配套实践插图
学习资源丰富

郭帆◎编著

网络攻防

技术与实战

深入理解信息安全防护体系

清華大學出版社

网络攻防
技术与实战

深入理解信息安全防护体系

郭帆◎编著

清華大學出版社
北京

内 容 简 介

本书围绕网络安全所涉及的网络安全体系结构、网络攻击技术、网络防御技术、密码技术基础和网络安全应用等方面展开，系统介绍了网络安全攻防技术的基础理论、技术原理、实现方法和实际工具应用。由于网络安全技术具有较强的工程实践性，本书极其重视理论和实践相结合，针对每种理论和技术，都给出相应的工具使用方法并配以实践插图，将抽象的理论和枯燥的文字转化为直观的实践过程和攻防效果，有助于读者理解相应技术原理。

全书共13章，内容包括信息收集、网络隐身、网络扫描、网络攻击、后门设置和痕迹清除等攻击技术，防火墙、入侵防御、恶意代码防范、操作系统安全和计算机取证等防御技术，对称加密、公钥加密、认证技术和数字签名等密码学基础理论，以及用于增强TCP/IP协议安全性的安全协议，如802.1X、EAP、IPSec、SSL、802.11i、SET、VPN、S/MIME和PGP等，最后一章详细介绍了Web程序的攻防原理。

本书层次分明，概念清晰，实践性极强，易于学习和理解，可以作为网络安全管理人员和开发人员的技术参考书或工具书，也可以作为高等院校信息安全、计算机科学与技术、网络工程、通信工程等专业的教材。

图书在版编目(CIP)数据

网络攻防技术与实战：深入理解信息安全防护体系/郭帆编著. —北京：清华大学出版社，2018(2018.10重印)
ISBN 978-7-302-50127-5

Ⅰ. ①网…　Ⅱ. ①郭…　Ⅲ. ①计算机网络－网络安全　Ⅳ. ①TP393.08

中国版本图书馆CIP数据核字(2018)第106239号

责任编辑：曾　珊
封面设计：李召霞
责任校对：李建庄
责任印制：宋　林

出版发行：清华大学出版社
网　　址：http://www.tup.com.cn，http://www.wqbook.com
地　　址：北京清华大学学研大厦A座　　邮　　编：100084
社 总 机：010-62770175　　邮　　购：010-62786544
投稿与读者服务：010-62776969，c-service@tup.tsinghua.edu.cn
质量反馈：010-62772015，zhiliang@tup.tsinghua.edu.cn
课件下载：http://www.tup.com.cn，010-62795954
印 装 者：三河市少明印务有限公司
经　　销：全国新华书店
开　　本：185mm×260mm　　印　　张：26.5　　字　　数：614千字
版　　次：2018年10月第1版　　印　　次：2018年10月第2次印刷
定　　价：79.00元

产品编号：077521-01

前言

随着计算机网络的迅速发展，电子商务和网络支付等关键业务剧增，对网络安全的需求不断提高，与此同时，互联网中的网络攻击事件持续不断，网络安全面临的威胁变化多样。因此，网络安全已经成为人们普遍关注的问题，网络安全技术也成为信息技术领域的重要研究方向。

当前有关计算机网络安全的图书各有特色，总体上可以分为三类。第一类着重讨论加/解密技术和安全协议等网络安全基础理论，特别是深入讨论各种具体算法和协议机制，但是没有与主流的网络安全工具和实际的网络攻防实践相结合，使得图书较为抽象和生涩难懂，读者很难学以致用。第二类专注于探讨网络攻击手段和对应的网络防御技巧，不对这些手段和技巧背后的技术原理做详细解释，同时也不对网络安全理论和技术做详细介绍，使得图书内容过于浅显，读者无法深入理解网络攻防过程中出现的各种现象的产生原因，也无法解决在实际工程实践中出现的各种问题。第三类则把各种安全机制放在一起讨论，类似于大杂烩，但是所有内容却都是浅尝辄止。上述三类图书的共同问题在于一是没有对当前主流的网络攻防技术进行深入探讨，二是空泛地介绍基本概念和方法，没有与具体的网络、系统和安全问题相结合，因此使得读者很难提高实际解决网络安全问题的能力。

