

## <<防黑防毒防钓大作战>>

### 图书基本信息

书名：<<防黑防毒防钓大作战>>

13位ISBN编号：9787302194576

10位ISBN编号：7302194572

出版时间：2009-2

出版时间：武新华、刘岩 清华大学出版社 (2009-02出版)

作者：武新华，刘岩 编

页数：335

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>

## &lt;&lt;防黑防毒防钓大作战&gt;&gt;

## 前言

随着社会各方面对网络技术的依赖性不断地增加，人们在体验互联网带来极大便利的同时，黑客入侵和网络安全也同样困扰着网络的发展，如僵尸网络(Botnet)、网络仿冒(Phishing)、木马及间谍软件、零时间威胁、熊猫烧香、网站挂马事件和木马产业链的曝光等，使得网络安全问题成为大家关注的重点。

由于互联网本身的复杂性、开放性等特点，网络的安全性已成为阻碍信息化进程的重要因素，其影响已从互联网领域逐步扩大到政府、通信、广电、金融、电力、交通等应用和建设领域，网络安全问题已引起了全世界的密切关注，黑客的恶意行为已成为全球新的公害。

大家或许都曾碰到过这样的情况，正当自己为精彩的网页着迷时，突然硬盘狂响不止，最后发现所有的程序都不能运行了；正在给网友写E-mail时，突然弹出一个对话框，上面写着“我是幽灵，我要毁了你的计算机！”

；正在聊天室里与网友激情聊天时，突然弹出一堆对话框，无论怎么关都关不掉，最后只能无奈地重启计算机；在登录QQ时却突然提示密码错误，试遍所有可能用过的密码却依然不能通过，这时才发现自己的QQ密码被盗了。

因此，就必须采取有力措施加强网络的自身安全防护性能，以有效地抵抗入侵和攻击破坏性。

但随着攻击手段的日趋复杂，有组织、有预谋、有目的、有针对性、多样化攻击和破坏活动的频繁发生，攻击点也越来越趋于集中化和精确性，攻击破坏的影响面不断扩大并产生连环效应，这就势必需要构筑一种主动的安全防御措施，才有可能最大限度地有效应对攻击方式的变化。

《防黑防毒防钓大作战（配光盘）》的写作目的主要是通过介绍黑客的攻击手段以提供相应的主动防御保护措施，使读者能够循序渐进地了解防御黑客入侵的关键技术与方法，提高安全防护意识，在实际遇到黑客攻击时能够做到“胸有成竹”。

希望读者能够运用《防黑防毒防钓大作战（配光盘）》介绍的知识去了解黑客，进而防范黑客的攻击，使自己的网络更加安全。

《防黑防毒防钓大作战（配光盘）》特别注重实例的使用，针对每一种攻防手段，都结合实例来进行介绍，并紧紧围绕黑客的“攻与防”这一主线，告诉读者如何建立个人计算机的安全防护措施，使自己远离黑客攻击的困扰，确保自己计算机数据的安全。

《防黑防毒防钓大作战（配光盘）》通俗易懂、图文并茂，即使是计算机新手也能无障碍阅读；任务驱动式的黑客软件讲解，揭秘每一种黑客攻击的手法；最新的黑客技术盘点，让用户“先下手为强”；先了解攻防互参的防御方法，全面确保用户的网络安全。

《防黑防毒防钓大作战（配光盘）》适合经常上网但缺乏网络安全和黑客知识的人员阅读，也可作为计算机网络爱好者的自学教材。

《防黑防毒防钓大作战（配光盘）》由众多经验丰富的高校教师编写，其中第1章由张克歌编写，第2章由李秋菊编写，第3章由陈艳艳编写，第4章由李防编写，第5章由杨平编写，第6章由段玲华编写，第7章由王英英编写，第8、9、10章由刘岩编写，第11章由武新华编写，第12章由孙世宁编写，最后由武新华统审全稿。

