第一图书网, tushu007.com

<<计算机网络信息安全与应用>>

图书基本信息

书名：<<计算机网络信息安全与应用>>

13位ISBN编号：9787302272960

10位ISBN编号：7302272964

出版时间：2012-2

出版时间：清华大学出版社

作者：贺思德

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

前言

计算机网络安全和信息安全是知识面十分宽广的研究领域，在与不断涌现的千变万化的互联网安全事件的攻防对抗中，促进了该学科的快速发展。
网络信息安全攻防对抗的博弈过程是永远不会结束的，往往旧的安全问题还未彻底解决，新的安全问题又出现了。
为了便于人们探索解决各种现实安全威胁的方法和途径，可将网络信息安全问题进行如下粗略分类：
（1）计算机操作系统的安全漏洞。
常用的计算机操作系统有Windows2003/XP、UNIX、Linux等。
在开发一个操作系统的时候，首先考虑的是如何实现系统目标所要求的各种功能。
只有当操作系统在使用过程中，其中某个环节被人恶意利用了，这时才会发现操作系统的此环节存在一个漏洞。
于是开发者设计出改进该环节的软件补丁，供用户安装来加强系统的安全。
因此在操作系统的整个使用寿命期内，都会不断地有新的漏洞发现，并且须及时安装补丁软件。
对于大部分操作系统内部的复杂安全问题，作为用户只能通过及时安装开发商提供的各种补丁软件来解决。
（2）应用软件系统的安全漏洞。
人们在计算机和网络上使用各种办公软件，如业务管理软件、财务管理软件等。
很多应用软件的开发商对解决自己产品中的安全问题不太在意，他们大多通过在自己开发的应用软件中集成某些第三方的安全软件模块，或者完全依赖于计算机操作系统和网络系统提供的安全保障环境。
（3）本地私有网络操作系统的安全。
当前常见的网络操作系统有以太网、Microsoft网络、NetWare网络、PPP远程拨号网络等。
每一种网络操作系统都有其特点和适用领域，也存在各自的安全漏洞和薄弱环节。
计算机网络管理员和用户应当根据自己的具体需要，正确地选择和安装网络操作系统，并且进行正确的网络参数配置。
网络管理员应当从内网用户计算机中卸载那些不需要的网络操作系统，以减少其安全漏洞所带来的隐患，净化内网数据环境，这是重要的网管基础工作。
（4）互联网协议的安全漏洞。
当前互联网的TCP/IP协议族中，各分层包含的协议共约20多种。
并且随着新的网络应用的不断出现，很多公司都在自己的互联网应用中采用了自主知识产权的网络通信协议（例如Web迅雷、QQ、网络游戏、PPlive等）。
每种网络协议都可实现其特定的功能，但是每种协议都存在各自的安全漏洞。
因此，很多网络安全攻击事件就是利用了某些协议的漏洞。
（5）信息安全。
信息安全提供的服务可分为5类：信息的保密和隐私，信息完整性的验证，信息发送者的身份认证和防拒认技术，信息的隐藏技术，对网络实体的认证技术等。
（6）物理层的安全问题。
网络通信是通过各种物理信道传输的，其安全问题包括双绞线的电磁泄漏，无线信道的数据泄密，光纤的安全防护、雷电、地震、火灾、治安等。
学习研究网络信息安全知识的最好方法是边学习边进行网络协议数据分析实践。
建议首先掌握第7章介绍的常用DOS命令和Wireshark网络协议数据分析软件的使用方法，然后结合本书中各章节的介绍，在学员自己的网络计算机上进行各种协议数据的捕获分析实验。
先从下层的数据链路协议开始，逐层向上至应用层，每周都应完成一个协议数据实验分析报告。
要求每个学员独立完成TCP/IP协议族中包含的20多个基本协议的数据捕获与分析实验，这样才能具备独立地分析和解决网络安全实际问题的能力。
本教材适用于本科生、研究生、计算机网络信息安全的管理维护人员和互联网的用户，因此分析

研究的重点放在上述第（3）、（4）和（5）项。
本书强调理论联系实际、深入浅出地研究分析网络信息安全监管和使用中出现的各种问题的原因，有了清晰的思路后，具体的解决方案就有多种不同的选择。
因此不希望教师将有限的教学课时用来讲解各种具体型号设备的操作，应“授人以渔”，充分利用学员自己的网络计算机和课外时间来完成对20多个常用协议的数据解剖与安全分析实验。
　　本书将一些重要的网络安全基础理论知识放在6个附录中，供高层次的学员深入学习。
作者在多年的教学过程中与教师和学员们多有交流，并不断地对本书进行修订和改进。
随着互联网的应用出现了很多新的变化，在本次出版中做了相应的内容调整和补充。
对本书做出部分贡献的有申浩如、者明伟、王哲等。
书中引用的有关资料源于参考文献中，特向有关作者致以诚挚的谢意。
　　贺思德　　2011年12月

