

<<黑客分析与防范技术>>

图书基本信息

书名：<<黑客分析与防范技术>>

13位ISBN编号：9787302034605

10位ISBN编号：7302034605

出版时间：1999-5

出版时间：清华大学出版社

作者：北京启明星辰信息技术有限公司

页数：231

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>

## <<黑客分析与防范技术>>

### 内容概要

本书较全面地介绍了当前计算机黑客使用的各种技术、攻击手段、攻击行为造成的后果及其防范措施

。书中在讲述原理的同时，结合了大量的实例，并介绍了各种防范对策。而且，本书对于保护广大计算机网络用户的信息安全和系统安全有着重要的参考价值。本书面向广大的计算机网络用户，对于系统管理员和网络安全管理员尤其有用。

## &lt;&lt;黑客分析与防范技术&gt;&gt;

## 书籍目录

第一章 安全面临的威胁	1.1 安全——一个倍受关注的话题	1.2 计算机安全
1.2.1 物理安全	1.2.2 操作系统提供的安全	1.2.3 连网安全
1.2.4 其他形式的安全	1.2.5 虚假安全	1.2.4 其他形式的安全
1.3 网络面临的安全威胁	1.3.1 黑客	1.3.2 计算机病毒
1.3.3 特洛伊木马 (Trojan Horses) 程序	1.3.4 陷门 (Trap door) 和后门 (Back door)	1.3.2 计算机病毒
1.3.5 拒绝服务攻击 (Denial of Service Attack)	1.4 信息系统安全脆弱性	1.3.2 计算机病毒
1.4.1 操作系统安全的脆弱性	1.4.2 网络安全的脆弱性	1.4.3 数据库管理系统安全的脆弱性
1.4.4 缺少安全管理	1.5 本书内容	1.4.3 数据库管理系统安全的脆弱性
1.6 本章小结	第二章	1.4.3 数据库管理系统安全的脆弱性
黑客行径分析	2.1 攻击事件	2.1 进程的执行
2.2 攻击的目的	2.2.1 进程的执行	2.2.2 对系统的非法访问
获取文件的传输中的数据	2.2.3 获得超级用户权限	2.2.4 对系统的非法访问
2.2.5 进行不许可的操作	2.2.6 拒绝服务	2.2.7 涂改信息
2.2.6 拒绝服务	2.2.7 涂改信息	2.2.8 暴露信息
2.3 实施攻击的人员	2.3.1 计算机黑客	2.3.2 不满或者被解雇的雇员
2.3.1 计算机黑客	2.3.2 不满或者被解雇的雇员	2.3.3 极端危险的罪犯和工业间谍
2.4 工具	2.5 攻击的三个阶段	2.5.1 寻找目标.收集信息
2.5 攻击的三个阶段	2.5.3 攻击其他系统	2.6 攻击时间
2.5.2 获得初始的访问权与特权	2.6 攻击时间	第三章 口令安全
2.7 攻击示例一	2.8 攻击示例二	3.1 口令与安全
2.8 攻击示例二	2.9 本章小结	3.2 口令破解
3.1 口令与安全	3.2 口令破解的可能性与其他认证方式	3.2.1 口令破解
3.2 口令破解的可能性与其他认证方式	3.3 好的口令——一个紧锁的门	3.3.1 不安全口令
3.2.2 认证方式	3.3.1 不安全口令	3.3.2 保持口令的安全
3.3 好的口令——一个紧锁的门	3.3.2 保持口令的安全	3.5.1 /etc/passwd文件
3.4 一次性口令	3.5 UNIX系统的口令	3.5.1 /etc/passwd文件
3.5.2 口令时效	3.5.3 网络数据库	3.6 UNIX口令加密与破译
3.5.3 网络数据库	3.6 UNIX口令加密与破译	3.6.1 crypt()函数
