

<<防黑缉毒擒木马之绝命追杀>>

图书基本信息

书名：<<防黑缉毒擒木马之绝命追杀>>

13位ISBN编号：9787030168542

10位ISBN编号：7030168542

出版时间：2006-4

出版时间：科学出版社

作者：程秉辉

页数：506

字数：584000

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>

<<防黑缉毒擒木马之绝命追杀>>

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，加入了大量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。

本书畅销两岸三地数年，现技术全面更新出版。

主要内容包括：利用仿真IP或隐藏IP来防止黑客入侵，设置个人防火墙，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，找出并干掉隐藏在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、快速查找与修改系统与各类软件的漏洞，从各种安全日志中判断是否有黑客或病毒入侵，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。

另外，对最新的无线网络防护手段进行了详细讲解并给出具体操作。

本书可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。

本书光盘中包含各种必备网络安全工具。

<<防黑缉毒擒木马之绝命追杀>>

书籍目录

Part 1 病毒入侵观念、下手目标与黑客行为 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哪些方法来入侵或攻击一般上网电脑的？

如何针对这些方法来进行围堵与防御，以有效地防护我们的上网电脑？

Q2 黑客或病毒通常使用哪些方法来入侵或攻击网站与各类型的服务器？

如何针对这些方法进行围堵与防御，以达到有效防护的目的？

Part 2 IP、端口防护与架构个人防火墙（含无在线网防护） Q3 如何对一般上网电脑进行有效地预防，以防止黑客或病毒的入侵或破坏？

Q4 一般上网电脑必须采取哪些防护措施？

Q5 一般上网电脑的防黑防毒流程是什么？

Q6 如何隐藏一般电脑的IP地址，避免黑客找到我电脑的IP地址、进行入侵或攻击？

Q7 有哪些方式可以将一般电脑的IP地址隐藏，不让别人找到？或找起来很困难？

Q8 有哪些方法可以架构出仿真IP地址？

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）才能实现吗？

Q11 如何用最低的成本架构出仿真IP？

Q12 必须使用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状态，并针对可疑的程序进行拦截检查？

Q14 如何阻挡正在进行存取的可疑的网络程序，不让它继续进行？

Q15 可以让我决定哪些程序可以进行网络存取，哪些程序不能进行网络存取吗？

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 如何根据自己的网络状况与需求来设置个人防火墙？

Q18 如何对已知木马程序所使用的端口进行阻挡？

Q19 我使用了网络防护程序（或防火墙软件），经常出现某个端口被扫描（或连接）的信息，实在很烦人，应该如何有效阻挡它而且不再弹出信息来烦我？

Q20 如何检查与判断当前是否有黑客正在连接到我的电脑？

Q21 如何检查当前我的电脑中有哪些程序正在上网连接？

与哪个网站或IP地址进行连接？

Q22 如何关闭当前正在进行的可疑连接，并关闭与该连接对应的程序？

Q23 黑客是如何偷用无线网络的？

是什么原因让无线网络门户大开？

Q24 黑客入侵无线网络后会造成哪些问题？

Q25 如何有效防范黑客偷用我的无线网络？

有哪些防护措施？

各有何缺点？

如何补救？

Part 3 Windows 的黑客病毒入侵防护 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 Q26 如何关闭端口139，彻底杜绝黑客利用此端口入侵我们的电脑？

