信息安全产品技术丛书

网络 NETWORK 入侵检测系统 原理与应用

丛书主编 顾健

主编 沈亮 陆臻 张艳 宋好好

電子工業出版社
PUBLISHING HOUSE OF ELECTRONICS INDUSTRY
http://www.phei.com.cn

014010726

TP393.08
697

信息安全产品技术丛书

网络 NETWORK 入侵检测系统 原理与应用

北京航空航天大学 藏书 图书馆

丛书主编 顾健

主编 沈亮 陆臻 张艳 宋好好

北航 C1697180

TP393.08
697

電子工業出版社
Publishing House of Electronics Industry
北京 • BEIJING

内 容 简 介

本书内容分为5章，从入侵检测系统的产品概述、技术详解、标准分析等内容入手，对入侵检测系统产品的产生需求、实现原理、技术标准、应用场景和典型产品等内容进行了全面翔实的介绍。

本书适合入侵检测系统产品的使用者（系统集成商、系统管理员）、产品研发人员及测试评价人员作为技术参考，也可供信息安全专业的学生及其他科研人员作为参考读物。

未经许可，不得以任何方式复制或抄袭本书之部分或全部内容。
版权所有，侵权必究。

图书在版编目（CIP）数据

网络入侵检测系统原理与应用 / 沈亮等主编. —北京：电子工业出版社，2013.10
（信息安全产品技术丛书）
ISBN 978-7-121-21584-1

Ⅰ. ①网… Ⅱ. ①沈… Ⅲ. ①计算机网络－安全技术－研究 Ⅳ. ①TP393.08

中国版本图书馆CIP数据核字（2013）第231793号

策划编辑：李 洁
责任编辑：刘 凡
印 刷：三河市鑫金马印装有限公司
装 订：三河市鑫金马印装有限公司
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：720×1 000 1/16 印张：9.5 字数：244千字
印 次：2013年10月第1次印刷
定 价：42.00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。

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。

服务热线：（010）88258888。

前言

<<<<< PREFACE

随着信息化时代飞速发展，为人们的生活带来了越来越多的便捷。但是一方面，互联网互联互通的开放性特性极大地方便了各种互联资源的联网，开创和拓宽了共享资源途径；另一方面，随着人类在经济、工业、军事领域方面越来越多地依赖信息化管理和处理，却由于信息网络在设计上对安全问题的忽视，以及爆发性应用背后存在的使用和管理上的脱节，逐渐使互联网中信息的安全性受到严重威胁。实用和安全矛盾逐渐显现，随着越来越多重要的信息应用以互联网作为运行基础，信息安全问题已经成为威胁民生、社会，甚至国家安全的重要问题。

如何来发现信息安全问题、防范安全威胁呢？入侵检测系统产品应运而生。

入侵检测系统产品通过提供精简的安全审计、入侵监测响应等功能，帮助系统安全管理员提高安全管理能力，使得系统安全管理员能够提早察觉，甚至挖掘出入侵威胁，辅助其及时采取安全措施弥补信息安全中存在问题和不足，从而提高信息系统整体安全防范的能力，特别在入侵问题定位及入侵行为取证方面具有良好的作用，对威胁信息安全的入侵者具有一定的威慑作用。

入侵检测系统产品产生的背景是什么？入侵检测系统产品的核心技术以及现行标准是如何实现的？本书就是带着这些问题开始展开陈述的。

本书是信息安全产品技术丛书之一。与以往注重产品和技术介绍的书籍不同，本书不仅从产品历史、技术方面进行了全面的描述，还特别对产品标准发展及应用方面进行了大量细致的介绍。本书内容力争全面，分析力求深刻，在产品历史、原理、标准、应用等几大方面均有翔实的描述。与此同时，本书力求使用，收集了许多实际数据与案例，期望能够给读者在入侵检测技术应用方面以一定的帮助。

本书的主要编写成员均来自公安部信息安全产品检测中心和公安部计算机信息系统安全产品质量监督检验中心，常年从事入侵检测系统产品的测评工作，对入侵检测系统产品有着深入的研究。本书的作者全程参与了入侵检测系统产品标准从规范、行标到国标制修订的工作。因此，本书在标准介绍和描述方面具有一定的权威性。