本书以将读者领进计算机网络安全技术的大门为目标。首先，系统地介绍网络攻击的完整过程，将网络攻击各个阶段的理论知识和技术基础与实际的攻击过程有机结合，使读者能够深入理解网络攻击工具的实现机制。其次，详细地介绍各种网络防御技术的基本原理，主要包括防火墙、入侵防御系统、恶意代码防范、系统安全和计算机取证等，同时结合当前主流开源防御工具的实现方法和部署方式，以图文并茂的形式加深读者对网络防御技术原理和实现机制的理解。最后，全面地介绍网络安全的基础理论，包括加/解密技术、加/解密算法、认证技术、网络安全协议等，将基础理论和主流工具的应用实践紧密结合，有利于读者理解抽象的理论知识及各种主流工具背后的实现机制。

全书共13章。第1章概述，全面介绍网络安全的目标、威胁和研究内容；第2章信息收集，详细讨论各种信息收集技术的原理和使用方式；第3章网络隐身，综合介绍IP地址欺骗和MAC欺骗、代理隐藏和NAT技术等隐藏主机的原理及主流工具的使用方法；第4章网络扫描，详细阐述端口扫描、服务和系统扫描、漏洞扫描、配置扫描、弱口令扫描等扫描技术的基本原

理，同时结合开源工具的实际扫描过程和扫描结果进行验证；第5章网络攻击，结合主流攻击工具的使用方法，详细说明各类网络攻击的技术原理，包括弱口令攻击、中间人攻击、恶意代码攻击、漏洞破解和拒绝服务攻击等；第6章网络后门与痕迹清除，结合实际工具和目标环境详细介绍如何设置各种系统后门，针对Windows和Linux系统环境，分别介绍不同的痕迹清除方法；第7章访问控制与防火墙，详细讨论各类访问控制方法以及包过滤防火墙、代理防火墙、有状态防火墙等技术的基本原理，结合Cisco ACL、Linux iptables、Windows个人防火墙和CCProxy等主流工具的配置方法和应用实践，分析它们的实现机制和相应的技术原理；第8章入侵防御，在详细说明基于主机的IPS和基于网络的IPS的工作流程及基本原理的基础上，分别结合开源软件OSSEC和Snort的配置方式和应用实践，进一步讨论有关技术原理；第9章密码技术基础，全面讨论密码学体制、加/解密算法、认证技术和PKI架构等理论知识，结合加/解密工具GnuPG的应用实践说明加/解密技术的使用方式；第10章网络安全协议，详细介绍链路层安全协议802.1X和EAP、网络层安全协议IPSec、传输层安全协议SSL和无线安全协议802.11i的实现机制，结合在Windows系统中应用IPSec协议的实践，进一步说明IPSec协议的原理，结合使用无线破解工具aircrack-ng破解WPA/PSK口令的应用实践，进一步说明802.11i协议的密钥交换机制；第11章网络安全应用，详细说明常见的应用层安全协议的实现机制，包括VPN、电子邮件安全协议PGP和S/MIME、安全电子交易协议SET，结合Cisco路由器的IPSec VPN应用实践说明IP隧道的实现原理，结合详细的加/解密流程图说明SET协议的工作过程；第12章恶意代码防范与系统安全，首先详细讨论病毒、木马和蠕虫的防范方法，并结合Windows自带工具说明常用的木马防御手段，然后展开讨论Windows和Linux操作系统的安全机制及有关安全配置方法，最后详细说明计算机取证的定义、步骤和技术原理，结合主流取证工具的配置方式和使用方法说明计算机取证的作用；第13章Web程序安全，首先详细介绍Web程序安全的核心安全问题和防御机制，以及与安全有关的HTTP内容和数据编码，然后结合DVWA项目着重讨论验证机制、会话管理、SQL注入和XSS漏洞等常见安全威胁的产生原因、攻击方法和防御技术。

作为一本理论和实践紧密结合的图书，正如网络的设计和部署可能存在漏洞一样，限于作者的水平，本书难免存在各种错误和不足。作者殷切希望读者批评指正，也希望读者能够就图书内容和叙述方式提出意见和建议。作者E-mail地址为：121171528@qq.com。