Q27 防止黑客通过端口139入侵Windows系统，有哪几道防御措施？

Q28 我需要与其他电脑进行网络连接，所以必须打开端口139，这样该如何防止黑客入侵呢？

Q29 我的电脑必须打开磁盘共享，该如何有效防止黑客入侵？

Q30 如何防止黑客利用注册表将我的磁盘设置成共享或可读写？

<<防黑缉毒擒木马之绝命追杀>>

Q31 如何防止黑客利用注册表将磁盘共享密码设置成不需输入密码就可进入？

Q32 如何有效地防止黑客猜中磁盘共享密码？

Q33 如何修补Windows 9x/ME的资源共享密码漏洞？

Q34 如何防止黑客在Windows NT/2000/XP系统中创建最高权限帐户？

Q35 什么是默认共享漏洞？

它的原理是什么？

Q36 Windows系统每次启动时都会自动打开默认共享，如何始终关闭它来防止黑客入侵？

Q37 如何防止黑客将默认共享打开？

Q38 为什么我的电脑提供了Telnet服务，我却没发现？

Q39 如何检查我的电脑是否有提供Telnet服务？

Q40 如何防止黑客打开Telnet服务？

Q41 如何彻底关闭Telnet服务，杜绝黑客使用此方式入侵？

Q42 为何我在上网时经常遇到奇怪的广告或垃圾信息窗口？

Q43 如何让自己的电脑完全阻止Internet上任意散发的垃圾信息？

Q44 我使用的是Windows 9x/ME，如何才能快速地关闭或打开磁盘共享？

有什么更好的方法？

Q45 我仅一块网卡，上网或连接到局域网时都要将网线拔来拔去，实在很麻烦，有什么好的解决方式？

Q46 如何对Windows系统的漏洞进行修补？

Q47 如何在连接网络时将重要文件夹隐藏或将重要文件加锁，万一被黑客入侵才不会造成重大伤害或重要数据被偷取？

Q48 如何防止黑客利用at远程运行命令运行你电脑中的各种程序？

如何关闭at命令？

185Part 4 木马、后门与病毒的防护、搜索与摧毁 Q49 木马、后门或跳板程序是什么？与病毒有何关系？

Q50 木马、后门或跳板程序可以帮黑客进行哪些工作？

Q51 防卸木马病毒入侵的方式都由哪些？

Q52 如何有效地预防被黑客植入木马病毒？

Q53 黑客通常使用哪些方式将木马病毒植入他人的电脑或服务中？

Q54 如何有效测试与检查下载的文件没有包含各种木马病毒、恶意或间谍程序？

Q55 我每次下载文件后都要使用杀毒软件检查，如何设置为下载完成后就自动检查？

Q56 我下载的文件是压缩文件，这样可以检查出其中是否有木马病毒、恶意或间谍程序吗？

Q57 如何检查或找出你的电脑中是否被植入了木马病毒或跳板程序，将它彻底干掉？

Q58 使用杀毒软件或网络防御程序检查各类木马病毒，要注意哪些地方？

Q59 如果杀毒软件或网络防御程序发现了木马病毒，应该如何处理最好？

Q60 要将杀毒软件或网络防御软件常驻吗？

如何使用才有最佳的效果，也不影响系统性能？

Q61 被黑客植入的木马程序都藏匿在哪些地方？

如何找出来砍头？

Q62 木马病毒使用哪些方法设置一进入Windows就自动运行？

Q63 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？

Q64 如何检查正在运行的.exe或.dll程序，找出可疑的程序将它干掉？

Q65 为何杀毒软件或我自己手动操作都无法将.dll木马病毒从电脑中卸载？

Q66 经过伪装或易容的木马程序如何才能辨识出来，然后将它彻底干掉？

Part 5 浏览器与电子邮件的入侵防护 Q67 电子邮件通常会受到黑客或病毒的哪些方式的入侵与攻击？如何各个击破？

Q68 如何避免受到邮件炸弹或一堆邮件的攻击？

<<防黑缉毒擒木马之绝命追杀>>

- Q69 受到邮件炸弹或一堆邮件的攻击时如何脱困？
- Q70 如果有人发一大堆的邮件给我，该如何解决？
- Q71 有哪些方法可以防止与避免邮件被他人截取？
- Q72 若发现邮件被他人截取，要采取什么样的补救措施以减少可能的损害？
- Q73 如何查看电子邮件的附件中是否有木马、病毒程序或各类具有破坏性的注册表文件和批处理文件？
- Q74 如何对邮件中的Java恶意源代码进行防护？
- Q75 如何避免遭到窗口炸弹或其他Java恶意源代码的攻击？
- Q76 我遭到了窗口炸弹的攻击，一打开邮件程序就会不断地冒出许多窗口，根本无法收信与寄信，该如何解决？
- Q77 如何对邮件中的ActiveX恶意源代码进行防护？
- Q78 通常黑客利用ActiveX程序进行哪些恶意行为？
- Q79 如何避免遭到ActiveX恶意源代码的攻击？
- Q80 如何对邮件中夹带的批处理文件进行判断与防护？
- Q81 为何杀毒软件或网络防护程序无法找出批处理文件病毒？
- Q82 如何查出某一封电子邮件是从哪个国家的哪个地区寄出来的？
