第一图书网, tushu007.com

<<狙击黑客>>

图书基本信息

书名：<<狙击黑客>>

13位ISBN编号：9787302174516

10位ISBN编号：7302174512

出版时间：2008-6

出版时间：清华大学出版社

作者：武新华，李秋菊，陈艳艳　等编著

页数：329

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

第一图书网, tushu007.com

<<狙击黑客>>

内容概要

本书以较详实的内容和浅显易懂的语言，介绍了黑客攻击计算机的一般方法、步骤，以及所使用的工具，并向读者详细讲述了防御黑客攻击的方法，使读者在熟悉基本网络安全知识的前提下，掌握基本的反黑知识、工具和修复技巧，以便在遇到别有用心者的入侵时能够尽可能做到心中有数，从而采取相关的方法来制定相应的自救措施，而不是茫然无措，不知如何应对。

在本书附带的多媒体教学光盘中包含了大量全程多媒体视频讲解，紧密结合书中内容和各个知识点，采用情景化教学、详细图文对照以及真实场景演示等方式进行了深入讲解，在扩充本书知识范围的基础上，有效地弱化了本书的学习难度并大大激发了读者对黑客技术的学习兴趣。

本书内容丰富，图文并茂，深入浅出，适用于广大网络爱好者，同时可作为一本速查手册，适用于从事网络安全的人员及网络管理员。

第一图书网, tushu007.com

<<狙击黑客>>

书籍目录

第1章 黑客其实并不神秘（视频录像：13分钟） 1.1 黑客基础知识概述 1.1.1 为什么会受到黑客入侵 1.1.2 全面认识IP地址 1.2 黑客的专用通道：端口 1.2.1 端口的概念与作用 1.2.2 端口分类 1.2.3 查看端口 1.2.4 对IP和端口进行扫描 1.2.5 如何限制端口 1.3 黑客常用的入侵令 1.3.1 Ping命令 1.3.2 Net命令 1.3.3 Telnet命令 1.3.4 FTP命令 1.3.5 Ipconfig命 1.4 可能出现的问题与解决方法 1.5 总结与经验积累 第2章 揭秘扫描、嗅探与欺骗（视频录像：41分钟） 2.1 经典的扫描与反扫描工具 2.1.1 用MBSA检测Windows系统的安全级别 2.1.2 剖析RPC的漏洞扫描 2.1.3 用WebDAVScan扫描个人服务器 2.1.4 用网页安全扫描器查看网页是否安全 2.1.5 防御扫描器追踪的利器：ProtectX 2.2 几款经典的嗅探器 2.2.1 用于捕获数据的Sniffer Pro嗅探器 2.2.2 网络间谍软件CaptureNet 2.2.3 用于局域网嗅探的Iris嗅探器 2.2.4 可实现多种操作的SpyNet Sniffer嗅探器 2.2.5 用于捕获网页内容的“艾菲网页侦探” 2.3 来自“蜜罐”的网络欺骗 2.3.1 极具诱捕功能的“蜜罐” 2.3.2 拒绝恶意接入的“网络执法官” 2.4 可能出现的问题与解决方法 2.5 总结与经验积累 第3章 系统漏洞的入侵与防御（视频录像：4分钟） 3.1 经典的本地提权类漏洞攻防 3.1.1 内核消息处理本地缓冲区溢出漏洞 3.1.2 LPC本地堆溢出漏洞剖析 3.1.3 OLE和COM远程缓冲区溢出漏洞 3.2 Windows系统的用户交互类漏洞 3.2.1 Task Scheduler远程任意代码执行漏洞 3.2.2 GDI+JPG解析组件缓冲区溢出漏洞 3.2.3 压缩文件夹远程任意命令执行漏洞 3.3 Windows系统的远程溢出漏洞 3.3.1 UPnP存在缓冲溢出漏洞 3.3.2 RPC接口远程任意代码可执行漏洞 3.3.3 