本书第 1 章主要由沈亮撰写，第 2 章主要由张艳撰写，第 3 章主要由陆臻撰写，第 4、5 章主要由宋好好、张艳、邵东撰写。顾健负责把握全书技术方向，并对各章节的具体编写提供了指导性意见，最后由沈亮完成全书修改和统稿工作。此外，邵

东、杨元原、王志佳、顾建新、张笑笑、俞优、吴其聪等同志也参与了本书资料的收集和部分章节的编写工作。由于编写人员水平有限和时间紧迫，本书不足之处在所难免，恳请各位专家和读者不吝批评指正。

在本书的编写过程中，得到了北京启明星辰信息安全技术有限公司、长沙博华科技有限公司、北京天融信科技有限公司、网神信息技术（北京）股份有限公司、北京冠群金辰软件有限公司、北京中科网威信息技术有限公司等单位的大力协助，在此表示衷心的感谢！

编著者

试读结束：需要全本请在线购买：www.ertongbook.com

目录

CONTENTS

Chapter 1

第1章 综 述

信息化技术的飞速发展为人们的生活带来了越来越多的便捷。但是一方面，互联网互联互通的开放性特性下极大地方便了各种互联资源的联网，开创和拓宽了共享资源途径；另一方面，随着人类在经济、工业、军事领域方面越来越多地依赖信息化管理和处理，却由于信息网络在设计上对安全问题的忽视，以及爆发性应用背后存在的使用和管理上的脱节，逐渐使互联网中信息的安全性受到严重威胁。实用和安全的矛盾逐渐显现，随着越来越多重要的信息应用以互联网作为运行基础，信息安全问题已经成为威胁民生、社会，甚至国家安全的重要问题。

如何来发现信息安全问题、防范安全威胁呢？入侵检测系统（IDS，Intrusion Detection System Product）应运而生。入侵检测系统通过提供精简的安全审计、入侵监测响应等功能，帮助系统安全管理员提高安全管理能力，使得系统安全管理员能够提早察觉，甚至挖掘出入侵威胁，辅助其及时采取安全措施弥补信息安全中存在问题和不足，从而提高信息系统整体安全防范的能力，特别在入侵问题定位以及入侵行为取证方面具有良好的作用，对威胁信息安全的入侵者具有一定的威慑作用。

从入侵检测系统实现形态上来看，它实际上是安全审计产品的一种重要的分支应用。它以网络中及重要主机节点上收集和审计的信息为基础，使用入侵检测算法分析出其中存在的违反安全策略的入侵和异常行为迹象。这种精简、突出的入侵检测信息能够大大降低系统安全管理员的管理成本，使他们能够集中精力解决信息系统中最危险的安全问题。因此，选用正确的入侵检测系统，对于提高整个信息系统架构的安全性，特别是复杂的多层结构信息系统的安全性，尤为重要。

本章首先对入侵检测系统的必要性进行分析，简要介绍入侵检测系统的基本原理，并介绍主机型和网络型入侵检测系统的发展历程。从宏观上使读者对入侵检测系统有充分的认识，为后续章节介绍具体的技术细节打下基础。

另外，入侵检测系统的英文翻译为 Intrusion Detection System，产品直译的意思为“入侵检测系统”。原来为了表示同其他等级保护信息系统标准的不同，行业标准使用了中文的“产品”进行标准命名。之后，随着系统标准同产品标准的区别越加明显，在国家标准中使用了中文的“系统”对标准进行了命名。本书对两种标准的命名方式都认可，因此在本书中“入侵检测系统”和“入侵检测系统产品”为同一个对象，不加以区别。

1.1 为什么需要入侵检测系统

1.1.1 黑客的产生严重威胁了信息的安全

自 20 世纪三四十年代世界上第一台电子计算机阿塔纳索夫-贝瑞在美国爱荷华州立大学诞生至今，计算机技术已经发生了翻天覆地的变化。计算机从当初用途单一的数学计算器已经发展成为具有无限扩展能力的一种超越计算的工具。而 ARPA 网络的建立，又使计算机互联成为现实，在全世界范围内掀起了基于互联网的信息化建设高潮，一个全新的基于虚拟信息资源为基础的全球信息化社会已经形成。非物质形态的信息成为一种新兴的重要资源，为越来越多的人们所重视。随着无限的计算能力和高度信息化成为可能，信息技术进入飞速发展时代。随之而来的是计算机信息时代催生出的计算机黑客。黑客们完成了从出生、成长、分化和壮大的演化过程，成为影响信息化社会有序环境的一支重要力量。

