

<<网络与系统攻击技术>>

图书基本信息

书名：<<网络与系统攻击技术>>

13位ISBN编号：9787811142228

10位ISBN编号：7811142228

出版时间：2007-8

出版时间：电子科技大学

作者：李毅超，曹跃，梁

页数：300

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>

## <<网络与系统攻击技术>>

### 内容概要

《普通高等学校信息安全十一五规划教材：网络与系统攻击技术》为普通高等学校信息安全“十一五”规划教材之一，内容深入浅出，新颖丰富，从网络安全和系统安全两个角度，深入剖析了各种入侵、攻击技术及原理，并给出了实例和防范策略。

《普通高等学校信息安全十一五规划教材：网络与系统攻击技术》内容涵盖了网络与系统攻击技术的目标、方法、模型；网络信息探测；系统信息探测；拒绝服务攻击；软件缓冲区溢出漏洞攻击；Web与数据库安全漏洞攻击；病毒、蠕虫和木马等恶意代码攻击以及新兴的网络攻击等。

《普通高等学校信息安全十一五规划教材：网络与系统攻击技术》注重科学性与实用性，并配有精选实例，供读者参考。

## &lt;&lt;网络与系统攻击技术&gt;&gt;

## 书籍目录

第1章 网络攻击原理与技术1.1 网络攻击概述1.2 网络攻击目录1.2.1 信息保密性1.2.2 信息完整性1.2.3 服务可用性1.2.4 运行可控性1.3 网络攻击分类1.3.1 基于攻击术语分类1.3.2 基于攻击种类分类1.3.3 基于攻击效果分类1.3.4 基于弱点分类矩阵1.3.5 基于攻击过程分类1.3.6 基于多维角度分类1.3.7 基于攻击步骤分类1.3.8 网络攻击分类实例1.4 网络攻击模型1.4.1 攻击隐藏1.4.2 信息收集1.4.3 弱点探测1.4.4 权限获取1.4.5 行为隐藏1.4.6 攻击设施1.4.7 后门安装1.4.8 痕迹清除1.4.9 攻击讨论第2章 网络信息探测2.1 目标系统确定2.1.1 网页搜寻2.1.2 链接搜索2.1.3 EDGAR搜索2.2 系统存活探测2.2.1 ICMP—ECHO探测2.2.2 ICMP SWEEP探测2.2.3 广播ICMP探测2.2.4 Non—ECHO ICMP探坝2.2.5 TCP扫射探测2.2.6 UDP扫射探测2.3 基本端口服务扫描2.3.1 TCP Connect扫描2.3.2 UDP扫描2.4 高级端口服务扫描2.4.1 TCP SYN扫描2.4.2 秘密扫描2.4.3 扫描扫射2.4.4 端口扫描策略2.4.5 常用扫描工具2.5 网络环境探测2.5.1 简单网络管理协议2.5.2 简单网络管理协议探测第3章 系统信息探测3.1 服务版本类型探测3.2 操作系统指纹探测3.2.1 TCP/IP栈指纹扫描技术3.2.2 ICMP栈指纹扫描技术3.2.3 操作系统被动扫描技术3.2.4 流行网站快照3.3 Windows系统信息探测3.3.1 NetBIOS简介3.3.2 利用NetBIOS3.3.3 资源工具箱内的查点工具3.4 Unix系统信息探测第4章 拒绝服务攻击4.1 拒绝服务类型4.1.1 概况4.1.2 基本形式4.1.3 攻击类型4.1.4 常见攻击实例4.2 本地拒绝服务攻击4.3 远程拒绝服务攻击4.3.1 SYN Flood攻击4.3.2 Smurf攻击4.3.3 00B Nuke攻击4.3.4 Teardrop攻击4.3.5 Land攻击4.3.6 Kiss of Death攻击4.4 分布式拒绝服务攻击4.4.1 DDoS的概念4.4.2 DDoS攻击常用工具4.4.3 DDoS监测4.4.4 DDoS防御策略与补救措施4.4.5 DDoS防御实例第5章 软件缓冲区溢出攻击5.1 缓冲区溢出概述5.1.1 原理与概念5.1.2 Windows缓冲区溢出5.1.3 构造缓冲区溢出5.1.4 缓冲区溢出攻击5.1.5 缓冲区溢出利用5.2 栈溢出攻击5.2.1 