3.6.2 crypt16()和其他算法	3.6.3 破译口令	3.6.1 crypt()函数
3.6.3 破译口令	3.7 本章小结	第四章 拒绝服务的攻击
3.7 本章小结	4.1 什么是拒绝服务的攻击	4.2 过载攻击
4.1 什么是拒绝服务的攻击	4.2 过载攻击	4.2.1 进程过载
4.2 过载攻击	4.2.1 进程过载	4.2.2 系统过载攻击
4.2.1 进程过载	4.2.2 系统过载攻击	4.2.3 磁盘攻击
4.2.2 系统过载攻击	4.2.3 磁盘攻击	4.2.4 树结构的攻击
4.2.3 磁盘攻击	4.2.4 树结构的攻击	4.2.5 交换空间的问题
4.2.4 树结构的攻击	4.2.5 交换空间的问题	4.2.6 /tmp目录的问题
4.2.5 交换空间的问题	4.2.6 /tmp目录的问题	4.2.7 防止拒绝服务的攻击
4.2.6 /tmp目录的问题	4.2.7 防止拒绝服务的攻击	4.3 针对网络的拒绝服务的攻击
4.2.7 防止拒绝服务的攻击	4.3 针对网络的拒绝服务的攻击	4.3.1 服务过载
4.3 针对网络的拒绝服务的攻击	4.3.1 服务过载	4.3.2 消息流
4.3.1 服务过载	4.3.2 消息流	4.3.3 信号接地
4.3.2 消息流	4.3.3 信号接地	4.4 本章小结
4.3.3 信号接地	4.4 本章小结	第五章 扫描
4.4 本章小结	5.1 扫描工具回顾	5.1.1 SATAN
5.1 扫描工具回顾	5.1.1 SATAN	5.1.2 ISS
5.1.1 SATAN	5.1.2 ISS	5.2 端口扫描
5.1.2 ISS	5.2 端口扫描	5.3 TCP FIN扫描
5.2 端口扫描	5.3 TCP FIN扫描	5.3.1 TCP connect()的扫描
5.3 TCP FIN扫描	5.3.1 TCP connect()的扫描	5.3.2 TCP SYN扫描
5.3.1 TCP connect()的扫描	5.3.2 TCP SYN扫描	5.3.3 TCP FIN扫描
5.3.2 TCP SYN扫描	5.3.3 TCP FIN扫描	5.3.4 Fragmentation扫描
5.3.3 TCP FIN扫描	5.3.4 Fragmentation扫描	5.3.5 UDP recfrom()和write()扫描
5.3.4 Fragmentation扫描	5.3.5 UDP recfrom()和write()扫描	5.3.6 ICMP的扫描
5.3.5 UDP recfrom()和write()扫描	5.3.6 ICMP的扫描	第六章 网络监听
5.3.6 ICMP的扫描	第六章 网络监听	6.1 什么是网络监听
6.1 什么是网络监听	6.1.1 监听的可能性	6.1.2 以太网中可以监听的原因
6.1.1 监听的可能性	6.1.2 以太网中可以监听的原因	6.2 网络监听的工具
6.1.2 以太网中可以监听的原因	6.2 网络监听的工具	6.2.1 截获通信的内容
6.2 网络监听的工具	6.2.1 截获通信的内容	6.2.2 对协议分析
6.2.1 截获通信的内容	6.2.2 对协议分析	6.3 常用的监听
6.2.2 对协议分析	6.3 常用的监听	6.3.1 Sniffit软件
6.3 常用的监听	6.3.1 Sniffit软件	6.3.2 NetXRay
6.3.1 Sniffit软件	6.3.2 NetXRay	6.3.3 其他网络监听软件
6.3.2 NetXRay	6.3.3 其他网络监听软件	6.4 网络监听的检测
6.3.3 其他网络监听软件	6.4 网络监听的检测	6.4.1 简单的检测方法