这些黑客们之所以能够以破坏信息化社会来达到威胁人类生活的原因，是由于构成信息化社会中基础的电子信息交流方式。随着文字、图像、语音、影像等数据依托信息化技术在互联网中生成和交流，电子信息交流方式对技术的依赖程度越来越强。使得计算机专业技能在一定程度上可以代替武力，成为控制信息化社会的力量。而掌握了很多专业技术的黑客们，自然也就能够成为在全新的信息化时代影响社会稳定的一股不可小视的力量。黑客们以个人或组织的形式广泛地存在于互联网中，时刻探寻着这些在信息系统中存在的安全问题，不断尝试，导致信息安全事件频发。

试读结束：需要全本请在线购买：www.ertongbook.com

辅助阅读

2011年最受关注的国外十大黑客事件

萨科奇爱丽舍宫网站被黑

一名黑客于2011年1月侵入法国总统尼古拉·萨科齐在社交网站Facebook上的账号，并在“状态更新”中模仿这位法国总统的口吻发布了一条信息：“亲爱的同胞们，考虑到我们国家目前正在经历的特殊环境，我已从内心深处决定，在2012年我的任期结束的时候，我不会再谋求连任。”超过35万Facebook粉丝阅读了这个消息。

EMC安全部门RSA系统遭受黑客攻击

2011年3月，EMC公司旗下著名的安全与解码技术企业RSA遭黑客攻击，使用的是一种业内称为高持续性威胁（Advanced Persistent Threat）的复杂网络攻击。这是一种“极其复杂”的攻击，会导致一些秘密信息从RSA的SecurID双因素认证（Two-factor Authentication）产品中被窃取。而Secure ID令牌是RSA公司的一次性密钥认证产品，广泛应用于一些大军事机构、政府、各种银行及医疗和医保设备。

Sony PlayStation账号被黑客破解

2011年4月的“索尼被黑”事件导致黑客从索尼在线PlayStation网络中窃取了7700万客户的信息，包括PlayStation Network/Qriocity的用户名和密码，handle/PSN online用户名，账号安全问题答案。这一黑客攻击事件导致索尼公司被迫关闭了Playstation Network服务，并损失了1.7亿美元。其后5月2日索尼公司另一个网络游戏服务也遭到攻击，导致2500万用户信息泄露。

Sega Pass用户资料信息被黑客非法侵入

游戏开发商世嘉公司欧洲分公司旗下一个网站Sega Pass于2011年6月被入侵，网站用户以欧美为主，130万名客户的个人资料被盗，外泄资料包括会员姓名、生日、电邮地址和密码。

花旗银行客户账户遭黑客攻击

美国花旗银行于2011年6月证实，该银行系统日前被黑客侵入，21万北美地区银行卡用户的姓名、账户、电子邮箱等信息可能被泄露。花旗银行的一位发言人称被盗取的信息包括用户的姓名、账号及电子邮箱地址等联系方式，约1%的信用卡持有者受到入侵事件的影响。专家们称此为对美国大型金融机构最大的一次直接攻击，并表示这次事件或将促成银行业数据安全体系的彻底大修。

黑客组织连环袭击

2011年6月，黑客组织LulzSec发起了名为“Titanic Takeover Tuesday”的攻击行动，对多家网站发动了DDoS攻击。游戏杂志The Escapist网站、IT安全公司Finfisher以及网游《EVE Online》、《英雄联盟》、《Minecraft》等多家的登录服务器遭其“毒手”。LulzSec还在Twitter中留下了黑客攻击请求热线，并表示：“现在开始接收真正Lulz粉丝的电话，让我们一起嘲笑那些被羞辱的玩家。614-LULZSEC，

我们会尽全力接收您的呼叫，一起来吧。”几个小时后，LulzSec 声称他们收到了 5000 个未接电话、2500 封语音邮件。由于游戏服务器的暂停导致不计其数的玩家暴怒，联合起来阻止 LulzSec 的非法行为。

