第一图书网, tushu007.com

<<防毒防黑全攻略>>

图书基本信息

书名：<<防毒防黑全攻略>>

13位ISBN编号：9787030134561

10位ISBN编号：7030134567

出版时间：2004-8-1

出版时间：科学出版社

作者：程秉辉,John Hawke

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

<<防毒防黑全攻略>>

内容概要

本书对Windows下的各种可能出现的漏洞进行彻底的整理，加入了最新的黑客技巧与攻防，提供更新、更方便的各种防黑防毒的操作，希望能帮助你实现彻底安全的个人电脑环境。

内容包括：利用仿真IP或隐藏IP来防止黑客入侵，如何针对自己的计算机或服务器设计专属防火墙，检查与判断是否正有黑客连接到我的计算机，Windows入侵的完全阻挡防护，如何找出与干掉隐藏在您计算机中的木马程序，电子邮件、Java、ActiveX、批处理文件的完全防护，IE被强迫更改、快速查找与修补系统与各类软件的漏洞，从各种安全日志 (log) 中判断是否有黑客或病毒入侵，如何防止安全日志被黑客删除或修改，追踪黑客IP的讨论与研究，蠕虫病毒、拒绝服务攻击、分布式攻击讨论与研究。

本书适合作为所有计算机用户的安全手册，同时对网络管理员和致力于网络安全的开发人员有很大参考价值。

本书配套光盘包含全球各地IP地址详细列表、端口列表以及NetInfo、Spybot - Search & Destroy、Magic Mail Monitor等各种必备网络安全工具。

第一图书网, tushu007.com

<<防毒防黑全攻略>>

书籍目录

Part 1　病毒入侵观念、下手目标与黑客行为（Internet Concept and Hacker, Virus Intrusion）　Internet世界的基本原理　端口的角色与功能　黑客与病毒入侵或攻击的目标　病毒的定义与说明　讨论与研究　Q1：黑客或病毒通常使用那些方法来入侵或攻击一般上网的个人电脑？
如何针对这些方法来进行围堵与防御来达到有效防护？
Q2：黑客或病毒通常使用那些方法来入侵或攻击网站与各类型服务器？
如何针对这些方法来进行围堵与防御来达到有效防护？
Part 2　事前预防与状况研判　Q3：如何对一般上网电脑进行有效的预防措施，以防止黑客或病毒的入侵或破坏？
Q4：有那些防护措施是一般上网的个人电脑必需要做到的？
Q5：一般上网个人电脑的防黑防毒流程是如何？
Q6：一般上网电脑如何将自己上网的IP地址隐藏起来，使黑客无法找到以避免被入侵或攻击？
Q7：有那些方式可以将自己的IP地址隐藏，不让别人找到？
或找起来很困难？
Q8：有那些方法可以架构出仿真IP地址来上网？
Q9：一般上网电脑如何使用仿真IP的方式来避免黑客的直接入侵与攻击？
Q10：仿真IP一定要使用路由器（Router）或集线器（HUB）才能做到吗？
Q11：如何以最低廉的工本来架构出仿真 IP？
Q12：一定要使用DHCP才能让网络中的每台电脑都有IP地址上网吗？
Q13：如何监控我的电脑中各网络程序的进出状况，并针对可疑的程序进行拦截查看？
Q14：如何对可疑的程序进行网络存取时进行阻挡，不让它进行？
Q15：可以让我来决定那些程序可以进行网络存取，那些不行？
Q16：如何对没有必要或未使用的 Internet 协议（Protocol）与端口进行阻挡设置？
Q17：如何依照自己的网络状况与需求来制定专属的防火墙规格？
Q18：如何对已知木马程序所用的端口进行阻挡？
Q19：我有使用网络防护程序（或防火墙软件），经常不断出现某个端口被扫描（或要连接）的信息，实在烦不胜烦，要如何有效阻挡而且不会弹出信息来烦我？
Q20：如何查看与判断目前是否正有黑客连接到我的电脑？
Q21：如何查看目前我的电脑中有那些程序正在上网连接？
与那个网站或IP地址进行连接？
Q22：如何关闭目前正在进行的可疑连接，并干掉该连接的程序？
Part 3　Windows 的黑客病毒入侵防护（Hacker and Virus Defense for Windows）　入侵基本原理与对象　黑客或病毒通过 Windows 的入侵流程　端口 139 的防护　磁盘共享防护　默认共享漏洞防护　RPC 防护　FTP 防护　Telnet 防护　终端机服务防护　漏洞修补与防护　电子邮件防护　死机攻击防护　恶意信息防护　讨论与研究　Q23：如何关闭端口139 彻底杜绝黑客利用此管道入侵？
Q24：防止黑客通过端口139 入侵 Windows，有那几道防御措施？
Q25：我需要与其它电脑进行网络连接，所以必须打开端口139，这样要如何防止黑客入侵呢？
Q26：我的电脑必须打开磁盘共享，如何有效防止黑客入侵？
Q27：如何防止黑客利用项病毒将我的磁盘设置成共享或设置成可读写？
Q28：如何防止黑客利用项病毒将磁盘共享密码设置成不必密码就可进入？
Q29：如何有效防止黑客猜中磁盘共享密码？
Q30：如何修补 Win9x 与 WinME 的资源共享密码漏洞？
Q31：如何防止黑客在 WinNT、Win2K、WinXP 电脑中创建最高权限帐户？
Q32：什么是默认共享漏洞？
它的原理是什么？
Q33：每次启动进入 Windows 系统都会自动打开默认共享，如何始终关闭它来防止黑客入侵？