内容概要

《高等学校计算机专业教材精选·网络与通信技术：计算机网络信息安全与应用》介绍了计算机网络远程连接的规划设计、运行管理、网络信息安全的保障与监测、网络用户上网行为监管等实际应用中的基础知识。
书中按照互联网参考模型的分层结构，从下层至上层，即按照网络数据包封装的逐层解剖顺序，深入浅出地讨论每一层的主流协议原理与实用技术，以及各层出现的现实安全威胁问题，图文并茂地列举了网络信息安全监管中的大量案例分析。
采用开源的网络数据捕获与分析软件作为教学实验工具，每章附有习题与实践课题，让读者在自己的网络计算机上理论联系实际、由浅入深地边学习边实践，掌握与提高分析解决网络信息安全系统规划、运维监管中的实际问题的能力。
《高等学校计算机专业教材精选·网络与通信技术：计算机网络信息安全与应用》可作为通信与计算机网络、信息安全、电子商务等相关专业的本科生、研究生的教材，也可作为计算机网络和信息安全运维管理的工程技术人员的参考书。

书籍目录

第1章 互联网及其应用概述1.1 网络应用与分层结构1.1.1 协议、服务和分层结构的例子1.1.2 开放系统互连OSI模型及规范化描述1.2 TCP/IP网络模型与协议构架1.2.1 TCP/IP网络协议的结构1.2.2 TCP/IP网络模型与OSI模型之间的关系1.2.3 异类网络之间如何互联通信1.3 利用Wireshark捕获分析网络数据及其安全性1.4 计算机网络知识中的若干基本概念1.5 本章小结习题与实践第2章 广域网接入与身份认证技术2.1 电信系统的互联网接入服务2.1.1 电路交换的概念2.1.2 电话系统的信令和数据传输系统2.1.3 电信系统提供的互联网接入服务2.1.4 拨号调制解调器2.1.5 数字用户线路xDSL2.1.6 点对点的数据通信协议PPP2.2 身份认证协议PAP和CHAP2.2.1 口令认证协议（PAP）2.2.2 挑战握手身份认证协议（CHAP）2.3 AAA与RADIUS协议原理与应用2.3.1 对用户的AAA认证、授权与计费管理2.3.2 RADIUS协议原理与应用2.4 基于SDH的多业务传输平台MSTP在互联网中的应用2.4.1 SDH同步数据通信网简介2.4.2 基于SDH的多业务传输平台MSTP的广域网接口技术2.4.3 千兆广域以太网在多业务传输平台MSTP上的实现2.5 本章要点习题与实践第3章 以太网家族及其安全应用3.1 以太网与IEEE 802.3.1.1 IEEE 802局域网标准3.1.2 IEEE 802.3与标准以太网3.1.3 以太网的物理层3.1.4 IEEE 802.3u快速以太网3.1.5 IEEE 802.3z千兆以太网3.1.6 IEEE 802.3ae十千兆以太网3.2 动态主机配置协议DHCP及其安全3.2.1 DHCP协议的工作过程3.2.2 DHCP协议的安全问题3.3 地址解析协议ARP及其安全问题3.3.1 静态ARP地址映射3.3.2 动态ARP地址查询3.3.3 ARP诱骗的原理与防御3.4 基于无源光纤网的千兆以太网EPON3.4.1 EPON的网络结构3.4.2 EPON的工作原理3.4.3 EPON在城域网的三网融合中的应用3.4.4 EPON的信息安全问题3.5 IEEE 802.11无线局域网3.5.1 IEEE 802.11无线局域网的结构3.5.2 IEEE 802.11无线局域网的MAC子层3.5.3 IEEE 802.11无线局域网的物理层3.5.4 IEEE 802.11无线局域网的安全性3.6 本章小结习题与实践第4章 IPv4和IPv6协议及其安全4.1 互联网IP地址4.1.1 IPv4地址及其分类4.1.2 无类IP地址分配4.1.3 