

<<信息安全技术与应用>>

图书基本信息

书名：<<信息安全技术与应用>>

13位ISBN编号：9787115302472

10位ISBN编号：7115302472

出版时间：2013-3

出版时间：人民邮电出版社

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>

<<信息安全技术与应用>>

内容概要

<<信息安全技术与应用>>

书籍目录

第1章信息安全概述 1.1信息安全基本概念 1.1.1信息安全定义 1.1.2信息安全目标 1.1.3信息安全模型 1.1.4信息安全策略 1.2信息安全漏洞与威胁 1.2.1软件漏洞 1.2.2网络协议漏洞 1.2.3安全管理漏洞 1.2.4信息安全威胁来源 1.3信息安全评价标准 1.3.1信息安全评价标准简介 1.3.2美国可信计算机系统评价标准 1.3.3其他国家信息安全评价标准 1.3.4国际通用信息安全评价标准 1.3.5国家信息安全评价标准 1.4国家信息安全保护制度 1.4.1信息系统建设和应用制度 1.4.2信息安全等级保护制度 1.4.3国际联网备案与媒体进出境制度 1.4.4安全管理与计算机犯罪报告制度 1.4.5计算机病毒与有害数据防治制度 1.4.6安全专用产品销售许可证制度 1.5信息安全等级保护法规和标准 1.5.1信息系统安全等级保护法规 1.5.2信息系统安全等级保护定级 1.5.3信息系统安全等级保护基本要求 1.6本章知识点小结 习题 第2章密码技术基础 2.1密码学理论基础 2.1.1信息论基础知识 2.1.2数论基础知识 2.1.3计算复杂性基础知识 2.2密码系统与加密标准 2.2.1密码系统的基本概念 2.2.2信息加密方式 2.2.3数据加密标准 2.3信息加密算法 2.3.1 DES加密算法 2.3.2 RSA加密算法 2.3.3 Diffie—Hellman算法 2.3.4 ElGamal加密算法 2.3.5椭圆曲线加密算法 2.4信息加密产品简介 2.4.1 PGP加密软件简介 2.4.2 CryptoAPI加密软件简介 2.5本章知识点小结 习题 第3章身份认证与访问控制 3.1身份认证技术概述 3.1.1身份认证的基本概念 3.1.2基于信息秘密的身份认证 3.1.3基于信任物体的身份认证 3.1.4基于生物特征的身份认证 3.2安全的身份认证 3.2.1身份认证的安全性 3.2.2 口令认证的安全方案 3.2.3基于指纹的电子商务身份认证 3.2.4 Kerberos身份认证 3.2.5基于X.509数字证书的认证 3.3访问控制 3.3.1访问控制的概念 3.3.2访问控制关系描述 3.3.3访问控制策略 3.4本章知识点小结 习题 第4章防火墙工作原理及应用 4.1防火墙概述 4.1.1防火墙的概念 4.1.2防火墙的功能 4.1.3防火墙的历史 4.1.4防火墙的原理 4.1.5防火墙的分类 4.1.6防火墙的组成及位置 4.1.7防火墙的局限性 4.1.8防火墙的发展趋势 4.2防火墙技术 4.2.1分组过滤技术 4.2.2代理服务器技术 4.2.3应用级网关技术 4.2.4电路级网关技术 4.2.5状态检测技术 4.2.6网络地址转换技术 4.3防火墙体系结构 4.3.1相关术语 4.3.2分组过滤路由器体系结构 4.3.3双宿主主机体系结构 4.3.4堡垒主机过滤体系结构 4.3.5被屏蔽子网体系结构 4.3.6组合体系结构 4.4防火墙选型与产品简介 4.4.1防火墙的安全策略 4.4.2防火墙的选型原则 4.4.3典型防火墙产品介绍 4.5防火墙应用案例 4.5.1 DMZ区域和外网的访问控制 应用案例 4.5.2某企业防火墙部署应用案例 4.6本章知识点小结 习题 第5章攻击技术分析 5.1网络信息采集 5.1.1常用信息采集命令 5.1.2漏洞扫描 5.1.3端口扫描 5.1.4网络窃听 5.1.5典型信息采集工具 5.2拒绝服务攻击 5.2.1基本的拒绝服务攻击 5.2.2分布式拒绝服务攻击 5.2.3拒绝服务攻击的防范技术 5.3漏洞攻击 5.3.1配置漏洞攻击 5.3.2协议漏洞攻击 5.3.3程序漏洞攻击 5.4木马攻击 5.4.1基本概念 5.4.2木马的特点 5.4.3木马的基本原理 5.4.4木马的防范技术 5.4.5常见木马的查杀方法 5.5蠕虫技术 5.5.1蠕虫技术的特点 5.5.2蠕虫的基本原理 5.5.3防范蠕虫的措施 …… 第6章入侵检测系统 第7章计算机病毒防治 第8章安全通信协议 第9章电子邮件系统安全 第10章无线网络安全 附录英文缩写对照表 参考文献