6.4 网络监听的检测	6.4.1 简单的检测方法	6.4.2 对付一个监听
6.4.1 简单的检测方法	6.4.2 对付一个监听	6.4.3 其他防范监听的
6.4.2 对付一个监听	6.4.3 其他防范监听的	第七章 缓冲区溢出
6.4.3 其他防范监听的	第七章 缓冲区溢出	7.1 缓冲区溢出的危害
7.1 缓冲区溢出的危害	7.2 使用缓冲区溢出程序取得特权	7.3 缓冲区溢出程序的原理及要素
7.2 使用缓冲区溢出程序取得特权	7.3 缓冲区溢出程序的原理及要素	7.4 一个缓冲区
7.3 缓冲区溢出程序的原理及要素	7.4 一个缓冲区	7.4.1 一个缓冲区溢出程序
7.4 一个缓冲区	7.4.1 一个缓冲区溢出程序	7.4.2 堆栈中执行
7.4.1 一个缓冲区溢出程序	7.4.2 堆栈中执行	7.5 缓冲区溢出的其他危害
7.4.2 堆栈中执行	7.5 缓冲区溢出的其他危害	7.6 缓冲区溢出攻击Windows
7.5 缓冲区溢出的其他危害	7.6 缓冲区溢出攻击Windows	7.6.1 几个例子
7.6 缓冲区溢出攻击Windows	7.6.1 几个例子	7.6.2 Ping o'Death攻击
7.6.1 几个例子	7.6.2 Ping o'Death攻击	7.7 关于缓冲区溢出的一些讨论
7.6.2 Ping o'Death攻击	7.7 关于缓冲区溢出的一些讨论	7.8 再论SUID
7.7 关于缓冲区溢出的一些讨论	7.8 再论SUID	7.9 本章小结
7.8 再论SUID	7.9 本章小结	第八章 程序攻击
7.9 本章小结	第八章 程序攻击	8.1 病毒
8.1 病毒	8.2 特洛伊木马程序	8.2.1 特洛伊木马
8.2 特洛伊木马程序	8.2.1 特洛伊木马	8.2.2 病毒与特洛伊木马程序的比较
8.2.1 特洛伊木马	8.2.2 病毒与特洛伊木马程序的比较	8.3 其他危险程序
8.2.2 病毒与特洛伊木马程序的比较	8.3 其他危险程序	8.4 本章小结
8.3 其他危险程序	8.4 本章小结	第九章 Web欺骗的攻击和对策
8.4 本章小结	第九章 Web欺骗的攻击和对策	9.1 Web面临的安全威胁
9.1 Web面临的安全威胁	9.2 安全相关的决策	9.3 Web攻击的行为和特点
9.2 安全相关的决策	9.3 Web攻击的行为和特点	9.4 攻击的原理和过程
9.3 Web攻击的行为和特点	9.4 攻击的原理和过程	9.4.1 改写URL
9.4 攻击的原理和过程	9.4.1 改写URL	9.4.2 开始攻击
9.4.1 改写URL	9.4.2 开始攻击	9.4.3 制造假象
9.4.2 开始攻击	9.4.3 制造假象	9.5 保护方法
9.4.3 制造假象	9.5 保护方法	9.6 Web服务器的一些安全措施
9.5 保护方法	9.6 Web服务器的一些安全措施	第十章 利用处理程序错误的攻击
9.6 Web服务器的一些安全措施	第十章 利用处理程序错误的攻击	10.1 攻击的现象及其后果
10.1 攻击的现象及其后果	10.2 IP.TCP包头简介	10.2.1 TCP包头格式
10.2 IP.TCP包头简介	10.2.1 TCP包头格式	10.2.2 IP包头格式
10.2.1 TCP包头格式	10.2.2 IP包头格式	10.3 泪滴攻击工具
10.2.2 IP包头格式	10.3 泪滴攻击工具	10.4 Land攻击工具
10.3 泪滴攻击工具	10.4 Land攻击工具	10.5 OOB攻击工具
10.4 Land攻击工具	10.5 OOB攻击工具	10.5.1 攻击代
10.5 OOB攻击工具	10.5.1 攻击代	

