第一图书网, tushu007.com

<<电子商务站点黑客防范>>

图书基本信息

书名：<<电子商务站点黑客防范>>

13位ISBN编号：9787111094463

10位ISBN编号：7111094468

出版时间：1900-01-01

出版时间：机械工业出版社

作者：美.罗索 等著 智慧东方工作室 译

页数：304

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

内容概要

本书对如何保护电子商务网站做了全面的介绍。
内容包括：灾难恢复、负载平衡和性能优化等，共涉及客户隐私策略和安全金融交易等专业主题。
本书由多位资深网络安全专家精心编著而成，书仔结合他们近10年的网络安全管理经验，以通俗的语言为读者提供了切实可行的解决方案，是一本实用的网络安全参考书。

书籍目录

第1章　为电子商务引入安全原则
1.1　概述
1.2　安全是基础
1.2.1　机密性
1.2.2　完整性
1.2.3　可用性
1.2.4　安全并不只是一个时髦词
1.2.5　电子商务的安全目标
1.2.6　精心计划安全策略
1.2.7　开发阶段的安全
1.2.8　实现安全方案
1.2.9　在安全环境中管理和维护系统
1.3　为现有站点引入安全原则
1.3.1　找出安全隐患
1.3.2　修补过程中的管理和维护
1.4　如何评估安全预算
1.4.1　标尺八法
1.4.2　刺激方法
1.5　安全作为一种限制
1.6　安全作为一种帮助
1.7　小结
1.8　要点
1.9　常见问题解答
第2章 DSoS攻击
2.1　概述
2.2　什么是DDoS攻击
2.2.1　DDoS基础
2.2.2　DDoS攻击详解
2.2.3 2000年2月的攻击
2.3　为何电子商务网站是DDoS的主要攻击目标
2.3.1 一个日益迫切的问题
2.3.2　媒体的"功劳"
2.4　攻击者为了什么
2.4.1　黑客的逻辑
2.4.2　黑客主义
2.4.3　追求短暂的出名
2.4.4　发泄愤怒
2.4.5　经济利益
2.4.6　心怀恶意
2.5　哪些工具可用来执行DDoS攻击
2.5.1 Ttinoo
2.5.2　TFN2K：可移植的作物
2.5.3 Stacheldraht：有刺的铁丝网
2.5.4　更多的DDoS家族
2.6　如何保护网站免遭攻击

2.7　小结
2.8　要点
2.9　常见问题解答
第3章　安全网站设计
3.1　概述
3.2　挑选Web服务器的方法
3.2? Web服务器与Web服务
3.2.2 考虑Web服务器的价格和支持的操作系统
3.2.3　对比Web服务器的安全特性
3.3　安全站点设计基础
3.3.1　拟定安全计划
3.3.2　将安全层次扩展到Web服务器之外
3.3.3　Apache和IIS的比较
3.3.4　安装
3.3.5　强化服务器软件
3.3.6　总体系统强化
3.3.7　密码破解和分析工具
3.3.8　和HTML代码有关的Web设计问题
3.4 Java、JavaScript和ActiveX设计指南
3.4.1　概述
3.4.2　防范Java、JavaScript和ActiveX的问题
3.5　安全脚本编程
3.6　代码签名：是解决问题还是带来更多的问题
3.6.1　理解代码签名
3.6.2　代码签名的优点
3.6.3　代码签名的缺点
3.7　网站应该让别人来设计吗
3.7.1　理解需要的技术
3.7.2　把设计工作承包给别人的优缺点
3.7.3　实施前应仔细检查
3.8　小结
3.9　要点
3.10　常见问题解答
第4章　设计和实现安全策略
4.1　概述
4.2　安全策略对电子商务网站的重要性
4.3　安全策略应强调哪此方面
4.3.1　保密性与个人隐私策略
4.3.2　信息完整性策略
4.3.3　服务策略的可用性
4.4　网上有现成的安全策略吗
4.4.1　每家单价的策略是不同的
4.4.2　示范策略和框架
4.4.3　让外人来制订策略的问题
4.5　如何利用安全策略来实现技术方案
4.6　如何将安全策略通知给客户
4.7　小结

