<<网络安全基础与应用>>

图书基本信息

书名：<<网络安全基础与应用>>

13位ISBN编号：9787115160294

10位ISBN编号：7115160295

出版时间：2007-7

出版时间：张千里 人民邮电出版社 (2007-07出版)

作者：张千里

页数：277

<<网络安全基础与应用>>

内容概要

《网络安全基础与应用》的主要目的，就是结合网络安全系统构建的需求，介绍一些常见的网络安全措施。

《网络安全基础与应用》首先简要介绍了当前网络安全方面的一些基础知识，然后重点介绍了三个方面的主要内容——网络安全协议、系统安全防护、网络安全防护以及入侵检测和响应。

网络安全协议所侧重的，是从协议的角度保护互联网络基础设施；系统安全防护指的是操作系统的安全防护；网络安全防护中重点介绍了网络安全管理政策、网络安全风险评估以及网络设备的访问权限控制；而入侵检测和紧急响应则侧重于从实际运营的角度来发现网络中的动态风险，并采取有效的措施。

根据这些技术，基于开放源代码软件，一个廉价、可靠的网络安全解决方案就可以构建出来。

《网络安全基础与应用》具有很强的实用性，通过《网络安全基础与应用》的阅读，读者可以得到有关安全系统构建所需要的基本理论知识和实际技巧；另一方面，《网络安全基础与应用》对于开源软件的侧重也是特色之一，开源软件，尤其是安全领域的开源软件，可以提供经济、可靠、安全的解决方案。

因此，相信《网络安全基础与应用》对于网络安全研究和从业人员，具有重要的参考作用。

<<网络安全基础与应用>>

书籍目录

第1章　因特网风险分析1.1　TCP/IP协议的安全问题1.1.1　TCP/IP概述1.1.2　拒绝服务攻击1.1.3　监听（Sniff）、假冒（Spoof）和劫持（Hijack）1.1.4　TCP/UDP应用层服务的安全问题1.2　软件实现缺陷1.2.1　缓冲区溢出1.2.2　堆溢出（Heap Overflow）1.3　用户使用引入的风险参考文献第2章　密码学基础2.1　密钥密码学介绍2.1.1　背景知识介绍2.1.2　当前密钥加密算法2.1.3　数据完整性和哈西2.1.4　密钥密码学的安全服务2.1.5　密钥的发布和管理2.2　公钥密码学2.2.1　公钥密码学的基础2.2.2　公钥加密服务2.2.3　公钥基础设施介绍参考文献第3章　安全协议3.1　无线局域网络安全3.1.1　IEEE 802.11协议的体系结构3.1.2　无线网络安全介绍3.1.3　TKIP算法原理3.2　IPSEC3.2.1　IPSEC体系结构3.2.2　Internet 密钥交换3.2.3　安全关联的使用模式3.2.4　ESP3.2.5　验证头（AH）3.3　TCP层安全SSL/TLS3.3.1　SSL操作3.3.2　报文格式3.3.3　传输层安全协议（TLS）参考文献第4章　操作系统安全防护4.1　操作系统安全概述4.1.1　操作系统安全概念4.1.2　计算机操作系统安全评估4.1.3　国内的安全操作系统评估4.1.4　操作系统的安全配置4.2　Windows系统安全防护4.2.1　Windows 2000操作系统安全性能简介4.2.2　Windows 2000安全配置4.3　UNIX/LINUX系统安全防护4.3.1　Solaris系统安全管理4.3.2　LINUX安全防护4.4　常见服务的安全防护4.4.1　WWW服务器的安全防护4.4.2　Xinetd超级守护程序配置4.4.3　SSH参考文献第5章　网络安全防护5.1　网络安全管理政策5.1.1　鉴定网络连接的类型5.1.2　审核网络特点和相关的信任关系5.1.3　确定安全风险的类型5.1.4　确定适当的潜在防护领域并建立防护措施……第6章　入侵检测和紧急响应第7章　使用开源软件构建安全系统后语　网络安全未来