由于作者水平有限，书中的疏漏之处在所难免，恳请广大读者批评指正。

最后，需要提醒大家的是：根据国家有关法律规定，任何利用黑客技术攻击他人的行为都属于违法行为，希望读者在阅读《防黑防毒防钓大作战（配光盘）》后一定不要使用《防黑防毒防钓大作战（配光盘）》中介绍的黑客技术对别人进行攻击，否则后果自负。

## <<防黑防毒防钓大作战>>

### 内容概要

在如今这个信息时代，互联网在人们的工作学习中发挥了越来越大的作用，但目前大多数人的网络信息安全意识还很薄弱，给黑客和别有用心者留下可乘之机。

《防黑防毒防钓大作战（附光盘）》的主要目的就是让读者在尽可能短的时间内，了解黑客的起源、常用工具以及攻击方式，并在熟悉网络信息安全基本知识的前提下，掌握基本的反黑知识、工具和修复技巧，并采取相应的方法来制订自救措施。

《防黑防毒防钓大作战（附光盘）》内容全面丰富，图文并茂，深入浅出，适用于广大互联网爱好者，同时还可供网络信息安全从业人员及网络管理员作为速查手册使用。

## &lt;&lt;防黑防毒防钓大作战&gt;&gt;

## 书籍目录

第1章 黑客必备的网络知识1.1 计算机网络基础知识1.1.1 为什么要使用IP1.1.2 了解网络协议1.2 黑客的惯用伎俩——扫描端口1.2.1 什么是端口1.2.2 查看端口的方法1.3 一些常用网络命令1.3.1 测试物理网络1.3.2 查看IP、DNS、MAC1.3.3 查看目标计算机名、所在组和域1.3.4 在网络邻居中隐藏计算机1.3.5 路由跟踪命令1.4 可能出现的问题和解决方法1.5 总结与经验积累第2章 黑客入侵前的准备2.1 寻找入侵目标2.1.1 窃取目标主机的IP地址2.1.2 获知目标主机的地理位置2.1.3 获取网站备案信息2.2 检测系统漏洞2.2.1 漏洞检测工具——扫描器2.2.2 运用扫描器扫描共享资源2.2.3 运用MBSA检测系统安全性2.3 常用扫描和反扫描工具2.3.1 剖析RPC的漏洞扫描2.3.2 用WebDAV扫描个人服务器2.3.3 用网页安全扫描器查看网页的安全隐患2.3.4 防御扫描器追踪的利器——ProtectX2.4 可能出现的问题与解决2.5 总结与经验积累第3章 Windows系统漏洞入侵防御3.1 Windows服务器系统入侵防御3.1.1 入侵Windows服务器3.1.2 组网协议和服务攻击3.1.3 IIS服务攻击3.1.4 缓冲区溢出攻击3.2 Windows桌面用户系统入侵防御3.2.1 木马的多功能捆绑3.2.2 绕过Windows系统文件保护3.2.3 绕过Windows系统组策略3.2.4 实现后门自动加载3.3 Windows桌面用户网络入侵防御3.3.1 JavaScript和ActiveX脚本攻击3.3.2 XSS跨站点脚本攻击3.3.3 跨Frame漏洞攻击3.3.4 网络钓鱼攻击3.3.5 MSN蠕虫攻击3.4 Windows系统应用层入侵防御3.4.1 星号密码查看3.4.2 绕过防火墙3.4.3 绕过杀毒软件的保护3.5 可能出现的问题与解决3.6 总结与经验积累第4章 局域网入侵防御常见技巧4.1 ARP欺骗与防范4.1.1 ARP欺骗概述4.1.2 用WinArpAttacker实现ARP欺骗4.1.3 网络监听的检测与防范4.1.4 金山ARP防火墙的安装与使用4.2 MAC地址的克隆与利用4.2.1 MAC地址克隆4.2.2 MAC地址利用4.3 局域网广播信息4.3.1 用netstat命令实施攻击4.3.2 用局域网助手(LanHelper)实施攻击4.4 网游盗号机的使用与防护4.4.1 中游盗号机的入侵步骤4.4.2 联众GOP的入侵步骤4.4.3 “传奇密码宝贝”的使用4.4.4 