工具的概述。第 13 章概述通用的安全标准（如橙皮书和通用准则等），该章还讨论各种安全模型（如 Bell-LaPadula 等）。第 14 章研究经常被忽视的物理安全和灾难恢复问题。第 15 章介绍一些基本的黑客技术和工具，目的是使你更了解对手，同时介绍一些减轻黑客攻击后果的策略。第 16 章介绍基本的取证原则，当你或你的公司成为计算机犯罪的受害者时，学习该章内容有助于你做好调查准备。第 17 章讨论基于计算机的间谍和恐怖活动，这是两个在计算机安全界日益受到关注但在教科书中经常被忽视的话题。

目录



第1章 网络安全概述

本章目标

在阅读完本章并完成练习之后，你将能够完成如下任务：

- 识别出最常见的网络风险。
- 理解基本的组网技术。
- 使用基本的安全术语。
- 找到适合自己所在机构网络安全的最佳方法。
- 评估影响网络管理员工作的法律问题。
- 使用可用于网络安全的资源。

1.1 引言

在新闻中，很难发现哪一周没有发生重大安全破坏。大学网站被攻击、政府计算机被攻击、银行数据受损、健康信息被泄露——这个清单还在不断增长。而且似乎每年对这个问题的关注都在增加。在任何工业化国家中，很难找到没听说过诸如网站被黑客入侵和身份被盗之类事情的人。

目前培训场所也有很多。许多大学都提供从学士层次到博士层次的信息保障（Information Assurance）学位。有大量的行业认证培训项目，包括 CISSP（Certified Information Systems Security Professional，注册信息系统安全专家）、国际电子商务顾问委员会（EC Council）的 CEH（Certificated Ethical Hacker，道德黑客认证）、Mile2 ⊖ Security、SANS（System Administration, Networking, and Security Institute，美国系统网络安全协会）认证以及美国计算机行业协会（Computing Technology Industry Association，CompTIA）的 Security+。现在还有一些大学提供网络安全学位，包括远程学习的学位。

尽管受到媒体的关注和有获得安全培训的机会，但仍有太多的计算机专业人员，包括数量惊人的网络管理员，对网络系统暴露的威胁类型以及哪些是最有可能发

⊖ Mile2 是美国的一家信息技术安全公司，开发并提供 15 种被国际上广泛认可的网络安全认证。

生的威胁没有清晰的认识。主流媒体关注的是最引人注目的计算机安全破坏，而不是给出最有可能的威胁场景的准确画面。

本章着眼于网络面临的威胁，定义基本的安全术语，为后续章节涉及的概念奠定基础。确保你的网络完整性和安全性所需的步骤条理清晰，并在很大程度上进行了概括。当你学完本书时，你将能够识别最常见的攻击，解释攻击的机理以便阻止它们，理解如何确保数据传输的安全。

1.2　网络基础

在深入研究如何保护网络安全之前，探索一下什么是网络可能是个不错的想法。对许多读者来说，本节内容仅仅是一次复习，但对于部分读者来说可能是新的知识。无论对你来说是复习还是新的知识，在深入研究网络安全之前，对基本的组网原理有透彻的理解都是至关重要的。此外请注意，这里只是对基本网络概念的简要介绍，没有探究更多细节。

网络是计算机进行通信的一种方式。在物理层，网络由所有要连接的机器和用来连接它们的设备组成。独立的机器可通过物理连接（一根 5 类电缆插入网络接口卡，即 NIC）或通过无线方式连接起来。为了将多台机器连接在一起，每台机器必须连接到集线器或交换机，然后这些集线器 / 交换机再连接在一起。在更大的网络中，每个子网络通过路由器连接到其他子网络。本书中的许多攻击（包括第 2 章介绍的几种攻击），都是针对网络中将机器连接起来的设备（即路由器、集线器和交换机）发起的。如果你发现本章的知识不够用，那么下述资源可能会有所帮助：http://compnetworking.about.com/od/basicnetworkingconcepts/Networking_Basics_Key_Concepts_in_Computer_Networking.htm。

