

<<网络信息对抗>>

图书基本信息

书名：<<网络信息对抗>>

13位ISBN编号：9787563525027

10位ISBN编号：7563525025

出版时间：2011-1

出版时间：北京邮电大学出版社

作者：杜晔，梁颖 编

页数：230

版权说明：本站所提供下载的PDF图书仅提供预览和简介，请支持正版图书。

更多资源请访问：<http://www.tushu007.com>

<<网络信息对抗>>

内容概要

本书详细地介绍了信息对抗基本概念、原理与方法，详尽、具体地披露了攻击技术的真相，以及防范策略和技术实现措施。

全书共分3个部分，内容由浅入深，分技术专题进行讨论。

第1部分介绍了网络信息对抗的基础知识、计算机及网络系统面临的威胁与黑客攻击方法、网络信息对抗的基础知识及典型的安全评估标准和模型。

第2部分是本书的核心内容，介绍了有代表性的网络攻击技术，包括网络扫描、嗅探、欺骗、缓冲区溢出、拒绝服务攻击、恶意代码等手段的原理与实现技术。

第3部分根据网络边界防护的要求着重讨论了防御手段，详细介绍了身份认证技术、访问控制技术和两种得到广泛应用的安全设备，即防火墙和入侵检测系统。

本书既可作为信息安全、信息对抗、计算机、通信等专业本科生、硕士研究生的教科书，也适合于网络管理人员、安全维护人员和相关技术人员参考和阅读。

书籍目录

第1部分 网络信息对抗基础	第1章 绪论	1.1 网络信息安全现状	1.2 网络信息对抗概述	1.2.1 网络信息对抗概念	1.2.2 网络信息对抗的基本原理	1.2.3 网络信息对抗的特点	1.3 网络信息对抗的层次	1.4 网络信息对抗的内涵	1.4.1 信息进攻	1.4.2 信息防御				
	第2章 网络信息对抗基础知识	2.1 计算机网络的体系结构	2.1.1 osi参考模型	2.1.2 tcp / ip参考模型	2.1.3 osi参考模型与tcp / ip参考模型比较	2.2 osi安全体系结构	2.2.1 安全服务	2.2.2 安全服务提供的安全机制	2.2.3 安全服务和特定安全机制的关系	2.2.4 osi安全管理				
	第3章 安全评估标准	3.1 安全评估国际标准的历程	3.2 tcsec标准	3.3 itsec标准	3.4 cc标准	3.5 我国测评标准的发展现状	第4章 安全模型	4.1 多级安全模型	4.2 多边安全模型	4.3 p2dr模型				
	第2部分 攻击技术	第3章 欺骗技术	3.1 ip欺骗	3.2 电子邮件欺骗	3.3 arp欺骗	3.4 dns欺骗	3.5 tcp会话劫持	第4章 嗅探技术	4.1 嗅探器简介	4.2 嗅探器工作原理				
								4.3 嗅探器的实现	4.4 嗅探器的检测与防范	第5章 扫描技术				
										5.1 端口扫描	5.2 漏洞扫描	5.3 扫描防范	5.4 常用扫描工具	
										第6章 拒绝服务攻击	6.1 拒绝服务攻击概述	6.2 分布式拒绝服务攻击概述	6.3 拒绝服务攻击防御	
											6.4 常用拒绝服务攻击工具	第7章 缓冲区溢出攻击	7.1 缓冲区溢出攻击概述	
												7.2 缓冲区溢出攻击原理	7.3 缓冲区溢出攻击分类	
												7.4 缓冲区溢出攻击防御	第8章 恶意代码	
													8.1 恶意代码概述	
													8.2 病毒	
													8.2.1 病毒的定义	
													8.2.2 病毒的分类	
													8.2.3 病毒的发展历史	
													8.2.4 病毒的结构	
													8.2.5 病毒的防治技术	
													8.3 蠕虫	
													8.3.1 蠕虫概述	
													8.3.2 蠕虫的传播过程	
													8.3.3 典型蠕虫分析	
													8.3.4 蠕虫的防御	
													8.4 木马	
													8.4.1 木马概述	
													8.4.2 木马的分类	
													8.4.3 木马的攻击过程	
													8.4.4 典型木马分析	
													8.4.5 木马的防御	
													8.5 病毒、蠕虫、木马的区别	
	第3部分 防护技术	第9章 身份认证技术	9.1 身份认证技术概述	9.2 基于口令的身份认证	9.2.1 简单口令认证	9.2.2 一次性口令	9.2.3 双因素认证	9.2.4 radius协议	9.3 kerberos认证技术	9.3.1 kerberos简介	9.3.2 kerberos v4协议	9.3.3 kerberos v5协议	9.4 基于pki身份认证	9.4.1 pki简介
													9.4.2 pki体系结构	
													9.4.3 pkix主要功能	
													9.4.4 x.509证书	
													第10章 访问控制技术	
													10.1 访问控制概念	
													10.1.1 策略与机制	
													10.1.2 访问控制矩阵	
													10.1.3 安全策略	
													10.1.4 访问控制的类型	
													10.2 访问控制技术	
													10.3 访问控制模型	
													10.3.1 自主访问控制模型	
													10.3.2 强制访问控制模型	
													10.3.3 基于角色访问控制模型	
													10.4 访问控制的实现	
													10.4.1 访问控制列表	
													10.4.2 能力表	
													10.4.3 锁与钥匙	
													10.4.4 保护环	
													第11章 防火墙	
													11.1 防火墙概述	
													11.2 防火墙分类	
													11.3 防火墙关键技术	
													11.3.1 包过滤技术	
													11.3.2 代理技术	
													11.3.3 网络地址转换	
													11.4 防火墙体系结构	
													11.4.1 双重宿主主机结构	
													11.4.2 屏蔽主机结构	
													11.4.3 屏蔽子网结构	
													11.5 防火墙技术的发展趋势	
													11.6 典型防火墙配置工具iptables及实验	
													11.6.1 netfilter / iptables介绍	
													11.6.2 iptables命令	
													11.6.3 iptables实验	
													第12章 入侵检测	
													12.1 入侵检测概述	
													12.2 入侵检测的发展史	
													12.3 入侵检测分类	
													12.4 入侵检测分析技术	
													12.4.1 误用检测技术	
													12.4.2 异常检测技术	
													12.5 入侵检测的发展趋势	
													12.6 典型入侵检测系统snort及实验	
													12.6.1 snort结构	
													12.6.2 snort工作模式	
													12.6.3 snort规则	
													12.6.4 snort安装	
													12.6.5 snort实验参考文献	