网络地址转换（NAT） 4.1.4 IPv6地址4.2 互联网层协议4.2.1 网络互联需解决的问题4.2.2 IPv4互联网协议4.2.3 IPv6互联网协议4.2.4 从IPv4网络到IPv6网络的过渡技术方案4.3 本章要点习题与实践第5章 传输层协议及其攻击案例5.1 进程对进程的传输5.2 用户数据报协议5.2.1 UDP协议使用的公认端口号5.2.2 UDP的数据报结构5.2.3 UDP数据报的传输5.2.4 UDP协议的应用领域5.3 传输控制协议5.3.1 TCP提供的服务5.3.2 TCP的特性5.3.3 TCP数据段5.3.4 建立TCP连接的过程5.3.5 TCP数据段的传输过程5.3.6 终止TCP的连接5.3.7 TCP的流量控制5.3.8 TCP的差错控制5.4 数据流控制传输协议简介5.5 传输层的网络攻击案例5.5.1 利用TCP对目标主机的开放端口扫描5.5.2 利用TCP对目标主机的半开放端口扫描5.5.3 利用TCP对目标主机的Xmas扫描5.5.4 无效包扫描5.6 本章小结习题与实践第6章 应用层协议及其安全6.1 万维网的基本构架6.2 域名系统及其安全6.2.1 域名系统概述6.2.2 DNS报文格式6.2.3 DNS域名/IP地址解析的工作流程6.2.4 DNS报文的封装实例6.2.5 域名系统的安全隐患6.3 超文本传输协议6.4 Cookie及其安全应用6.5 文件传输协议及其安全6.5.1 FTP工作过程举例6.5.2 FTP的安全问题6.6 电子邮件及其信息安全6.6.1 电子邮件的传输过程6.6.2 邮件传输代理和邮件访问代理6.6.3 多功能互联网邮件扩展与安全邮件6.6.4 垃圾电子邮件及其防范6.7 本章要点习题与实践第7章 网络故障诊断与信息安全分析工具7.1 网络测试常用命令7.1.1 PING在线连通性测试命令7.1.2 路由跟踪探测命令Traceroute7.1.3 本机联网状态检测命令Netstat7.1.4 地址解析协议命令Arp7.1.5 IPconfig 本机网络配置状态命令7.1.6 net命令7.2 网络数据捕获与信息安全诊断7.2.1 网络数据捕获工具的分类7.2.2 网络数据流的监测点选择7.2.3 捕获网络数据流的方法7.2.4 网络协议分析软件Wireshark7.3 本章小结习题与实践第8章 恶意软件及其监测防护8.1 恶意软件8.1.1 恶意软件及其威胁8.1.2 病毒的本质8.1.3 蠕虫8.2 病毒对抗措施8.2.1 对抗病毒的方法8.2.2 高级反病毒技术8.3 木马的工作原理与检测防范8.3.1 木马程序的工作原理8.3.2 木马的种类8.3.3 被木马入侵后出现的症状8.3.4 木马常用的启动方式及检测8.3.5 木马的隐藏与检测方法8.4 特洛伊木马入侵后的网络数据分析案例8.4.1 木马SubSeven Legend8.4.2 后门木马NetBus 8.4.3 木马RST.b8.5 蠕虫的网络数据捕获分析案例8.5.1 SQL Slammer（监狱）蠕虫8.5.2 Code Red Worm（红色代码蠕虫）8.5.3 Ramen蠕虫8.6 本章小结习题与实践第9章 防火墙、IPS入侵保护与安全访问控制9.1 防火墙的设计目标9.1.1 防火墙的控制功能9.1.2 防火墙功能的局限性9.1.3 防火墙的日志记录9.2 防火墙的类型与参数配置9.2.1 网络层的包过滤防火墙9.2.2 网络层的全状态检测防火墙9.2.3 应用层防火墙9.2.4 堡垒主机9.2.5 代理服务器9.3 网络防火墙的配置案例9.3.1 防火墙与NAT功能的组合配置9.3.2 防火墙的路由模式配置案例9.4 入侵检测与入侵保护系