1.2.1　基本网络结构

在你的网络和外部世界之间一定存在一个或几个连接点。在网络和 Internet 之间建立一个屏障，这通常以防火墙的形式出现。本书讨论的许多攻击都要穿越防火墙并进入网络。

网络的真正核心就是通信——允许一台机器与另一台机器进行通信。然而，通信的每条通道也是一条攻击的通道。因此，理解如何保护网络的第一步，就是详细了解计算机如何通过网络进行通信。

前面提到的网卡、交换机、路由器、集线器以及防火墙都是网络基本的物理部件，它们连接的方式以及通信的格式就是网络体系结构。

1.2.2　数据包

当你与网络建立连接之后（无论是物理连接还是无线连接），就可以发送数据了。第一件事就是确定你想发送到哪里。我们先讨论 IPv4 的地址，在本章稍后部分再看一下 IPv6。所有的计算机（以及路由器）都有一个 IP 地址，该地址由四个 0 到 255 之间的数字组成，中间以圆点分隔，例如 192.0.0.5（注意这是一个 IPv4 地址）。第二件事是格式化要传输的数据。所有数据最终都采用二进制形式（多个 1 和 0 组成）。这些二进制数据被放入数据包（packet）中，总长度要小于大约 65 000 字节。前几个字节是首部（header）。首部内容说明数据包去往哪里、来自何方、本次传输还有多少个包。实际上，数据包有多个首部，但现在我们仅把

首部作为单个实体来讨论。我们将研究的一些攻击（例如，IP 欺骗）会试图改变首部以提供虚假信息。其他的攻击方法则只试图截获数据包并读取其内容（从而危害数据的安全）。

一个数据包可以有多个首部。事实上，大多数数据包至少有三个首部。IP 首部包含源 IP 地址、目标 IP 地址以及数据包的协议等信息。TCP 首部包含端口号等信息。以太网首部则包含源 MAC 地址和目的 MAC 地址等信息。如果一个数据包用传输层安全（Transport Layer Security，TLS）进行加密，那么它还将有一个 TLS 首部。

1.2.3　IP 地址

第一个要理解的主要问题是如何将数据包送到正确的目的地。即使是一个小型网络，也存在许多计算机，它们都有可能是发送数据包的最终目的地，而 Internet 上有数百万台遍布全球的计算机。如何保证数据包到达正确的目的地呢？这个问题就像写封信并确保信件能到达正确的目的地一样。我们从 IPv4 寻址开始讨论，因为它是目前使用最普遍的，但本节也会简要讨论一下 IPv6。

一个 IPv4 地址是用圆点分隔的由 4 个数字组合的数字序列（例如 107.22.98.198）。每个数字必须在 0 到 255 之间。可以看到，107.22.98.466 就不是一个有效的地址。之所以有这个规则，是因为这些地址实际上是 4 个二进制数，计算机用十进制格式把它们简单地显示出来。回想一下，1 字节是 8 位（1 和 0 的组合），而 8 位二进制数转换成十进制格式后将在 0 到 255 之间。总共 32 位则意味着大约存在 42 亿个可能的 IPv4 地址。

计算机的 IP 地址可以告诉你该台计算机的很多信息。地址中的第一个字节（或第一个十进制数）告诉你该机器属于哪一类网络。表 1-1 概括了 5 种网络类别。

表 1-1　网络分类

分　类	首字节的 IP 范围	用　途
A	0～126	特大型网络。目前 A 类网络地址已用尽，没有剩余
B	128～191	大型公司和政府的网络，所有的 B 类 IP 地址都已被使用
C	192～223	最常见的 IP 地址组，你的 ISP 可能有一个 C 类地址
D	224～247	预留给多播[⊖]（在同一信道上传送不同数据）
E	248～255	预留给实验用