第一图书网, tushu007.com

Q34：如何防止黑客将默认共享打开？
Q35：为什么电脑有 Telnet 提供服务，我却没发现？
Q36：如何查看我的电脑是否有提供 Telnet 服务？
Q37：如何防止黑客打开我电脑的 Telnet 服务？
Q38：如何彻底关闭我电脑的 Telnet 服务，完全杜绝黑客使用此方式入侵？
Q39：为何我在上网时经常出现奇怪的广告或垃圾信息窗口？
Q40：如何让自己的电脑完全不再收到 Internet 上任意散发的垃圾信息？
Q41：我使用 Win9x（或 WinME），如何才能快速的关闭或打开磁盘共享？
有什么更好的方法？
Q42：我仅一片网卡，上网或连接到局域网时都要将网络线拔来拔去，实在很麻烦，有什么好的解决方式？
Q43：如何对 Windows 系统的漏洞进行修补防护？
Q44：如何在连接网络时将重要文件夹隐藏，万一不幸被黑客入侵才不致造成重大伤害或被偷取重要数据？
Q45：如何防止黑客利用 at 命令运行你电脑中的各种程序文件？
如何关闭 at 远程运行命令？
Part 4　木马、后门与病毒的防护、搜索与摧毁（Search and Destroy for Trojan、Back Door Programs and Virus）　Q46：木马、后门或跳板程序是什么？
与病毒有何关系？
Q47：木马、后门或跳板程序可以帮黑客进行那些工作？
Q48：木马病毒的防护方式为何？
Q49：如何有效的预防被黑客植入木马病毒？
Q50：黑客通常使用那些方式将木马病毒植入他人电脑或服务器中？
Q51：要如何有效测试与查看下载的文件是没有包含各种木马病毒或跳板程序？
Q52：我每次下载文件后都要使用防毒软件查看，如何设置为下载完成后就自动查看？
Q53：我下载的文件是压缩文件，这样可以查看出其中是否有木马病毒或跳板程序？
Q54：如何查看或找出你的电脑是否有被植入木马病毒或跳板程序，然后将它彻底干掉？
Q55：使用扫毒软件或网络防御程序查看各类木马病毒，要注意那些地方？
Q56：若扫毒软件或网络防御程序有发现木马病毒，要怎样处理最好？
Q57：要将扫毒软件或网络防御软件常驻吗？
如何使用才会有最佳的效果，也不影响系统性能？
Q58：被植入的木马病毒通常藏在那些地方？
Q59：木马病毒有那些方法设置一进入 Windows 就自动运行？
Q60：如何判断与找出隐藏在注册表（Registry）或系统服务中设置运行的木马病毒？
Q61：如何查看目前正在运行的 EXE 或 DLL 程序，找出可疑的程序将它干掉？
Q62：为何扫毒软件或我自己操作都无法将 DLL 木马病毒从电脑中卸载？
Q63：经过伪装或改变容貌的木马程序要如何辨识出来，然后将它彻底终结掉？
Part 5　浏览器与电子邮件的入侵防护（Virus and Hacker Defense for E-Mail Programs and Browser）
Q64：电子邮件通常会受到那些方式黑客或病毒的入侵与攻击？
如何各个击破？
Q65：如何避免受到邮件炸弹或一堆信件的攻击？
Q66：受到邮件炸弹或一堆信件的攻击时如何脱困？
Q67：若有人发一大堆的信件给我，要如何解决？
Q68：有那些方法可以防止与避免被他人截取信件？
Q69：若发现被他人截取信件要如何进行补救措施以减少可能的损害？
Q70：如何查看信件中所附加的文件中是否有木马、病毒程序或各类破坏项、批处理文件？
Q71：如何对信件中的 Java 恶意源码进行防护？