传奇密码终结者4.4.5 光媒奇迹木马4.4.6 盗秘之王——密码解霸4.4.7 防护网游密码4.5 可能出现的问题与解决4.6 总结与经验积累第5章 轻松实现远程网络监控5.1 通过篡改注册表实现远程监控5.1.1 运用注册表启动终端服务5.1.2 Telnet中的NTLM权限验证5.2 端口监控与远程信息监控5.2.1 运用URLyWarning实现远程信息监控5.2.2 用SuperScan实现端口监控5.3 远程控制技术5.3.1 用CuteFTP实现上传下载5.3.2 通过WinVNC尝试远程控制5.3.3 用WinShell定制远程服务端5.3.4 进行多点控制的得力帮手——QuickIP5.3.5 定时抓屏的天才——屏幕间谍5.3.6 用魔法控制2007实现远程控制5.4 远程控制的冠军——pcAnywhere5.4.1 安装pcAnywhere程序5.4.2 设置pcAnywhere的相关功能5.4.3 使用pcAnywhere进行远程控制5.5 可能出现的问题与解决5.6 总结与经验积累第6章 黑客脚本攻击防御实战演练6.1 编程攻击实例6.1.1 通过程序创建木马6.1.2 隐藏防拷程序的运行6.2 恶意脚本攻击实例6.2.1 运用点歌台漏洞攻击6.2.2 针对Discuz论坛的攻击6.2.3 恶意网页代码攻击6.3 剖析恶意脚本的巧妙运用6.3.1 剖析SQL注入攻击6.3.2 全面提升ASP木马权限6.3.3 电影网站的SQL注入漏洞6.3.4 轻松拿下WEBSHELL.smv6.4 可能出现的问题与解决6.5 总结与经验积累第7章 QQ和MSN的攻击与防御7.1 QQ攻防实战7.1.1 攻击QQ的方法7.1.2 用QQsee查看聊天记录7.1.3 用QQ掠夺者盗取QQ密码7.1.4 用“QQ枪手”在线盗取密码7.1.5 “QQ机器人”在线盗取密码7.2 防不胜防的QQ远程盗号7.2.1 并不友好的“好友号好好盗”7.2.2 可以进行远程控制的“QQ远控精灵”7.2.3 不可轻信“QQ密码保护”骗子7.2.4 防范QQ密码在线破解7.3 QQ消息炸弹与病毒7.3.1 用IPSniper进行消息轰炸7.3.2 在对话模式中发送消息炸弹7.3.3 向指定的IP地址和端口号发送消息炸弹7.3.4 如何对付QQ消息炸弹7.4 斩断伸向MSN的黑手7.4.1 MSNMessengerHack盗号揭秘7.4.2 用MessenPass查看本地密码7.5 可能出现的问题与解决7.6 总结与经验积累第8章 嗅探、欺骗和陷阱8.1 网络嗅探器8.1.1 用嗅探器SnifferPro捕获数据8.1.2 用嗅探器SpyNetSniffer实现多种操作8.1.3 艾菲网页侦探8.1.4 局域网中的嗅探精灵Iris8.2 网络上的欺骗与陷阱8.2.1 具备诱捕功能的“蜜罐”8.2.2 拒绝恶意接入的“网络执法官”8.3 可能出现的问题与解决8.4 总结与经验积累第9章 跳板、后门与日志的清除9.1 跳板与代理服务器9.1.1 代理服务器概述9.1.2 “跳板”概述9.1.3 代理服务器的设置9.1.4 制作一级跳板9.2 入侵后门9.2.1 手工克隆账号9.2.2 在命令行下制作后门账号9.2.3 克隆账号工具9.2.4 用Wolff留下木马后门9.2.5 SQL后门9.3 巧妙清除日志文件9.3.1 利用elsave清除日志9.3.2 手工清除服务器日志9.3.3 用清理工具清除日志9.4 恶意进程的追踪与清除9.4.1 区分进程和线程9.4.2 查看、关闭和重建进程9.4.3 隐藏进程和管理远程进程9.4.4 消灭潜藏在自己计算机中的病毒进程9.5 可能出现的问题与解决9.6 总结与经验积累第10章 系统优化软件和杀毒软件10.1 系统优化软

