第一图书网, tushu007.com

<<黑客技术攻防擂台木马任务大作战>>

图书基本信息

书名：<<黑客技术攻防擂台木马任务大作战>>

13位ISBN编号：9787030218032

10位ISBN编号：7030218035

出版时间：2008-6

出版时间：科学出版社

作者：程秉辉　Jonh Hawke　合著

页数：446

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

内容概要

这是一本基于病毒、木马攻击与防护技术的系统安全图书。
网络安全问题层出不穷，千万不要因为缺乏准备的头脑而成为下一个替罪羔羊！
在来自Internet安全领域的战争中，木马攻防是其重要战场之一。
高深的网络与系统技术一直是兵家必争之地，本书将彻底颠覆传统观念，独家公开黑客内幕，你不必潜心钻研高深的网络与系统技术，甚至不需要学习程序设计知识，也无须具备诸多常识或经验，只要使用一般的软件及工具，就能够轻松设计出让防毒软件不追杀、防火墙不阻挡……同时具有多种功能的木马。
或者让设计不周到的木马或小工具如虎添翼、更加完美，使众多防黑杀毒软件厂家惊慌失措、疲于奔命……将黑客历史的发展推向一个崭新的境界！
本书作者竭尽所能、挖空心思，用尽一切创意和想象，将黑客制作与组合出这类木马的完整过程呈现给大家，同时针对各种木马的弱点提出相应的有效防护办法，希望能够在众多杀毒软件束手无策的情况下，让广大用户走出木马的威胁与阴影，这便是本书的意义和价值所在。
本书适合每位Windows联网用户以及各类网络办公企业。
同时也适合Windows——特别是Vista和操作系统DIY爱好者，更是诸位黑客狂想者的练兵演习的习武之地。
光盘内容为书中所用部分软件工具的安装程序。

作者简介

作者：程秉辉 (英国)Jonh Hawke

书籍目录

Part 1 什么是木马　Q1 什么是木马、恶意或间谍程序、后门程序、跳板程序、病虫？
它们有什么样的危险性？
Q2　使用木马与其他黑客入侵或攻击的手法有何不同之处？
Q3　木马与一般病毒有何不同？
它可以拿来做什么？
Q4　为何许多人很想做黑客？
是出于什么样的心态与心理？
Q5　哪种黑客最喜欢而且善用木马？
做黑客可以挣钱吗？
Q6　木马有哪几种类型7如何区分？
各有何优缺点？
Q7　如何针对不同类型木马的特性来找出可能隐藏在电脑中的不速之客？
Q8　木马技术在发展与演变上是如何进行的？
分成哪几个阶段？
各使用什么样的技术？
Q9　如何针对木马入侵的各环节进行防护、阻挡与破解？
Q10　黑客利用木马入侵的流程为何？
Q11 黑客如何选择、查找与获取所要使用的木马？
Q12　有哪些方法可以防止黑客查找与获取所想要的木马？
有何优缺点？
Part 2 木马伪装与破解 木马伪装技术的演变 木马伪装测试流程 不必伪装的木马 木马伪装易容术 测试伪装的木马 自行设计的木马 Q13　黑客为何要伪装木马程序？
Q14　什么情况或条件下黑客不需要伪装木马，而且还可以名正言顺地叫被黑者运行？
Q15　为什么遥控软件也可以当木马？
为何它比真正的木马更容易成功？
Q16　为何许多木马无法被杀毒软件找出来？
是什么原因？
Q17　有哪些方法可以找出杀毒软件无法找到的木马？
Q18　黑客会使用哪些方法来伪装木马？
有何优缺点？
Q19　如何找出伪装的木马后将它斩首？
Q20　黑客如何检验伪装后的木马？
有何盲区与注意之处？
Q21　同一个伪装后的木马，为何有的杀毒软件找得出来，有些却没发现？
这是什么原因？
Q22　黑客可能设计出任何杀毒软件或网络防护程序都无法找出来而且永久有效地伪装的木马？
Part 3 诱骗技巧与运作木马 Q23　黑客会使用哪些方法将木马植入并在被黑电脑中运行？
流程为何？
各有何优缺点？
Q24　黑客通常使用哪些方式直接进入被黑者电脑中，然后植入与运行木马？
各有何优缺点？
如何防护？
Q25　我没有接收邮件，也未从网络下载任何文件，只是上网就被植入木马？
是什么原因？
如何防护？