统9.4.1 入侵检测系统9.4.2 入侵保护系统9.4.3 分布式NIPS入侵保护系统配置案例9.5 主机安全访问控制系统9.5.1 安全访问控制的基本概念9.5.2 可信任系统的概念9.5.3 一种盗号木马的工作原理与防护9.5.4 Windows XP操作系统的安全访问控制9.6 本章小结习题与实践第10章 信息加密与安全验证的基本技术10.1 对称密钥通信系统10.1.1 传统的对字符加密的方法10.1.2 数据加密的基本技术10.1.3 数据加密标准DES和AES10.2 非对称密钥通信系统10.2.1 RSA加密算法10.2.2 Differ-Hellman对称密钥交换算法10.3 信息安全技术提供的服务10.3.1 网络信息的保密通信10.3.2 报文的完整性验证10.3.3 对报文的数字签名10.3.4 网络实体的身份认证10.3.5 对称密钥系统的密钥分配10.3.6 非对称密钥系统的公钥发布方式10.3.7 CA数字证书应用实例10.4 本章要点习题与实践第11章 互联网安全协议与电子商务应用11.1 网络层安全协议IPSec与VPN11.1.1 IPSec的传输模式11.1.2 IPSec的隧道模式11.1.3 IPSec的两个安全协议AH和ESP11.1.4 实现虚拟私有网络的各类技术11.2 传输层安全协议11.2.1 SSL/TLS中4个子协议的功能11.2.2 传输层安全协议TLS与SSL和HTTPS的关系11.2.3 基于单方认证的TLS安全电子邮件案例分析11.3 PGP安全协议及其应用11.3.1 PGP安全电子邮件11.3.2 PGP采用的加密与验证算法11.4 安全电子交易SET系统11.4.1 安全电子交易SET系统概况11.4.2 SET系统的组成部分11.4.3 SET系统的工作流程11.4.4 对订货单与支付信息进行双重签名11.4.5 SET的业务类型11.4.6 SET的购货请求11.4.7 安全电子交易SET货款的授权与支付11.4.8 互联网电子商务中使用SSL/TLS与SET的比较11.4.9 Visa公司的“ 3D安全交易 ”（3-D Secure）协议简介11.5 本章要点习题与实践第12章 P2P对等网络应用与上网行为管理12.1 P2P对等网络应用系统的结构12.1.1 非结构化的P2P网络12.1.2 结构化的P2P网络系统12.2 P2P对等网络应用系统12.2.1 P2P应用系统的优缺点12.2.2 常见的P2P应用系统12.2.3 某校园网数据流分类统计案例12.3 网络用户的上网行为管理12.3.1 上网行为管理系统及其功能12.3.2 P2P上网行为的监测与控制12.4 P2P网络数据流的识别方法12.4.1 P2P网络数据流识别方法的分类12.4.2 基于特征码的P2P网络数据识别技术12.5 P2P应用系统及其特征码分析案例12.5.1 案例分析Bit Torrent原理及其特征码12.5.2 PPlive的工作过程12.5.3 P2P应用系统的特征码提取方法总结习题与实践附录A 传输层常用的端口号附录B 校验和的计算B.1 部分和的计算B.2 和的计算B.3 校验和的计算附录C 各种进制的数值换算与IPv4地址C.1 十进制数C.2 二进制数与十进制数的转换C.3 十六进制数与十进制数的转换C.4 256进制数与十进制数的转换C.5 计算举例： IPv4地址的4种数值表达方式附录D CRC循环冗余校验码的计算D.1 数组的运算可以转换为多项式的运算D.2 数据通信系统中CRC码的使用方法附录E 素数与模运算的基本概念E.1 素数与互素数E.2 模运算的几个规则附录F ASCII编码表429参考文献

章节摘录

版权页：插图：由于以太局域网内工作站之间的通信是根据目的和源端的网卡的MAC地址进行寻址的，MAC地址是无层次的平面地址，平面地址只适合在用户量不多的小环境中使用。
类似于，在同一个班的教室中每个学生的名字是不分等级的平面地址，若要寻找某个学生，可在班的教室中广播呼叫其姓名，每个学生都听到呼叫了，但是只有被呼叫名字的学生给出响应。
若要在全省范围内广播呼叫某个学生的名字，那是很难找到该学生的。
而互联网的主机之间的通信是根据目的和源主机的IP地址进行寻址的，IP地址是分层次等级的地址，分层次的地址适合于在大用户量的广域范围内使用。
一个IP地址中包含了网络ID、子网ID和主机1D等。
类似于，当一个学生要给家里写信时，收信人的地址中必须包含：省的名称、市县的名称、街道名称和门牌号码，然后才是收信人的名字。
只有使用这种分层次的地址才能在广域网内进行通信。
现在的问题是，如何在以太网中传输IP包？
因为以太网卡只认识MAC地址，不能识别IP地址。
因此就需要在每台计算机的以太网卡中建立一个本地网络中邻居的MAC地址与IP地址的对照表，即ARP表。
如果一台计算机要传输一个IP包给某网络邻居，首先根据IP包中的目的IP地址从ARP表中查到其对应的MAC地址，然后将IP包封装到一个以太帧中发送出去，该帧的目的MAC地址就设为来自ARP表中的查询结果。
如果以太网计算机中没有ARP表，那么它就不能传输IP包，就不能访问互联网。
ARP地址解析协议就是用于在以太网的每台计算机中自动生成ARP表的。
关于ARP表的结构和分析参看第7.1.4节。
当一台计算机初次接入以太网时，可自动运行DHCP客户端协议，向本地DHCP服务器申请获取分配给本机的互联网IP地址、本地网关的IP地址等5个参数。
但是计算机还必须知道本地网关的MAC地址才能与外网进行通信，这就需要启用ARP协议来获取这些本地网邻居的IP地址对应的MAC地址参数。

编辑推荐

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