Messenger服务远程堆溢出漏洞 3.3.4 WINS服务远程缓冲区溢出漏洞 3.3.5 即插即用功能远程缓冲区溢出漏洞 3.4 Windows XP系统漏洞入侵与防御 3.5 对个人电脑实施防护 3.5.1 安装必要的杀毒软件与防火墙 3.5.2 分类设置复杂密码 3.5.3 预防网络病毒与木马 3.5.4 “网络钓鱼”与间谍软件防御 3.5.5 及时备份重要数据 3.5.6 一些必要的安全措施 3.6 可能出现的问题与解决方法 3.7 总结与经验积累 第4章 揭秘木马和间谍软件（视频录像：36分钟） 4.1 捆绑木马和反弹端口木马 4.1.1 熟悉木马的入侵 4.1.2 轻松制作捆绑木马 4.1.3 极易上当的WinRAR捆绑木马 4.1.4 用“网络精灵”木马（NetSpy）实现远程监控 4.1.5 初识反弹端口木马：“网络神偷” 4.2 反弹型木马的经典：“灰鸽子” 4.2.1 生成木马的服务端 4.2.2 木马服务端的加壳保护 4.2.3 把木马植入他人的电脑中 4.2.4 小心别被对方远程控制 4.2.5 “灰鸽子”的手工清除 4.3 全面防范网络蠕虫 4.3.1 网络蠕虫概述 4.3.2 网络蠕虫病毒实例分析 4.3.3 网络蠕虫病毒的全面防范 4.4 自动安装“后门”程序的间谍软件 4.4.1 什么是间谍软件 4.4.2 如何拒绝潜藏的间谍软件 4.4.3 用Spybot揪出隐藏的间谍 4.4.4 间谍广告的杀手：Ad-Aware 4.4.5 对潜藏的“间谍”学会说“不” 4.5 来自微软的反间谍专家 4.5.1 反间谍软件Microsoft Windows Defender 4.5.2 手动扫描查杀间谍软件 4.5.3 设置定时自动扫描 4.5.4 开启对间谍软件的实时监控 4.5.5 附带的特色安全工具 4.6 可能出现的问题与解决方法 4.7 总结与经验积累 第5章 斩断伸向QQ和MSN的黑手（视频录像：30分钟） 5.1 QQ攻防实战 5.1.1 QQ的常用入侵方式 5.1.2 用“QQ登录号码修改专家”和“QQ聊天记录查看器”查看聊天记录 5.1.3 用“QQ掠夺者”盗取本地QQ密码 5.1.4 用“QQ眼睛”在线获取QQ号与密码 5.1.5 疯狂的“QQ机器人”盗号者 5.2 防不胜防的QQ远程盗号 5.2.1 并不友好的强制聊天 5.2.2 进行远程控制的“QQ远控精灵” 5.2.3 使用“QQ狙击手IpSniper”进行探测 5.2.4 不可轻信“QQ密码保护”骗子 5.2.5 防范QQ密码的在线破解 5.3 QQ信息炸弹与病毒 5.3.1 用“QQ狙击手IpSniper”进行信息轰炸 5.3.2 在对话模式中发送消息炸弹 5.3.3 向指定的IP地址和商品号发送消息炸弹 5.4 斩断伸向QQ与MSN的黑手 5.4.1 QQ密码破译预防 5.4.2 预防IP地址被探测 5.4.3 Msn Messenger Hack盗号揭秘 5.4.4 用Messen Pass查看本地密码 5.5 可能出现的问题与解决方法 5.6 总结与经验积累 第6章 浏览器的恶意入侵与防御 6.1 网页恶意入侵与防御 6.1.1 剖析利用网页实施的入侵 6.1.2 剖析Office宏删除硬盘文件的入侵 6.1.3 剖析ActiveX对象删除硬盘文件的入侵 6.1.4 防止硬盘文件被删除 6.2 最让人心有余悸的IE炸弹 6.2.1 IE炸弹入侵的表现形式 6.2.2 IE死机共享炸弹的入侵 6.2.3 IE窗口炸弹的防御 6.3 IE执行任意程序入侵与防御 6.3.1 利用chm帮助文件执行任意程序的攻击 6.3.2 chm帮助文件执行任