福克斯推特账号被盗

2011 年 7 月，美国新闻网站“福克斯新闻”（Fox News）的 Twitter 账户遭到黑客劫持并用于发布虚假新闻，其中包括美国总统奥巴马遇刺身亡的消息。黑客更改了福克斯新闻账户密码，令其数小时内无法修正错误消息。尽管 Twitter 账户被黑并不鲜见，但这条虚假信息却在全球引发了轩然大波。具悉，这些黑客属于一个名为“脚本小子”（Script Kiddies）的黑客组织。

Lady Gaga

2011 年 7 月，Swagsec 黑客小组透露他们已经黑进美国流行音乐天后 Lady Gaga 的英国网站，环球音乐在一份声明中确认了该消息，黑客获得了成千上万歌迷的详细信息，包含姓名、E-Mail 地址。其 Twitter 账户又于 2012 年 12 月被黑客入侵，黑客先是通过 Lady Gaga 账户发布免费赠送 iPad 2 的推文，并附上了恶意链接，随后又发布了赠送 Macbook 的信息。虽然帖子和钓鱼网站已被删除，但根据 BBC 网络统计数据表明，此前有超过 10 万的 Lady Gaga 粉丝通过点击该网站提交了个人信息。

Yingluck Shinawatra

继福克斯新闻网的微博账号被盗并发布奥巴马“死讯”后，泰国新任女总理英拉·西瓦那成为黑客的又一元首级别受害者，其英文 twitter 账号于 2012 年 10 月 1 日晨被盗，黑客甚至在上面发布了 8 条指责她的消息。第一条微博一上来就质疑英拉的执政能力：“如果她连自己的推特账号都保不住，如何能保卫国家？想想吧。”

Facebook

社交巨头 Facebook 在 2011 年 11 月遭到黑客攻击，数百万 Facebook 用户的 Newsfeed（信息流）页面出现了色情和暴力图片、网络链接以及视频，其中包括部分伪造的名人不雅照和虐待动物等极端暴力行为，此次遭到攻击是由于黑客利用了浏览器的漏洞。

从以上黑客攻击事件中就可以看出，目前整个互联网网络还是面临着巨大的黑客攻击威胁，而且由其而产生的危害也越来越严重，受害面也越来越广。如何对这些黑客攻击进行发现和防范呢？其实在 20 世纪计算机产生之后，没有互联网的时代，人们就已经开始进行研究和防范了。可以说，黑客们对计算机系统进行攻击手段的不断提高，推动了信息安全防范技术的飞速发展。

本书中所提到的黑客包括 Hacker、Cracker 及误操作人员。Hacker 是指那些反传统精神的程序员，他们遵守黑客行为准则，不进行恶意破坏。而 Cracker 则是指那些具有不良企图、强行闯入他人系统或以某种恶意目的干扰他人系统，运用自己的知识去做出有损他人权益事情的人。他们是互联网中真正的入侵者和破坏者。当然，无论是 Hacker 还是 Cracker 都具有高超的计算机专业技术。误操作者虽然可能没有

任何高深的计算机专业知识，但是不管其主观意愿如何，其行为也可能产生入侵和异常行为。因此，从计算机技术的角度看来，无意识的误操作人员也可以归为本文中黑客中的一员。

1.1.2　黑客防范技术应运而生

1. 黑客常用手段

“知己知彼，百战不殆”，了解黑客常用手段是安全技术防范最先入手的方法。常见黑客手段见表 1-1。

表 1-1　常见黑客手段

黑客攻击手段	
信息收集型攻击	简单信息收集
	信息扫描
	信息嗅探
欺骗型攻击	IP 欺骗
	Web 欺骗
	邮件欺骗
漏洞与缺陷型攻击	缓冲区溢出
	拒绝服务攻击
	分布式拒绝服务攻击
利用型攻击	猜口令
	木马攻击
病毒型攻击	