4.8　要点
4.9　常见问题解答
第5章　实现一个安全的电子商务网站
5.1　概述
5.2　实现安全区
5.2.1　非军事区
5.2.2　每种需要设置一个区
5.2.3　多区网络存在的问题
5.3　理解防火墙
5.3.1　探索防火墙选项
5.3.2　设置防火墙规则集
5.4　把组件放到哪里
5.4.1　按风险来定义系统
5.4.2　建立风险控制需求
5.4.3　通过需求分组来创建安全区
5.5　实现入侵侦测
5.5.1　什么是入侵侦测
5.5.2　在入侵侦测中选择
5.5.3　基于网络的IDS的例子
5.5.4 基于主机的IDS的例子
5.6　管理和监视系统
5.6.1　需要执行哪些管理任务
5.6.2　应进行哪些监视
5.7　站点托管
5.7.1　站点托管的优缺点
5.7.2　服务器寄放
5.7.3　挑选承包合作伙伴或者ASP
5.8　小结
5.9　要点
5.10 常见问题解答
第6章 保护金融交易
6.1　概述
6.2　理解网上支付卡系统
6.2.1　信用卡、签账卡或借记卡
6.2.2　销售点处理
6.2.3　清算和结算
6.2.4　网上支付卡交易步骤
6.3　商业支付方案中的选项
6.3.1　商业服务器供应商
6.3.2　直接使用内部资源
6.4　安全支付处理环境
6.4.1　其他服务器控制
6.4.2　在应用层的控制
6.5　密码学
6.5.1　方法
6.5.2　密钥在密码系统中扮演的角色
6.5.3　密码学原理

6.5.4　数字证书
6.6　探讨电子商务中的密码学
6.6.1　散列功能
6.6.2　区块密码
6.6.3　PPK密码的实现
6.6.4　SSL协议
6.6.5　传输层安全
6.6.6　PGP
6.6.7　S／MIME
6.6.8　安全电子交易
6.6.9　XML数字签名
6.7　虚拟POS实现
6.8　其他支付系统
6.8.1　基于智能卡的方案
6.8.2　代理付账
6.8.3　电子货币
6.9　小结
6.10　要点
6.11　常见问题解答
第7章　检查网站漏洞
7.1　概述
7.2　已知的各类攻击
7.2.1　拒绝服务攻击
7.2.2　信息泄漏攻击
7.2.3　文件访问攻击
7.2.4　讹信攻击
7.2.5　特殊文件／数据库访问攻击
7.2.6　提高权限攻击
7.3　对站点进行一次风险分析
7.3.1　资产评估
7.3.2　攻击原因
7.4　检测自己站点的安全漏洞
7.4.1　决定检测技术
7.4.2　研究自己的漏洞
7.4.3　使用自动扫描工具
7.5　雇佣一个入侵测试小组
7.6　小结
7.7　要点
7.8　常见问题解答
第8章　灾难恢复计划
8.1　概述
8.2　什么是灾难恢复计划
8.2.1　拟定灾难恢复计划
8.2.2　保证符合质量标准
8.3　确保安全的信息备份和恢复
8.3.1　进行备份和验证的必要性
8.3.2　保护敏感信息的备份

8.4　预防硬件故障或服务丢失
8.5　如何防范自然灾害
8.5.1　热站：进行恢复的另一个办法
8.5.2　如何挑选一个热站
8.5.3　进行测试
8.6　保险选择
8.6.1　错误和疏忽保险
8.6.2　知识产权保险
8.6.3　第一方电子商务保护
8.6.4　决定保险范围
8.6.5　一些可能不必要的保险
8.7　小结
8.8　要点
8.9　常见问题解答
第9章　控制大流量网络传输
9.1　概述
9.2　想不到站点如此受欢迎，怎么办
9.2.1　判断站点负载
9.2.2　性能调节Web服务器
9.3　怎样管理带宽需求
9.3.1　洽商带宽大小
9.3.2　如何规划带宽升级
9.3.3　根据需要获取带宽
9.4　负载平衡概论
9.4.1　什么是负载平衡
9.4.2　负载平衡的优缺点
9.4.3　负载平衡和安全
9.5　小结
9.6　要点
9.7　常见问题解答
第10章　事故反应、司法调查和法律
10.1　概述
10.2　事件反应策略的重要性
10.2.1　惊慌还是冷静
10.2.2　如何才能不去管一个事件
10.2.3　正确的策略权衡
10.2.4　再论事件反应策略
10.3　建立一个事件反应小组
10.4　设置起诉范围
10.4.1　试图越界的攻击者
10.4.2　理解管制链
10.5　建立一个事件反应规程
10.6　司法调查
10.7　事件跟踪
10.8　资源
10.8.1　法律／政府／执法
10.8.2　备份／司法

10.8.3　事件跟踪系统
10.8.4　杂项
10.9　小结
10.10　要点
10.11　常见问题解答
附录A　进行内容发布的Cisco方案

第一图书网, tushu007.com

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