第一图书网, tushu007.com

意程序的攻击防范 6.3.3 利用IE执行本地可执行文件进行入侵 6.4 可能出现的问题与解决方法 6.5 总结与经验积累 第7章 代理与日志的清除（视频录像：38分钟） 7.1 跳板与代理服务器 7.1.1 代理服务器概述 7.1.2 跳板概述 7.1.3 代理服务器的设置 7.1.4 制作一级跳板 7.2 代理工具的使用 7.2.1 代理软件CCProxy中的漏洞 7.2.2 代理猎手的使用技巧 7.2.3 代理跳板建立全攻略 7.2.4 利用SocksCap32设置动态代理 7.2.5 用MultiProxy自动设置代理 7.3 巧妙清除日志文件 7.3.1 手工清除服务器日志 7.3.2 用清理工具清除日志 7.4 恶意进程的追踪与清除 7.4.1 理解进程与线程 7.4.2 查看、关闭和重建进程 7.4.3 管理隐藏进程和远程进程 7.4.4 杀死自己机器中的病毒进程 7.5 可能出现的问题与解决方法 7.6 总结与经验积累 第8章 远程控制技术大集合（视频录像：33分钟） 8.1 修改注册表实现远程监控 8.1.1 通过注册表开启终端服务 8.1.2 突破Telnet中的NTLM权限认证 8.2 基于认证的远程入侵 8.2.1 IPC$入侵与防御 8.2.2 Telnet入侵与防御 8.3 端口监控与远程信息监控 8.3.1 用SuperScan监控端口 8.3.2 URLy Warning实现远程信息监控 8.4 远程控制技术实战 8.4.1 用WinShell自己定制远程服务端 8.4.2 用QuickIP实现多点控制 8.4.3 可实现定时抓屏的“屏幕间谍” 8.4.4 用“魔法控制2007”实现远程控制 8.5 经典的远程控制工具pcAnywhere 8.5.1 安装pcAnywhere程序 8.5.2 设置pcAnywhere的性能 8.5.3 用pcAnywhere进行远程控制 8.6 可能出现的问题与解决方法 8.7 总结与经验积累 第9章 留后门与清脚印（视频录像：3分钟） 9.1 给自己的入侵留下后门 9.1.1 手工克隆账号 9.1.2 命令行方式下制作后门账号 9.1.3 克隆账号工具 9.1.4 用Wollf留下木马后门 9.1.5 SQL后门 9.2 清除登录服务器的日志信息 9.2.1 使用批处理清除远程主机日志 9.2.2 通过工具清除事件日志 9.2.3 清除WWW和FTP日志 9.3 清除日志工具elsave和CleanIISLog 9.3.1 日志清除工具elsave的使用 9.3.2 日志清除工具CleanIISLog的使用 9.4 可能出现的问题与解决方法 9.5 总结与经验积累 第10章 黑客入侵实战演练 10.1 网络欺骗入侵演练 10.1.1 入侵原理 10.1.2 入侵演练 10.2 口令猜测入侵演练 10.2.1 入侵原理 10.2.2 入侵演练 10.3 缓冲区溢入侵演练 10.3.1 入侵原理 10.3.2 入侵演练 10.4 可能出现的问题与解决方法 10.5 总结与经验积累 第11章 黑客入侵防范技术（视频录像：30分钟） 11.1 驱逐间谍软件 11.1.1 用Ad-aware软件驱逐间谍 11.1.2 反间谍专家 11.2 木马清除的好帮手 11.2.1 用Windows进程管理器管理进程 11.2.2 用“超级兔子”清除木马 11.2.3 使用Trojan Remover清除木马 11.3 维护系统安全的360安全卫士 11.3.1 查杀恶评软件与病毒 11.3.2 系统全面诊断 11.3.3 修复IE浏览器和LSP连接 11.3.4 清理使用痕迹 11.4 拒绝网络广告 11.4.1 过滤弹出式广告的浏览器傲游Maxthon 11.4.2 过滤网络广告的广告杀手Ad Killer 11.4.3 广告智能拦截的利器：Zero Popup 11.4.4 使用MSN的MSN Toolbar阻止弹出广告 11.5 可能出现的问题与解决方法 11.6 总结与经验积累 第12章 备份升级与数据恢复（视频录像：13分钟） 12.1 数据备份升级概述 12.1.1 什么是数据备份 12.1.2 系统的补丁升级 12.2 使用、维护硬盘和数据恢复 12.2.1 使用和维护硬盘的注意事项 12.2.2 数据恢复工具EasyRecovery和FinalData 12.3 可能出现的问题与解决方法 12.4 总结与经验积累 第13章 打好网络安全防御战（视频录像：40分钟） 13.1 建立系统漏洞防御体系 13.1.1 检测系统是否存在可疑漏洞 13.1.2 如何修补系统漏洞 13.1.3 监视系统的操作进程 13.1.4 防火墙安装应用实例 13.2 几款杀毒软件的介绍 13.3 可能出现的问题与解决方法 13.4 总结与经验积累