（1）信息收集型攻击：信息收集就是对目标主机及其相关设施、软硬件情况进行非公开的了解，用于攻击前对目标安全状况的掌握。

① 简单信息收集：可以在主机上或网络中通过一些命令对目标主机进行信息查询。

② 信息扫描：在主机上或网络中对目标主机开放端口、用户列表、服务漏洞等情况进行扫描。

③ 信息嗅探：对主机上或者网络中的数据信息进行监听，以获得主机系统用户敏感信息。

（2）欺骗型攻击：通常利用实体之间的信任关系，骗取目标系统信任，使之将敏感信息发向攻击者的一种攻击方式。

① IP 欺骗：使用其他主机的 IP 地址来获得信息或者得到特权。

② Web 欺骗：通过主机间的信任关系，以 Web 形式实施的一种欺骗行为。

③ 邮件欺骗：冒充合法 E-mail 地址进行欺骗。

欺骗型攻击中还有一种主要手段称为社会工程学攻击，是指利用人性的弱点、社会心理学等知识来获取目标系统敏感信息的行为。当攻击者无法通过物理入侵直接取得所需要的资料时，就会通过计策或欺骗等手段间接获得密码等敏感信息。他们通常以交谈、欺骗、假冒或口语等方式，使用电话、电子邮件等形式从合法用户中套取用户秘密信息，再利用这些资料获取主机权限以达到其攻击的目的。本节黑客常用手段中所说的欺骗技术属于技术类社会工程学攻击，通过人力因素进行攻击的非技术类欺骗则不在本书讨论的范围之内。

（3）漏洞与缺陷型攻击：通常是利用系统漏洞或缺陷进行的攻击。

① 缓冲区溢出：通过有意安装的程序或者通过网络攻击造成目标主机程序产生缓冲区溢出的错误，目的是使目标主机死机或者获得主机系统的特权。

② 拒绝服务攻击（DOS）：通过非法占用目标大量资源，导致系统服务能力下降，甚至产生死机等的一种攻击。

③ 分布式拒绝服务攻击（DDOS）：这是 DOS 的一种大规模应用，攻击者通常控制多个分布式的僵尸主机（也有称“肉鸡”），对某一个目标发动拒绝服务攻击。

（4）利用型攻击：是指试图直接对主机进行控制的攻击。

① 猜口令：通过分析或暴力攻击等手段获取合法账户的口令。

② 木马攻击：通过植入木马对主机进行控制。

（5）病毒型攻击：使用计算机病毒对主机进行感染，从而造成系统损坏、数据丢失、拒绝服务、信息泄漏等现象的攻击。

2. 信息安全防范技术

针对黑客常用手段，信息安全防范技术也不断发展和提高。当然完善的信息安全防范体系包括：关注于主机、网络、应用等信息数据安全的属于技术层面的防范技术，以及贯穿整个信息系统生命周期的安全策略、安全评估和安全管理的、属于非技术层面的防范管理技术。本书主要关注技术层面对黑客攻击的安全防范技术。下面介绍最常用的安全防范技术。

1）入侵检测技术

入侵检测技术可以称为动态保护技术。这个动态表现为：入侵检测技术可以使用协议分析或内容分析等方法，针对具体内容进行深度审计。并且在使用入侵检测算法分析违反安全策略的入侵行为的同时，还可以分析未到入侵阶段的异常行为或潜在的入侵行为。因此，可以进行全新的动态挖掘入侵行为。由于入侵检测技术的这种强大的信息获取能力以及专业的入侵分析功能，所以入侵检测技术可以主动发现和防范较多的黑客入侵行为。特别是针对网络上的扫描/攻击和主机上的木马攻击

等非正常情况的防范。

2）访问控制技术

访问控制是指按用户身份及其所归属的某项定义组来限制用户对某些信息项的访问，或限制对某些控制功能的使用。访问控制通常应用于系统管理员控制用户对服务器、目录、文件等网络资源的访问，主要实现防止非法的主体进入受保护的网络资源、允许合法用户访问受保护的网络资源、防止合法用户对受保护的网络资源进行非授权的访问等功能。

访问控制是实现安全防范的最基本也是最有效的安全技术。通过访问控制，可以实现信息的初级过滤和控制。网络访问控制技术可以对网络中的数据容量、访问连接等进行控制；信息系统访问控制技术可以对主机、信息系统中的程序运行、数据访问等进行控制。之所以说访问控制技术是最有效的安全技术，是因为如果结合对攻击行为的准确分析能力，访问控制技术可以对几乎所有攻击进行控制。例如，通过对网络服务/地址的控制，或者对主机程序访问权限的控制等方式，防范黑客的信息收集型攻击；通过对虚假地址的控制等方式，防范黑客的欺骗型攻击；通过网段保护/服务端口控制，或者对主机程序访问权限的控制等方式，防范黑客的漏洞与缺陷攻击型攻击；通过登录用户网络地址或者服务端口控制，防范黑客的利用型攻击。网络型访问控制技术实现的典型产品就是不同层次的防火墙产品；主机型访问控制技术实现的典型产品就是操作系统安全加固产品。