第一图书网, tushu007.com

Q72：如何避免受到窗口炸弹或其它 Java 恶意源码的攻击？
Q73：我受到窗口炸弹的攻击，一打开信件程序就会不断的冒出许多窗口，根本无法收信与寄信，要如何解决？
Q74：如何对信件中的 ActiveX 恶意源码进行防护？
Q75：通常黑客利用 ActiveX 程序进行那些恶意行为？
Q76：如何避免受到 ActiveX 恶意源码的攻击？
Q77：如何对信件中夹带的批处理文件进行判断与防护？
Q78：为何防毒软件或网络防护程序无法找出批处理文件病毒？
Q79：为什么所有程序都无法运行？
Q80：控制面板中的所有项目都无法运行，而且还出现未找到的错误信息，如何解决？
Q81：为什么我的注册表编辑器不可用？
如何解决？
Q82：为什么在 "开始" 菜单中的 "运行" 不见了？
如何恢复？
Q83：通常 IE 浏览器会受到那些方式的黑客攻击或病毒入侵？
如何防护？
有什么彻底有效的解决方式？
Q84：我的 IE 每次打开动自动连接到某个网站，无法改回来，要如何解决？
Q85：我的 IE 主页与上方标题被改成某个网站，无法改回来或改回来后又被改掉，要怎么办？
Q86：我的 IE 有许多功能被关闭（如右键菜单、Internet 选项、高级设置、查看信件原始码…都不可用），如何打开？
Q87：IE 工具栏被加入指向某网站的按钮，要如何将它取去掉？
Q88：如何找出与干掉我的电脑中被某些网站植入的可恶程序、Cookies 或项？
Q89：如何提高 IE 浏览器发送数据的安全性？
Q90：如何更新 IE 浏览器到 128 位的加密版本？
Q91：如何防范木马程序、病毒或破坏程序利用邮件程序或浏览器漏洞进行入侵？
Q92：如何快速对 IE 或 Outlook 漏洞进行修补？
Part 6　网络服务器的黑客病毒防护（Virus and Hacker Defense for Internet服务器）　入侵或攻击方式　安全与防护　找出幕后的黑手（黑客的追踪与研究）　Q93：什么是蠕虫病毒？
它有何破坏与影响？
Q94：蠕虫病毒是如何寄生、扩散与攻击？
如何有效防护它？
Q95：什么是拒绝服务攻击？
它会造成那些影响？
Q96：拒绝服务攻击（DoS，Denial of Service）通常有那些方式？
各有何优缺点？
基本原理为何？
Q97：什么是分布式攻击（DDoS）？
它与一般拒绝服务攻击（DoS）有何不同？
Q98：什么数据包溢出死机攻击？
如何修补它？
Q99：什么是设备命令死机漏洞？
如何修补它？
Q100：什么是 SMB 缓冲区溢出漏洞？
如何修补它？
Q101：如何对自己的服务器进行测试查看，找出可能的漏洞？
Q102：如何查找 Windows 系统、IIS、Apache、SQL 服务器是否有新的漏洞出现？

第一图书网, tushu007.com

如何修补？
Q103：如何设置 Win2K 或 WinXP 系统的防火墙功能？
Q104：如何为我的服务器打造专属的防火墙？
Q105：如何从安全记录中判断是否有黑客或病毒入侵？
Q106：如何查看与判断系统记录、任务计划记录、IIS 记录？
Q107：如何判断安全记录是否被黑客删除？
Q108：如何防止安全记录被黑客删除或修改？
Q109：如何追踪与找出黑客的所在，进一步找出黑客是谁？
Q110：黑客有那几种方式隐藏自己的IP来进行入侵？
附录　附录A　端口列表　附录B　TCPView　附录C　NetInfo　附录D　SyGate Personal Firewall　附录E　TaskInfo　附录F　StartupCPL　附录G　Magic Mail Monitor　附录H　FolderShield　附录I　Spybot - Search & Destroy　附录J　N-Stealth　附录K　GetRight

第一图书网, tushu007.com

<<防毒防黑全攻略>>

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