## <<防黑防毒防钓大作战>>

件10.1.1 用金山清理专家实现系统优化10.1.2 完美卸载2008的杀毒功能10.2 驱逐间谍软件10.2.1 用Ad-aware软件驱逐间谍10.2.2 反间谍专家10.3 木马清除的好帮手10.3.1 用“ Windows进程管理器 ” 管理进程10.3.2 用“ 超级兔子 ” 清除木马10.3.3 使用TrojanRemover清除木马10.4 杀毒软件使用实战10.4.1 瑞星杀毒软件200810.4.2 江民杀毒软件200810.4.3 金山毒霸200810.4.4 卡巴斯基杀毒软件10.5 可能出现的问题与解决10.6 总结与经验积累第11章 数据备份升级与恢复11.1 数据备份升级概述11.1.1 什么是数据备份11.1.2 系统的补丁升级11.2 造成数据丢失的原因11.3 使用和维护硬盘注意事项11.4 强大的数据恢复工具11.4.1 数据恢复的概念11.4.2 数据恢复工具EasyRecovery11.4.3 简单易用的恢复工具FinalData11.5 可能出现的问题与解决11.6 总结与经验积累第12章 病毒木马主动防御清除12.1 关闭危险端口12.1.1 一键关闭危险端口12.1.2 利用IP安全策略关闭危险端口12.2 用防火墙隔离系统与病毒12.2.1 Windows系统自带的防火墙12.2.2 用“ 天网 ” 将攻击挡在系统之外12.2.3 免费网络防火墙ZoneAlarm12.3 对未知病毒木马全面监控12.3.1 监控注册表与文件12.3.2 监控程序文件12.3.3 未知病毒木马的防御12.4 维护系统安全的360安全卫士12.4.1 查杀恶评软件与病毒12.4.2 系统全面诊断12.4.3 修复InternetExplorer浏览器和LSP连接12.4.4 清理使用痕迹12.5 拒绝网络广告12.5.1 过滤弹出式广告——遨游Maxthon12.5.2 过滤网络广告杀手——AdKiller12.5.3 广告智能拦截的利器——ZeroPopup12.5.4 使用MSN的MSNToolbar阻止弹出广告12.6 可能出现的问题与解决12.7 总结与经验积累

## <<防黑防毒防钓大作战>>

### 章节摘录

插图：步骤2：在其中选择一项或多项之后，单击【启用选中项】按钮或【禁用选中项】按钮，即可完成所需操作，如图10.10所示。

在高级设置中，可以指定特定的驱动器是否允许自动运行功能。

21文件粉碎机大多数情况下，windows系统自带的文件删除并不彻底，文件被删除之后，仍然可以通过一些磁盘工具进行恢复。

所以对于一些想彻底删除的文件，可以使用金山清理专家的文件粉碎机进行彻底删除。

具体的操作步骤如下。

步骤1：在【金山清理专家】主窗口中，选择【安全再宝箱】，【文件粉碎机】命令，即可打开【文件粉碎机】窗口。

在其中添加所要删除的文件或文件夹并选中，则可将此文件（或文件夹）列入即将删除的列表中，如图10-11所示。

步骤2：单击【彻底删除】按钮，即可打开确认是否删除对话框。

单击【是】按钮，该文件被彻底删除；单击【否】按钮，则取消当前操作。



## <<防黑防毒防钓大作战>>

### 编辑推荐

《防黑防毒防钓大作战》由安防专家讲解，揭秘多种黑客工具，确保网络安全，实战攻防互动，剖析黑客入侵技术，提供防御措施，真正通俗易懂，全面揭露防黑防毒防钓作战全过程，视频图解实例，彻底打破电脑初学者的知识壁垒。

从基本命令和使用工具讲起，让初学者快速入门。

结合实例详尽剖析黑客攻击技术与防黑防毒防钓技巧。

涉及扫描与嗅探、欺骗与陷阱、木马和间谍等使用内容和最新应用。

从菜鸟到大虾，真正做到无师自通和完全掌握。

## <<防黑防毒防钓大作战>>

### 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>