3）漏洞扫描技术

漏洞扫描是指基于漏洞数据库，通过扫描等手段对指定的远程或者本地计算机系统的安全脆弱性进行检测，发现可利用的漏洞的一种安全检测（渗透攻击）行为。漏洞扫描技术可以通过对网络和主机设备进行安全状态测评，对有可能引起网络和主机整体安全漏洞的系统本身缺陷、配置不当或者其他恶意程序/服务进行分析和探测。漏洞扫描技术是一把双刃剑，它既是黑客攻击中信息收集型攻击的组成技术，也是安全管理员对整个信息系统进行安全评估的最重要技术。漏洞扫描技术能够模拟黑客寻找可能成功的攻击手段，安全管理员可以使用这种技术定时、定期检查和调整信息系统的安全状态，防止重要信息泄露以及安全漏洞的产生。不像其他安全防范技术直接参与安全防范，漏洞扫描技术主要辅助安全管理员，提供了间接安全防范能力，它和防火墙、入侵检测系统互相配合，能够有效避免黑客攻击行为，提高网络的安全性。

4）身份鉴别技术

身份鉴别技术是对访问者身份和权限进行鉴定和识别。作为防护网络资产的第一道关口，身份鉴别有着举足轻重的作用。其作用是阻止非法用户的不良访问。一般通过三种方式验证主体身份：一是主体了解的秘密，如用户名、口令、密钥；二是主体携带的物品，如磁卡、IC卡、动态口令卡和令牌卡等；三是主体特征或能力，如指纹、声音、虹膜、签名等。一般前两种方式运用较多。通过提高使用者的安全

意识，使用身份鉴别技术将大大降低黑客进行欺骗型攻击的成功率。另外，通过增加身份鉴别安全保护机制，能够防止口令暴力猜测等针对利用型的黑客攻击手段。

5）加密技术

加密技术是对信息进行保护的一种可靠方法，使用加密算法对原始数据内容变化和隐藏的一种技术。对敏感数据在不安全链路上传输时进行保护，防止信息泄露以及被嗅探。根据加密技术在 TCP/IP 协议栈的作用层次，可以将其分为链路层加密、网络层加密及应用层加密。最著名技术实现产品就是 SSL 安全套件及虚拟专用网（Virtual Private Network）产品。

6）防病毒技术

防病毒技术就是通过病毒样本比对、行为特征分析等方法，对病毒程序、病毒攻击流进行识别的技术。主机防病毒技术部署实现时，将对主机自身或应用系统进行病毒预警和杀除。网络部署时有两种方法实现：一种是网络分布式部署的主机防病毒技术，在强调主机防病毒系统自身的查毒、杀毒功能的同时，还强调对分布在整个网络中各个主机防病毒系统的集中管理、监控、审计、升级等能力；另一种是网络部署方式的病毒网关防范技术，通过对网络数据流中的病毒识别，可以结合访问控制技术，提供病毒的预警、连接限制等控制。这两种方法都能够防范黑客的病毒型攻击。

7）冗余技术

冗余技术是解决信息系统单点故障的重要措施。对关键性的网络线路、信息系统节点设备通常采用双热或多热备份的方式。信息系统运行时对运营状态实时监控并自动调整，当网络的网段或信息系统重要节点发生故障或安全状态发生突变时能在有效时间内进行切换分配，保证信息系统正常的运行。冗余技术能够减缓一定的漏洞与缺陷攻击影响，特别是信息系统应用单点故障造成的拒绝服务问题。

从以上分析，不难得到各种信息安全防范技术防范黑客攻击手段的对应情况（详见表 1-2 所示）。可以看出，入侵检测系统是防范黑客入侵最有效的产品之一。

表 1-2 信息安全防范技术防范黑客攻击手段的对应情况表

黑客攻击手段		信息安全防范技术						
		入侵检测技术	访问控制技术	漏洞扫描技术	身份鉴别技术	加密技术	防病毒技术	冗余技术
信息收集型攻击	简单信息收集	√		√				
	信息扫描	√	√	√				
	信息嗅探					√		
欺骗型攻击	IP 欺骗	√			√			
	Web 欺骗	√			√			
	邮件欺骗				√			

试读结束：需要全本请在线购买： www.ertongbook.com