Q26 我使用最新的杀毒软件，也有防火墙，从不下载或运行任何网络上的文件，也经常修补系统与各种网络程序的漏洞，为何还是被植入木马？
这是什么原因？
如何防范？
Q27 黑客使用哪些方法利用电子邮件将木马植入被黑电脑与运行它？
各有何优缺点？
如何阻挡？
Q28 什么是电子邮件钓鱼？
黑客如何利用它来将木马植入被黑电脑与运行它？
如何防护？
Q29 黑客会使用哪些说法或藉口欺骗被黑者接受木马程序与运行它？
Q30 黑客会使用哪些理由来说服特定(熟识)被黑者下载与运行木马？
Q31 黑客通过哪些管道来让特定(熟识)被黑者下载与运行木马？
Q32 对于任意查找下手目标的黑客会使用哪些方法来让被黑者下载与运行木马？
Q33 黑客通过哪些管道来让任意被黑者下载与运行木马？
Q34 黑客会使用哪些理由来说服任意被黑者下载与运行木马？
Q35 网络上哪些种类的文件最可能藏匿木马(或间谍、恶意源码)？
Q36 什么是动画或游戏木马帮凶(Flash木马帮凶)？
黑客如何制作与使用它？
如何有效防护？
Q37 黑客如何利用Flash木马帮凶来诱骗被黑者下载、植入与运行木马？
有何优缺点？
Q38 什么是多媒体木马帮凶(例如RealPlayer木马帮凶)？
黑客如何制作与使用它？
如何有效防护？
Q39 黑客如何利用多媒体木马帮凶来自动下载与运行木马？
Q40 黑客如何让浏览网页就能自动植入并运行木马？
Q41 我只是浏览网页，并没有下载任何文件，为何也会中木马？
这是什么原因？
如何解决？
Q42 什么是木马网页？
黑客如何制作它？
如何有效防护？
Q43 什么是木马帮凶生成器？
它有何优缺点？
黑客如何利用它？
Q44 网络上可以找到许多木马帮凶生成器，下载后就能使用吗？
有什么问题与缺点？
Q45 黑客如何快速设计出设计帮助木马植入被黑电脑与运行的工具？
Q46 不会写程序的黑客可以设计出木马的帮凶工具，而且不会被杀毒软件抓出来吗？
如何实现？
Q47 木马帮凶工具如何关闭各种防火墙与杀毒软件来帮助木马更加安全？
Q48 黑客如何利用安装生成工具设计出帮助木马植入被黑电脑与运行(并设置每次进入Windows自动运行)的工具？
Q49 黑客有哪些方法让植入的木马立刻运行？
各有何优缺点？
如何防护？