这 5 种网络类别在本书后面将变得更加重要（或者，现在你应该决定在更深的层次上学习网络）。仔细观察表 1-1，你可能会发现 127 的 IP 范围没有被列出来，之所以存在这种省略，是因为该范围是被保留用于测试的。不管你的机器被指定为什么 IP 地址，地址 127.0.0.1 都是指你自己正在使用的这台机器。这个地址常被称为环回地址（loopback address），常用于测试你的计算机和网卡。我们将在本章稍后的网络实用程序部分讨论它的用法。

这些特定的地址分类很重要，因为它告诉你，地址的哪些部分代表网络、哪些部分代表节点。例如，在 A 类地址中，第一个 8 位的字节代表网络，其余三个表示节点。在 B 类地

⊖ IP 多播也称组播，使用多播地址可以将一个数据包发送给加入该组的多台主机。——译者注

址中，前两个 8 位的字节代表网络，后两个表示节点。而在 C 类地址中，前三个 8 位的字节代表网络，最后一个代表节点。

你还需要注意一些特殊的 IP 地址和 IP 地址范围。第一个是如前所述的 127.0.0.1，即环回地址。它是引用你正在使用的机器网卡的另一种方法。

另一个需要注意的问题是私有（private）IP 地址[⊖]。IP 地址中某些特定范围被指定仅用于网络内部。这些地址不能用作公开的 IP 地址，但可以用作内部工作站或服务器的地址。这些 IP 地址包括：

- 10.0.0.10 到 10.255.255.255
- 172.16.0.0 到 172.31.255.255
- 192.168.0.0 到 192.168.255.255

网络新人有时对公有 IP 地址和私有 IP 地址的理解有些困难。我们以办公楼做个类比：在一栋办公楼内，每个办公室的编号必须是唯一的。例如，在一栋大楼里只能有一个 305 办公室。如果讨论 305 办公室，你马上就明白说的是哪个房间。但还有其他的办公楼，许多楼都有自己的 305 办公室。因此，你可以将私有 IP 地址视为办公室编号，在它们所在的网络中它们的编号必须是唯一的，但在其他网络中可能有相同的私有 IP。

公有 IP 地址更像传统的邮件地址，它们在世界范围内必须是独一无二的。当从办公室到办公室通信时，你可以使用办公室号码，但是要给另一个建筑物发信，你必须使用完整的邮件地址。这与网络是一样的，你可以使用私有 IP 地址在网络内部进行通信，但要与网络外部的任何计算机进行通信时，都必须使用公有 IP 地址。

网关路由器的作用之一是执行所谓的网络地址转换（Network Address Translation，NAT）。通过 NAT，路由器将发出的数据包中的私有 IP 地址替换为网关路由器的公有 IP 地址，从而可以在 Internet 中路由该数据包。

我们已经讨论了 IPv4 网络地址，现在把注意力转移到划分子网上。如果你已经熟悉这个主题，那么请跳过本节。由于某种原因，这个话题往往会给学生带来很大麻烦。所以下面我们从理解概念开始。所谓划分子网（subnetting）就是简单地将网络切成更小的部分。例如，如果你拥有一个使用 IP 地址 192.168.1.X 的网络（X 代表任何具体计算机的地址），那么你已经被分配了 255 个可能的 IP 地址。如果想把它分成两个单独的子网络怎么办呢？你需要做的就是划分子网。

说得更专业一点，子网掩码（subnet mask）是分配给每个主机的一个 32 位数字，用于将 32 位二进制的 IP 地址划分为网络部分和节点部分。子网掩码不能随意指定，有特定的要求。子网掩码的第一个值必须是 255，剩下的三个值可以是 255、254、252、248、240、224 或 128。你的计算机把自己的 IP 地址和子网掩码通过二进制“AND”操作（二进制的“按位与”）结合起来。

你可能会很奇怪，因为即使你没有划分过子网，也已经拥有了一个子网掩码。这是默认子网掩码。如果你有一个 C 类 IP 地址，那么子网掩码是 255.255.255.0。如果有一个 B 类 IP 地址，那么子网掩码是 255.255.0.0。而如果是 A 类地址，则子网掩码是 255.0.0.0。

⊖ Internet 标准 RFC 1918 对私有网络地址分配进行了规定。——译者注