- Q83 如何查出某个邮件地址是在哪个国家或哪个地区？
- Q84 如何查出寄件者的寄送邮件时的IP地址？
- Q85 为什么所有程序都无法运行？
- Q86 控制面板中的所有项目都无法运行，而且还出现未找到文件的错误信息，如何解决？
- Q87 为什么我的注册表编辑器不可用？
- 如何解决？
- Q88 为什么在 菜单中的 不见了？
- 如何恢复？
- Q89 通常浏览器会受到黑客或病毒的哪些攻击和入侵方式？
- 如何防护？
- 有什么彻底有效的解决方式？
- Q90 什么是网页钓鱼法（Phishing）？
- 黑客如何利用它来窃取各种帐户与密码？
- 如何防护？
- Q91 如何借助网站的相关信息来判断是否为钓鱼的假网页？
- Q92 我的IE每次打开时都自动连接到某个网站，无法改回来，该如何解决？
- Q93 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又被改回去，该怎么办？
- Q94 我的IE有许多功能被关闭（如右键菜单、Internet选项、高级设置、查看邮件源文件等都不可用），如何打开？
- Q95 在IE工具栏中加入了指向某网站的按钮，该如何将它去掉？
- Q96 如何找出与干掉藏匿在我的电脑中偷改IE各项设置的可恶程序？
- Q97 什么是间谍或恶意源代码？
- 会造成哪些伤害与影响？
- Q98 如何找出并干掉电脑中被某些网站植入的恶意源代码、间谍程序、Cookies或注册项？
- Q99 如何管理、判断电脑中已存在的Cookies信息？
- Q100 当有Cookies要写入到电脑中时，可以让我决定是否保存吗？
- 该怎么做？
- Q101 恶意或间谍防护软件有哪些不足之处？
- 如何补其不足？
- Q102 如何对任何软件（特别是共享软件或免费软件）的可疑网络连接进行判断与阻挡？
- Q103 如何提高IE浏览器发送数据的安全性？

<<防黑缉毒擒木马之绝命追杀>>

Q104 如何降低浏览器数据包被破解的概率？

Q105 如何升级IE浏览器到128位的加密版本？

Q106 如何防止木马程序、病毒或破坏程序利用邮件程序或浏览器漏洞进行入侵？

Q107 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）

Q108 什么是蠕虫病毒？

它有何破坏与影响？

Q109 蠕虫病毒是如何寄生、扩散与攻击的？

如何有效防护它？

Q110 什么是拒绝服务攻击？

它会造成哪些影响？

Q111 拒绝服务攻击（DoS，Denial of Service）通常有哪些方式？

各有何优缺点？

基本原理为何？

Q112 什么是分布式攻击（DDoS）？

它与一般拒绝服务攻击（DoS）有何不同？

Q113 什么是SMB缓冲区溢出漏洞？

如何修补它？

Q114 如何对自己的服务器进行测试和检查，以找出可能的漏洞？

Q115 如何查找Windows系统、IIS、Apache、SQL服务器中是否有新的漏洞？

如何修补？

Q116 如何设置Windows 2000/XP系统的防火墙功能？

Q117 如何为我的服务器打造专用的防火墙？

Q118 如何从安全日志中判断是否有黑客或病毒入侵？

Q119 如何查看与判断系统日志、任务计划记录、IIS记录？

Q120 如何判断安全日志是否被黑客删除？

Q121 如何防止安全日志被黑客删除或修改？

Q122 如何追踪并查出黑客的位置，进一步查出黑客是谁？

Q123 黑客都是使用哪几种方式隐藏自己的IP来进行入侵的？

如何追踪？

附录 附录A 端口列表 附录B Currports 附录C NetInfo 附录D SyGate Personal Firewall 附录E

TaskInfo 附录F Startup 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 附录L IPNetInfo 附录M File Encryption Shell Extension 附

录N eMailTrackerPro 附录O Netcraft Toolbar 附录P Cookies Wall

<<防黑缉毒擒木马之绝命追杀>>

编辑推荐

一波未平、一波又起，是许多人面对病毒与黑客入侵的无奈。

据统计，平均每台电脑中至少有3~4个间谍或恶意程序(还不包含木马或病毒)，实在可怕。

真理是：事前预防永远胜于事后治疗。

其实，防止黑客或病毒进入你的电脑中并不像我们想象的那么困难，只要坚守一些基本原则，防护好几个重要的关卡，就可以让它们很难越雷池一步！

<<防黑缉毒擒木马之绝命追杀>>

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>