Q50 黑客如何使用at命令来运行被黑电脑中的任何程序？
如何防护？
Q51 黑客如何使用net命令来运行被黑电脑中的木马？
如何防护？
Q52 黑客会使用哪些方法让被黑电脑尽快或立刻重启动，让植入的木马运行？
如何防护？
Q53 黑客如何以简单的欺骗方式就可以使被黑者很听话地重启动？
Part 4 木马的藏匿与运作 Q54 黑客如何设置每次启动进入Windows就自动运行木马？
Q55 黑客植入的木马程序都藏匿在哪些地方？
各有何优缺点？
如何找出来砍头？
Q56 我知道木马在注册表(Registry)中设置自动运行，但为何就是未找到呢？
Q57 木马如何使用替换某个系统文件的方式来自动运行？
有何优缺点？
如何防护？
Q58 木马隐藏在被黑者电脑中的方式有哪些新的技术与发展方向？
如何道比魔高？
Q59 黑客如何将一般木马程序转换成系统服务方式来运行？
如此就可逃过任务管理器或Tasklnfo之类工具的查杀？
如何防护？
Q60 黑客如何在木马帮凶工具中设计以系统服务方式来运行木马？
Q61 如何查找、判断与干掉以系统服务方式运行的木马？
有哪些困难之处？
Q62 木马成功运行与启动后，黑客要如何使用它？
可以阻挡吗？
要怎么做？
Q63 既然黑客已经成功植入与启动木马，为何还会失败？
有哪些原因？
Q64 什么是ICMP木马？
它的原理为何？
它如何突破防火墙的阻挡？
如何防护？
Q65 哪些情况下即使木马成功植入而且启动，但黑客无法获取被黑者IP或者与木马连接？
Q66 黑客如何让植入局域网电脑(或网吧电脑)的木马服务器程序也可以正常运作？
Q67 木马Server程序在使用虚拟lP的被黑电脑中要如何与黑客的木马Client程序进行连接？
Q68 要对位于某个局域网中的电脑进行远程遥控，但遥控端的电脑并不在该局域网中，要如何实现？
Part 5 各类型木马专论剖析 昨日黄花之远程遥控软件 昨日黄花之黑客之门 多功能木马典范—Optix PRO 突破虚拟IP…反向连接木马Splone 回归自然的发展方向 Q69 不会编程的黑客也能设计出符合自己需要的简单木马吗？
要如何实现？
Q70 只利用各种工具就能设计出一个功能完整、打开后门的木马吗？
要怎么做？
Q71 黑客如何利用安装生成工具设计出打开Telnet与终端机后门的木马？
Q72 黑客如何让使用动态lP的被黑电脑在成功打开后门后都能随时进出？
Q73 如何使用安装生成工具设计偷取交谈日志、各种重要文件、注册表中各类帐户的木马？
Q74 如何防护使用安装生成工具设计出来的各种木马？

Q75 Optix PRO木马可对被黑电脑进行哪些黑客行为？
会造成哪些损失与伤害？
如何进行防护？
Q76 Optix PRO木马如何关闭杀毒软件与防火墙来避免其被抓出来？
Q77 黑客如何在茫茫网海中查找可利用的发信服务器？
Q78 如何找出我的电脑中是否有OpUx PRO木马藏匿？
如何彻底干掉它？
Q79 现在许多电脑都使用虚拟IP上网，对于这个传统木马的天敌——虚拟IP，黑客有什么方法可以有效突破？
Q80 什么是反向连接木马？
黑客如何利用它来突破虚拟IP？
它有何优缺点？
Q81 黑客如何使用一般工具制作组合出所Q85 黑客如何不使用任何工具就能偷取到各种实时通信软件的交谈日志？
附录1 选择可用网页空间附录2 获取多媒体文件地址附录3 各地IP地址详细列表附录4 端口列表附录5 Tasklnfo附录6 Stanup附录7 ASPack附录8 木马捆绑器附录9 PECompact附录10 UPXShell附录11 EXE Stealth附录12 ASProtect SKE附录13 Private exe Protector附录14 XN Resource Editor附录15 AppToService附录16 avast！
Home杀毒软件附录17 Comodo个人防火墙附录18 卡巴斯基杀毒软件附录19 各类密码寻回工具附录20 tftp32附录21 CurrPorts附录22 OptixPro附录23 Splone附录24 VNN虚拟IP电脑连接工具附录25 SuperScan附录26 Angry IP Scanner附录27 at命令说明附录28 NetBrute Scanner附录29 SetupFactory附录30 EmEditor附录31 黑客之门

章节摘录

Part1 什么是木马Q1 什么是木马、恶意或间谍程序、后门程序、跳板程序、病虫？
它们有什么样的危险性？
不论是木马、恶意源码、间谍程序、后门程序、跳板程序、病虫等，其实广义上说都可以统称为木马，因为都是潜藏在被黑电脑中进行各种活动，而依照它的行为而出现许多种不同的名称，例如：间谍程序、后门程序、跳板程序、病虫、僵尸程序、傀儡程序、键盘侧录程序、桌面监控程序等等。

编辑推荐

《黑客技术攻防擂台:木马任务大作战》适合每位Windows联网用户以及各类网络办公企业。
同时也适合Windows——特别是Vista和操作系统DIY爱好者，更是诸位黑客狂想者的练兵演习的习武之地。
光盘内容为书中所用部分软件工具的安装程序。

第一图书网, tushu007.com
<<黑客技术攻防擂台木马任务大作战>>

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