<<黑客分析与防范技术>>

码	10.5.2 一些临时措施	10.6 本章小结	第十一章 X Windows安全
	11.1 X Windows系统特点	11.2 X Windows系统组成结构	11.2.1 X服务器程序
	11.2.2 客户程序	11.2.3 通讯通道	11.3 X Windows系统实用工具
的控制	11.3.2 转储窗口内容	11.3.3 本地主机的问题	11.3.1 X显示
11.3.5 Xterm——保护键盘选项	11.3.6 xlock和基于X的注册程序	11.3.4 读取键盘	11.3.7 X安全工具
11.4 X系统的一个易忽略的漏洞	11.4.1 问题描述	11.4.2 使用Windows系统上的X仿真程序	11.4.2 使用Windows系统上的X仿
11.5 本章小结	第十二章 一些网络服务的安全问题	12.1 网络	12.1 网络
文件系统安全	12.1.1 网络文件系统的安全问题	12.1.2 攻击实例	12.1.3 NFS
的RPC认证	12.1.4 从服务端调出文件系统	12.1.5 showmount命令	12.1.6 不安
全的NFS对系统的危害	12.1.7 NFS服务器的攻击	12.1.8 安全措施	12.1.9 安
全NFS	12.2 网络信息系统 (NIS)	12.2.1 NIS与分布环境的管理	12.2.2 NIS如
何解决分布环境问题	12.2.3 NIS对/etc/passwd文件的集中控制	12.2.4 NIS组成	12.2.4 NIS组成
12.2.5 NIS的安全性问题	12.2.6 欺骗服务器	12.3 远程登录/远程shell服务作为作案工具	12.3 远程登录/远程shell服务作为作案工具
12.4 文件传输协议服务作为作案工具	12.5 Sun OS系统的网络安全	12.5.1 NFS	12.5.1 NFS
的安全	12.5.2 NFS安全性方面的缺陷	12.5.3 远程过程调用 (RPC) 鉴别	12.5.4
UNIX鉴别机制	12.5.5 DES鉴别系统	12.5.6 公共关键字的编码	12.6 本章小结
	第十三章 电子邮件攻击	13.1 电子邮件欺骗	13.1.1 什么是电子邮件欺
骗	13.1.2 邮件的发送过程	13.1.3 发送一封假冒的邮件	13.1.4 保护电子邮件信
息	13.2 电子邮件轰炸和电子邮件“滚雪球”	13.3 本章小结	第十四
章 IP欺骗及其防范对策	14.1 关于盗用IP地址	14.2 欺骗 (Spoofing)	14.2.1 IP
欺骗	14.2.2 可以实施欺骗的对象	14.2.3 UNIX环境下的R系列服务	14.3 IP欺骗
的实施	14.3.1 关于信任关系	14.3.2 IP欺骗攻击分类	14.3.3 攻击的几个过程
14.3.4 IP欺骗出现的频率	14.4 IP欺骗攻击的防备	14.5 本章小结	14.5 本章小结
第十五章 针对攻击的处理对策	15.1 一些原则	15.1.1 不要惊慌	15.1.2 作好记
录	15.1.3 进行计划	15.2 发现并促信入侵者	15.2.1 发现入侵者
地异常事件分析	15.2.3 发现入侵后的对策	15.3 预防和补救	15.3.1 使用安全工
具	15.3.2 使用防火墙	15.3.3 过滤网上通信	15.3.4 限制系统
律武器	15.4 本章小结	第十六章 安全措施	15.3.5 法
16.1.1 记帐	16.1.2 其他检查命令	16.1.3 安全检查程序	16.1 安全检查
16.3 加密	16.3.1 通信中的数据加密	16.3.2 PGP	16.2 系统管理员意识
16.5 备份.清除与物理安全	16.5.1 备份	16.5.2 清除措施	16.4 用户身份鉴别
16.6 本章小结			16.5.3 物理安全

<<黑客分析与防范技术>>

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>