第一图书网, tushu007.com

章节摘录

第1章 黑客其实并不神秘随着互联网对人们日常生活影响的深入，人们的生活已经很难离开网络。
与此同时，网络的安全问题也引起了人们的高度关注。
而黑客则是网络世界中很神秘的一类人，他们有时会义务去维护网络的安全，有时却又以网络破坏者的形象出现。
本章将揭开黑客的神秘面纱，并对与他们有关的常用知识进行初步介绍。
1.1　黑客基础知识概述黑客（Hacker）的原意是指那些精通操作系统和网络技术，并利用其专业知识编制新程序的人。
但到了今天，黑客一词已被用于泛指那些专门利用计算机搞破坏或恶作剧的家伙，对这些人的正确英文叫法是Cracker，故又称“骇客”。
这些人往往具有非凡的计算机技术和网络知识，除通过正当手段来对他人的计算机进行物理性破坏和重装系统外，他们还可以通过网络来操作其他人的计算机，例如，将别人的计算机当跳板来盗取另一台计算机内的文件、破坏系统、格式化磁盘、监视他人计算机、偷窥他人隐私、远程控制他人计算机、入侵攻击他人或公司的服务器等。
1.1.1 为什么会受到黑客入侵其实，许多时候，大多数黑客进行攻击的理由都很简单，大体存在如下几个方面的原因。
（1）想要在别人面前炫耀一下自己的技术，例如进入心仪女孩的机器上去修改一个文件或目录名，算是打个招呼，不但给其一个惊喜，也会让她对自己更加崇拜。
（2）看不惯一些人的做法，可又不便当面指责，于是攻击他的电脑，更有甚者获得他的隐私，在适当的时机揭其老底，令其难堪。
（3）好玩、恶作剧、练功。
这是许多人，其中包括学生，入侵或破坏网络的主要原因，除了有练功的效果外，同时还有一种网络探险的刺激。
（4）窃取数据。
偷取入侵的主机硬盘中的文件或各种网上密码之后，从事各种商业应用活动，甚至恶意偷窃银行存款等。
（5）抗议与宣示。
这是敌对国、敌对势力之间最常出现的黑客行为，例如2001年5月中美黑客大战，两国的黑客互相攻击对方网站，双方均有数千计的网站遭到攻击，轻者被篡改主页面，严重者则整个系统遭到毁灭性的打击。
1.1.2　全面认识IP地址在网络上，只要利用IP地址都可以找到目标主机。
因此，如果想要攻击某个网络主机，首先就要确定该目标主机的域名或者IP地址。
所谓IP地址就是一种主机编址方式，给每个连接在Internet上的主机分配一个32位（bit，比特）地址，也称为网际协议地址。
按照TCP／IP（Transport Conlrol Protocol／Internet Protocol，传输控制协议mltenlet协议）协议的规定，IP地址用二进制来表示，每个IP地址长32位，位换算成字节就是4个字节。
例如一个采用二进制形式的IP地址是00001010000000000000000000000001，这么长的地址人们处理起来就会很费劲，为了方便使用，IP地址经常被写成十进制的形式，中间使用符号“.”分为4个不同的十进制数，这样就可以用XXX.XXX.XXX.XXX的形式来表示，每组XXX代表小于等于255的十进制数，例如l92.168.38.6。
IP地址的这种表示方法称为“点分十进制表示法”，这显然比二进制的1或0容易记忆。
IP地址是如何划分的呢？
在互联网中的每个接口有一个唯一的IP地址与其对应，该地址并不是平面形式的地址空间，而是具有一定的结构，一般情况下，IP地址可以分为5大类，如图1.1所示。
在A类中，第1段为网络位，后3段为主机位，其范围为1——-127，例如127.255.255.255；在B类中，前两段是网络位，后两段为主机位，其范围为128～191，例如191.255.255.255；在C类中，前3段为网络位