章节摘录

版权页：插图：传播模块又可以分为3个基本模块：扫描模块、攻击模块和复制模块。蠕虫程序的一般传播过程包括如下步骤。

扫描。

由蠕虫的扫描功能模块负责探测存在漏洞的主机。

当程序向某个主机发送探测漏洞的信息并收到成功的反馈信息后，就得到一个可传播的对象。

攻击。

攻击模块按漏洞攻击步骤自动攻击步骤 中找到的对象，取得该主机的权限（一般为管理员权限），获得一个shell。

复制。

复制模块通过原主机和新主机的交互，将蠕虫程序复制到新主机并启动。

这里可以看到，传播模块实现的实际上是自动入侵的功能。

所以蠕虫的传播技术是蠕虫技术的首要技术，没有蠕虫的传播技术，也就谈不上什么蠕虫技术了。

2.入侵过程的分析 用各种方法收集目标主机的信息，找到可利用的漏洞或弱点。

搜集信息，有很多种方法，包括技术的和非技术的。

采用技术的方法包括用扫描器扫描主机，探测主机的操作系统类型和版本、主机名、用户名、开放的端口、开放的服务、开放的服务器软件版本等。

非技术的方法包括和主机的管理员拉关系套口风，骗取信任，威逼利诱等各种少儿不宜的手段。

当然是信息搜集的越全越好。

搜集完信息后进入下一步。

针对目标主机的漏洞或缺陷，采取相应的技术攻击主机，直到获得主机的管理员权限。

对搜集来的信息进行分析，找到可以有效利用的信息。

如果有现成的漏洞可以利用，上网找到该漏洞的攻击方法，如果有攻击代码就直接复制下来，然后用该代码取得权限就好了；如果没有现成的漏洞可以利用，就用根据搜集的信息试探猜测用户密码，另一方面试探研究分析其使用的系统，争取分析出一个可利用的漏洞。

<<网络信息对抗>>

编辑推荐

《网络信息对抗》：北京市重点学科共建项目：计算机应用技术

版权说明

本站所提供下载的PDF图书仅提供预览和简介，请支持正版图书。

更多资源请访问:<http://www.tushu007.com>