章节摘录

一旦入侵检测系统发现攻击或者入侵，它们会有一定的响应。
这些响应包括相关入侵的报告文档、追踪入侵发起源和入侵者。
有的入侵检测系统具有自动响应功能。
虽然不受到很多研究员的重视，响应工作却是一件很实际和十分重要的事。
入侵检测商业产品一般都有多个响应选项，一般可分成主动响应和被动响应或者两者的混合。
1.主动响应　　入侵检测系统的主动响应就是当一次攻击或入侵被检测到，检测系统自动作出一些动作。
主动响应分成三类：　　（1）收集相关信息　　一种最基本但最花时间的主动响应就是再一次深入地收集可疑攻击和入侵的有关信息。
在生活当中，当夜里被一个奇怪的声音吵醒，我们可能也会做_个类似于这种响应的工作。
在这种情况下，每个人一般都想办法靠近发出声音的地方，听得更清楚，收集、理解相关信息再决定采取什么行动。
在入侵检测系统的场合上，这种响应一般是检查一些敏感的信息源（例如，查看操作系统审计记录的事件，查看网络上的数据包等）。
收集相关信息并总结出多种可能的原因。
这些相关信息可以帮助用户确定入侵事件的状态（特别是确定攻击是否成功地穿入用户的系统）。
这个选项也帮助调查入侵者的身份，提供入侵行为的法律证据。
（2）改变环境　　另一种自动响应就是中断攻击过程和阻止攻击这的其他行动。
通常，入侵检测系统没有能力阻止一个人的行为，但是它可以封闭这个人可能使用的IP地址。
封闭一个有经验的攻击者是一件很困难的事，下面的行动可以阻止新手攻击者，对有经验的攻击者有一定的限制。
在攻击者和受害系统的连接中插入TCPReset包。
根据TCP/IP协议，连接就被终止。
重新配置路由器和防火墙，禁止来自攻击者的IP地址的包。
重新配置路由器和防火墙，禁止攻击者访问文件系统的网络端口和服务。
（3）反击攻击者　　有些人认为，入侵检测系统的主动响应的第一选项应该是反击攻击者。
这种响应包括反攻击攻击者的主机或者网站，或者利用攻击方法去收集攻击者身份的信息。
但这不是一个对的主意！
在一个没有明确的法律的网络环境下，这样的措施可能有很大的风险。
第一个原因就是反攻击别的主机可能是非法的行为；此外，很多攻击者使用假的网络地址，所以反攻击很可能会伤害无辜；最后，反击攻击者有可能会把情况弄得更坏，攻击者本来只是想浏览一下用户的站点，一旦受到反攻击后，可能会采取一些其他的行动。
我们建议这个选项不应该随意使用。
虽然是自动响应，但管理员也要有一定的监控和控制。
2.被动响应　　被动响应提供攻击和入侵的相关信息，再由管理员根据所提供的信息采取适应的行动。
这种响应方法是很多入侵检测系统商业产品的选择。
（1）报警和告示　　当攻击被检测出来，入侵检测系统作出报警和告示通知管理员或者使用者。
大多数入侵检测系统的商业产品允许使用者灵活地决定系统在什么场合上作出报警和通知给谁。
一种常用的报警就是在屏幕上打出报警或者弹出报警窗口。
这些报警在入侵检测系统的控制台还是其他地方显示由管理员在安装、配置的时候指定。
报警信息有各种形式，简单的就是什么入侵事件发生，详细的就是攻击者的身份、使用的攻击工具和入侵造成的危害。
另一种报警和告示是通知给多个远程管理员和有关组织。

有的入侵检测系统允许用户选择在紧急响应的时候使用的通知方式：呼机和手机。
　　有的产品提供电子邮件的通知方式。
这种通知方式不是很安全，因为，攻击者经常能监视到电子邮件系统，甚至可以阻止它。
　　（2）SNMP协议通知　　有的入侵检测系统类型的商业产品提供报警和告示通知给网络管理系统。
这些消息使用SNMP协议作出报警和告示。
SNMP协议是网络管理系统所使用的协议，所以网络管理系统的组件和管理员可以对入侵检测系统的报警信息进行操作。
使用这种报警方式有很多好处，包括允许整个网络参与到入侵检测和响应过程。
另一个好处就是可以很快地把入侵事件通知到入侵发起源的负责机构，让他们协助调查和处理。
　　很多入侵检测系统类型的商业产品提供定期事件报告文档。
有的允许用户选择要报告的期间（如一个星期、一个月等）。
有的还提供入侵事件的统计数据，甚至提供标准的数据库接口，让用户使用其他数据统计的软件包。
　　……

<<网络安全基础与应用>>

版权说明