进程空间内存分布5.2.2 程序的堆栈使用5.2.3 栈溢出攻击利用5.3 堆溢出攻击5.3.1 基本概念5.3.2 堆溢出攻击5.3.3 堆溢出防护5.4 格式化字符串攻击5.4.1 相关函数5.4.2 漏洞原理5.4.3 漏洞检查5.4.4 攻击实例5.5 Shell Code编写5.6 缓冲区溢出防范第6章 Web与数据库攻击6.1 跨站脚本攻击6.1.1 CGI简介6.1.2 跨站脚本执行漏洞6.2 ASP脚本攻击6.2.1 ASP简介6.2.2 ASP源码泄露6.2.3 ASP脚本攻击及防范6.3 PHP脚本攻击6.3.1 PHP漏洞威胁6.3.2 PHP漏洞攻击6.4 MySQL注入攻击6.4.1 MySQL注入简介6.4.2 PHP+MySQL注入6.4.3 语句构造6.5 SQL SerVer注入攻击6.5.1 注入漏洞判断6.5.2 数据库服务器类型6.5.3 XP—CMDHELL可执行6.5.4 WEB虚拟目录6.5.5 ASP木马6.5.6 SQL—SERVER专用方式第7章 计算机木马7.1 计算机木马特征7.2 计算机木马发展趋势7.2.1 木马的种类及其技术特征7.2.2 计算机木马发展趋势7.3 系统服务木马7.3.1 WindOws NT / 20007.3.2 UNIX系统7.4 反弹端口木马7.4.1 反弹端口木马原理7.4.2 反弹型木马攻防实战7.4.3 反弹型木马防范7.5 SPI隐蔽木马7.5.1 服务提供者接口7.5.2 SPI木马7.6 木马的启动第8章 计算机病毒与蠕虫8.1 计算机病毒8.1.1 计算机病毒特征8.1.2 计算机病毒分类8.1.3 计算机病毒工作方式8.2 计算机病毒感染机制8.3 计算机病毒触发机制8.4 计算机病毒实例8.4.1 引导扇区病毒8.4.2 COM文件病毒8.4.3 EXE文件型病毒8.5 计算机蠕虫8.5.1 蠕虫定义8.5.2 蠕虫与病毒8.5.3 蠕虫发展史8.5.4 蠕虫行为特征8.5.5 蠕虫分析与防范8.6 计算机蠕虫传播8.6.1 基本结构与传播过程8.6.2 蠕虫入侵过程分析8.6.3 蠕虫传播一般模式8.6.4 蠕虫传播其他模式8.7 计算机蠕虫实例第9章 新兴网络攻击9.1 Phishing9.1.1 Phishing概述9.1.2 Phishing工具策略9.1.3 Phishing技术9.1.4 Phishing防范9.2 P2P攻击9.2.1 P2P简介9.2.2 P2P应用9.2.3 P2P安全缺陷9.2.4 P2P攻击9.2.5 P2P攻击防范附录 专家们公认最危险的20个安全弱点与防范影响所有系统的漏洞 ( G ) G1 操作系统和应用软件的缺省安装G2 没有口令或使用弱口令的账号G3 没有备份或者备份不完整G4 大量打开的端口G5 没有过滤地址不正确的包G6 不存在或不完整的日志G7 易被攻击的GGI程序最危险的windOWS系统漏洞 ( w ) W.1 UniCcode漏洞W.2 IsAPI缓冲区扩展溢出W.3 IIS RDS的使用 ( MicroSOft Remote Data Services ) W.4 NETBIOS——未保护的windows网络共享W.5 通过空对话连接造成的信息泄露W.6 Wleak 11ashing in SAM ( LM Ilash ) UniX系统漏洞 : Top Vulnerabilities To Unix Systems ( U ) U.1 RPC服务缓冲区溢出U.2 Sendmail漏洞U.3 Bind脆弱性U.4 R命令U.5 LPD ( remote print lprotocol daemon ) U.6 sadmind and mountdU.7 缺省SNMP字符串附I 中华人民共和国计算机信息系统安全保护条例附 计算机信息网络国际联网安全保护管理办法参考文献



<<网络与系统攻击技术>>

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>