作　者

2018年7月

学习建议

本书面向网络信息安全领域的科技人员，同时也可作为高等院校计算机、电子信息、通信工程类专业的教材。作为教材时，对应的课程类别属于网络与信息安全类。参考学时为96学时，包括理论教学环节64课时和实验教学环节32课时。

理论教学环节主要包括课堂讲授和演示教学。理论教学以课堂讲授为主，部分内容可以通过学生自学加以理解和掌握。演示教学针对课程内容中涉及的各种攻防工具的技术原理和实施效果进行演示、分析和探讨，要求学生根据教师的课堂演示和讨论结果在课后进行实验，重复课堂的演示过程，并就实验过程中出现的各种问题进行课内讨论讲评。

实验教学环节涉及的系统环境包括Kali Linux、Ubuntu Linux、Windows 7、VmWare等，涉及的攻防工具众多，但是都在课程内容中有相关描述，教学时可以灵活安排，在每一类工具中选择其中一两个完成即可。由于实验内容较多，有些实验有较大难度，部分学生可能无法按时在实验课时内完成，此时可以允许学生课后继续自学完成，老师进一步提供在线支持和问题答疑。

因为本门课程的工程实践性非常强，实验老师应该确保每位同学独立地完成每一次的攻防工具实验，并且在实验课堂上负责点评和检查，帮助同学们逐一过关。为了防止学生作弊、抄袭和复制，应该采用问答式检查方式，在学生进行演示时提出相应问题，根据学生的回答情况判定其是否独立完成实验。

本课程的主要知识点、重点、难点及课时分配见下表。

各章序号	知识单元(章节)	知 识 点	要求	推荐学时
1	概述	网络安全的定义	掌握	4
		面临的安全威胁	掌握	
		网络安全体系结构	了解	
		网络攻击和防御技术	掌握	
		密码技术应用	理解	
		网络安全应用	了解	

续表

各章序号	知识单元(章节)	知　识　点	要求	推荐学时
2	信息收集	Whois 查询	掌握	4
		域名和 IP 信息收集方法	掌握	
		Web 挖掘分析方法	掌握	
		社会工程学实施信息收集	理解	
		拓扑确定方法	掌握	
		网络监听原理	掌握	
3	网络隐身	IP 地址欺骗原理	理解	3
		MAC 地址欺骗原理和方法	掌握	
		网络地址转换原理	掌握	
		代理隐藏方法	掌握	
4	网络扫描	端口扫描原理和方法	掌握	6
		服务扫描原理	理解	
		操作系统扫描原理和方法	掌握	
		漏洞扫描原理和方法	掌握	
		弱口令扫描方法	掌握	
		Web 漏洞扫描原理	了解	
		系统配置扫描原理	了解	
5	网络攻击	口令破解的方法和工具使用	掌握	10
		中间人攻击的原理和方法	掌握	
		恶意代码的生存和隐蔽技术	掌握	
		漏洞破解原理和利用方法	掌握	
		DoS/DDoS 原理和工具实施	掌握	
6	网络后门与痕迹清除	开放连接端口和修改系统配置方法	掌握	3
		系统文件替换方法	掌握	
		安装监控器和建立隐蔽连接	了解	
		创建用户账户	掌握	
		各种后门工具的使用方法	掌握	
		Windows 痕迹清除	掌握	
		Linux 痕迹清除	理解	
7	访问控制与防火墙	访问控制方法	理解	6
		包过滤防火墙技术原理	掌握	
		代理防火墙技术原理	了解	
		防火墙体系结构	理解	
		防火墙的优缺点	了解	
		Windows 个人防火墙原理和设置方法	掌握	
		Linux iptables 原理和设置方法	掌握	
		Cisco ACL 原理和设置方法	掌握	
		CCProxy 代理防火墙原理和设置方法	掌握	