，后1段为主机位，其范围为l92～223，例如223.255.255.255；D类地址用于多播，也叫做组播地址，在互联网上不能作为接点地址使用，其范围为224～239，例如239.255.255.255；E类地址用于科学研究，也不能在互联网上使用，其范围为240——-254。
注意：全0和全1的口地址禁止使用，因为全0代表本网络，而全1是广播地址（在CISCO上可以使用全O地址）。
一般情况下，常用的是A、B、C这3类地址。
1.2 黑客的专用通道：端口随着网络技术的发展，原来物理上的端口（例如，鼠标、键盘、网卡、显卡等输入／输出接口）已不能满足网络通信的要求，而TCP／IP协议则被集成到了操作系统的内核中，这就相当于在操作系统中引入了一种新的输入/输出接口技术。
因为在TCP／IP协议中引入了一种被称为Socket的应用程序接口技术，这就使得一台计算机可以通过软件方式与任何一台具有Socket接口的计算机进行通信。
1.2.1 端口的概念与作用端口（port）可以认为是计算机与外界通讯交流的出口。
其中硬件领域的端口又称接口，例如，USB端口、串行端口等。
软件领域的端口一般指网络中面向连接服务和无连接服务的通信协议端口，是一种抽象的软件结构，包括一些数据结构和I／O（基本输入／输出）缓冲区。
端口是传输层的内容，是面向连接的，它们对应着网络上常见的一些服务。
这些常见的服务可划分为使用TCP端口（面向连接，如打电话）和使用UDP端口（无连接，如写信）两种。
在网络中可以被命名和寻址的通信端口是一种可分配资源，由网络OSI（Open SystemInterconnection Reference Model，开放系统互联参考模型）协议可知，传输层与网络层的区别是传输层提供进程通信能力，网络通信的最终地址不仅包括主机地址，还包括可描述进程的某种标识。
所以，当应用程序（调入内存运行后一般称为进程）通过系统调用与某端口建立连接（Bindin9，绑定）后，传输层传给该端口的数据都被相应的进程所接收，相应进程发给传输层的数据都从该端口输出。
1.2.2　端口的分类在网络技术中，端口大致有两种意思：一是物理意义上的商品，例如，集线器、交换机、路由器等用于连接其他网络设备的接口；二是逻辑意义上的端口，一般指TCP／IP协议中的端口，范围为0～65535，例如，浏览网页服务的80端口，用于FTP服务的21端口等。
逻辑意义上的端口有多种分类标准，常见的分类标准有如下两种。
1.按端口号分布划分按端口号分布划分可以分为公认端口、注册端口以及动态和／或私有端口等。
公认端口公认端口（WeU Known Ports）也称为常用端口，端口号为0～1023，它们紧密地绑定于一些特殊的服务。
通常，这些端口的通信明确地表明了某种服务协议，不可再重新定义它的作用对象。
例如，21端口分配给FTP服务；23号端口分配给Telnet服务专用；25号端口分配全SMTP（简单邮件传输协议）服务；80端口是HTTP通信使用的；135端口分配给RPC（远程过程调用）服务等，通常不会被像木马这样的黑客程序利用。
注册端口注册端口（RegisteredPorts）的端口号为1024——49151，它们松散地绑定一些服务，也即有许多服务绑定于这些端口，这些端口同样用于许多其他目的，并且多数没有明确定义对象，不同的程序可以根据需要自己定义。
记住这些常见程序端口，在木马程序的防护和查杀上非常有必要。
动态和／或私有端口动态和／或私有端口（Dynamic and／or Private Ports）的端口号为49152～65535，理论上不应该把常用服务分配在这些端口上，但实际上有些较为特殊的程序，特别是一些木马程序就非常喜欢使用这些端口，因为这些端口常常不会引起人们的注意，容易隐蔽。
2.按协议类型划分根据所提供的服务方式，端口又可分为TCP端口和UDP端口两种。
一般直接与接收方进行的连接方式，大多是采用TCP协议：如果只是把信息放在网上发布出去而不去关心信息是否到达，也就是无连接方式，这种方式则大多采用UDP协议。
使用TCP协议的常见端口主要有如下几种。
FTP定义了文件传输协议，使用21端口。

第一图书网, tushu007.com

某计算机开通了FTP服务便启动了文件传输服务，下载文件和上传主页都要用到FTP服务。
Telnet一种用于远程登录的端口，用户可以以自己的身份远程连接到计算机上。
通过这种端口可提供一种基于DOS模式的通信服务，例如支持纯字符界面BBS的服务器会将23端口打开，以对外提供服务。
SMTP现在很多邮件服务器都是使用这个简单邮件传送协议来发送邮件的。
例如常见免费邮件服务中使用的就是此邮件服务端口，所以在电子邮件设置中经常会看到有SMTP端口设置栏，服务器开放的是25号端口。
POP3POP3协议用于接收邮件，通常使用110端口。
只要有相应使用POP3协议的程序（例如Outlook等），即可直接使用邮件程序收到邮件（例如使用l26邮箱的用户就没有必要先进入126网站，再进入自己的邮箱来收信了。
）

第一图书网, tushu007.com

<<狙击黑客>>

编辑推荐

《狙击黑客:黑客攻防技术见招拆招》内容丰富，图文并茂，深入浅出，适用于广大网络爱好者，同时可作为一本速查手册，适用于从事网络安全的人员及网络管理员。

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