章节摘录

版权页：插图：②不受加密和交换设备影响。

HIDS只关注主机本身发生的事件，并不关心主机之外的网络事件，所以检测性能不受数据加密、隧道和交换设备影响。

网络入侵检测系统利用网络监听采集网络中传输的数据流，通过网络协议解析还原成传输层或应用层的网络连接记录，然后根据连接记录属性特征识别网络异常行为。

但是当数据采用加密传输或使用加密技术进行攻击时，由于没有密钥解密，自然不能获得协议类型、IP地址和服务类型等基本属性。

此外，网络传感器只采集所在网段的数据，不能采集位于不同网段的数据。

使用交换设备划分多个网段后，将减小网络入侵检测系统监测的范围。

网络传感器造价十分昂贵，安装多台网络传感器将大大增加系统的部署成本。

③不受网络流量影响。

由于网络传感器解析网络数据需要耗费许多计算资源，当网络流量过高时，网络传感器不能及时采集就会丢失数据，在高速网络环境下数据处理和分析能力显著下降是网络入侵检测系统的致命缺陷，因此，随着网络流量的增加，攻击检测率将迅速下降，而且网络流量与检测率之间的矛盾随着吉比特网和10吉比特网的日益普及显得更加突出。

HIDS并不采集网络数据，不会因为网络流量增加而丢失对系统行为的监视，故其检测性能与网络流量无关。

但HIDS也存在许多缺点，HIDS安装在需要保护的主机上，必然会占用主机系统资源，额外负载将降低应用系统的效率。

此外，HIDS完全依赖操作系统固有的审计机制，所以必须与操作系统紧密集成，导致平台的可移植性差。

而且，本身的健壮性也受到主机操作系统安全性的限制。

HIDS只能检测针对本机的攻击，而不能检测基于网络协议的攻击。

(2) 网络入侵检测系统 当入侵检测监视的对象为网络关键路径上的网络数据时，称为网络入侵检测系统(network-based intrusion detection system, NIDS)。

局域网通常采用的都是基于广播机制的以太网协议，以太网协议能够使主机接收同一网段内的所有广播数据。

以太网网络适配器有正常和混杂两种工作模式，正常模式只接收本机地址和广播地址的数据，混杂模式则接收本网段内的所有数据。

NIDS正是利用了网络适配器的混杂工作模式来实时采集通过网络的所有数据，通过网络协议解析与模式匹配实现入侵行为检测，主要用于发现试图危害网络基础设施的行为。

相对于HIDS而言，NIDS具有下列优点。

①检测与响应速度快。

NIDS能够在成功入侵之前发现攻击和可疑意图，在攻击目标遭受破坏之前即可执行快速响应中止攻击过程。

而HIDS只有当系统日志记录入侵行为之后才能开始检测，此时，关键应用服务有可能已经遭到破坏。

②入侵监视范围大。

由于每个网络传感器能够采集共享网段内的所有数据，一个网络传感器就可以保护一个网段。

因此，只在网络关键路径上安装网络传感器，就可以监视整个网络通信。

③入侵取证可靠。

NIDS通过捕获网络流量收集入侵证据，攻击者无法转移证据。

对HIDS而言，如果攻击者破坏了审计记录和系统日志，就很难获得可靠的入侵证据。

④能够检测协议漏洞攻击。

许多攻击程序是基于网络协议漏洞编写的，诸如同步洪流(SYNflood)、Smurf攻击、泪滴攻击(teardrop)等只有通过查看首部或有效载荷才能识别。

NIDS同样也存在一些缺点，网络传感器只监视网段内的通信，所以在交换以太网环境中监测范围受到限制。
在高速网络流量环境下检测精度下降；不能检测加密数据、隧道数据和加密数据攻击；网络传感器向控制台回传数据量大等。

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>