续表

各章序号	知识单元(章节)	知 识 点	要求	推荐学时
8	入侵防御	IPS 工作过程和分类	了解	4
		IPS 分析方法	掌握	
		IPS 部署和评估	理解	
		HIPS 基本原理和工作流程	掌握	
		HIPS 实例——OSSEC 使用方法	掌握	
		NIPS 实例——Snort 使用方法	掌握	
9	密码技术基础	密码编码学和密码分析学概念	了解	6
		对称加密原理与 DES 算法	掌握	
		公钥加密原理与 RSA 算法	掌握	
		散列函数和 SAH-512 算法	掌握	
		密钥分配原理	理解	
		消息认证码和 HMAC	理解	
		数字签名原理	掌握	
		身份认证	理解	
		PKI 基本架构	了解	
		GnuPG 的使用方法	掌握	
10	网络安全协议	802.1X 和 EAP	了解	4
		IPSec AH、ESP 协议	掌握	
		IPSec IKE 协议	理解	
		SSL 记录和握手协议	掌握	
		SSL 的安全性	理解	
		TKIP 和 CCMP 加密机制	掌握	
		802.11i 建立安全关联	理解	
		WPA/PSK 无线破解原理和方法	掌握	
11	网络安全应用	IP 隧道原理	理解	3
		强制隧道远程接入原理	理解	
		自愿隧道远程接入原理	理解	
		虚拟专用局域网原理	理解	
		IP 隧道 Cisco 配置	掌握	
		PGP 实现原理	了解	
		S/MIME 实现原理	了解	
		SET 的工作过程	理解	
12	恶意代码防范与系统安全	病毒原理和防范方法	理解	4
		木马原理和防范方法	理解	
		蠕虫原理和防范方法	理解	
		恶意代码的区别	了解	
		Windows 7 安全机制	掌握	
		Windows 7 常用安全配置	掌握	
		Linux 安全机制	理解	
		Linux 通用安全配置	掌握	
		计算机取证的原则和方法步骤	了解	
		各类取证工具的作用和使用方法	掌握	

续表

各章序号	知识单元(章节)	知　识　点	要求	推荐学时
13	Web 程序安全	核心问题和防御机制	理解	5
		HTTP 内容和编码方式	掌握	
		验证机制的安全性	掌握	
		会话管理的安全性	掌握	
		存储区域的安全性	掌握	
		Web 用户的安全性	掌握	

目录

第 1 章

概　述

学习要求：

- 掌握网络安全的定义以及网络面临的各种安全威胁。
- 了解网络安全体系结构中各个层次的安全定义和作用。
- 掌握各种网络攻击技术的定义和作用。
- 掌握各种网络防御技术的定义和作用。
- 理解不同密码体制、不同数据加/解密技术及不同认证技术的定义和作用。
- 了解 PKI 的定义和作用。
- 了解 802.1X、IPSec、SSL、VPN、802.1i 和 SET 协议的作用。

随着计算机网络的迅速发展和应用，网络在给人们的工作和生活带来便利的同时，也带来了巨大的安全隐患。如今，网络攻击事件屡见不鲜，给国家和社会带来巨大的经济利益损失，有时甚至危害国家安全。网络安全主要研究计算机网络的安全理论、安全应用和安全管理，使得网络能抵御各种安全威胁和网络攻击，保持正常工作。

网络安全属于信息安全的一个分支。信息安全要求信息在采集、存储、处理和传输过程中不会被破坏、窃取和修改，由计算机安全和网络安全保障。其中，计算机安全负责信息存储和处理过程的安全；网络安全负责信息传输过程的安全。网络安全不仅保证信息安全传输，还必须区分网络病毒和正常信息、区分正常和非法访问、区分授权和非授权用户。

信息安全发展的四个阶段分别是通信安全阶段、计算机系统信息安全阶段、网络系统安全阶段和物联网安全阶段。通信安全阶段的主要任务是解决数据传输的安全问题，解决方案主要是密码技术，此时信息安全技术还处于原始阶段；计算机系统信息安全阶段的主要任务是解决计算机系统中信息存储和运行的安全问题，解决方案主要是根据访问者和信息的安全级别，实施访问者对信息的访问控制；网络系统安全阶段的主要任务是解决网络中信息存储和传输的安全问题，主要措施是提供完整信息安全解决方案，包括防御、检测、响应和恢复；信息安全的未来发展是物联网的安全保障，目前信息安全发展还处于网络系统安全阶段。

网络系统安全阶段要解决的问题是：当通过网络把分布在不同地理位置的计算机连接起来后，如何保护在网络中各台计算机存储的大量数据以及在不同计算机之间传输的数据。