<<黑客达人迷>>

图书基本信息

书名：<<黑客达人迷>>

13位ISBN编号：9787115293480

10位ISBN编号：7115293481

出版时间：2013-1

出版时间：人民邮电出版社

作者：Kevin Beaver

页数：325

字数：439000

译者：傅尔也

前言

妈妈，这本书献给您。
您在顽强地同癌魔做着斗争，从未想到您给我带来了多大的灵感。
我深深地爱您，想念您。

欢迎阅读《黑客达人迷》。
本书以平实的日常用语简要介绍了计算机黑客的技巧和技术，利用它们，可以评估信息系统的安全性，找出重要的安全漏洞，并在黑客犯罪分子和恶意用户利用这些漏洞前进行修复。
这种黑客攻击是专业、公开而且合法的安全测试，我在全书中都会称其为道德黑客攻击（ethical hacking）。

计算机和网络安全是个复杂多变的主题。
大家必须登高望远，才能确保自己的信息得到保护，不受坏人侵扰。
这就是我在本书中介绍的工具和技术能派上用场的地方。

大家可以实施这里介绍的所有安全技术，以及其他可以运用的最佳做法，这样大家的系统可能就安全了，就如你所知。
不过，只有了解了恶意攻击者的想法，运用这种了解，使用合适工具从恶意攻击者的角度对系统进行评估，大家才能真正明白自己的信息到底有多安全。

道德黑客攻击融合了正式且有条不紊的渗透测试、白帽黑客攻击和漏洞测试，对找出安全漏洞并确保信息系统始终处于真正安全的状态来说是必需的。
本书为大家提供了成功实施道德黑客攻击计划所需的知识，还介绍了可以用来防止外部黑客和恶意用户影响业务的对策。

读者对象　　声明：如果利用书中信息进行黑客攻击或未经授权恶意侵入计算机系统，一切责任自负。
我以及其他与本书相关的人员，都不会为利用本书介绍的方法和工具进行非文明或犯罪的行为承担任何责任。
本书的意图仅限于让IT和信息安全专业人员在得到授权的情况下测试（自有系统或客户系统的）信息安全。

好了，现在题外话扯完了，言归正传！
本书面向网络管理员、信息安全经理、安全顾问、安全审计人员、合规经理，或那些有兴趣更多地了解计算机系统正规测试以及IT运营从而让系统更安全的人。

作为在执行周密信息安全评估的道德黑客，大家可以检测并指出其他情况下可能被忽视的安全漏洞。
如果是在自己的系统上执行这些测试，那么在测试中发现的数据将有助于说服管理层，证明信息安全真是应该认真对待的业务问题。
如果是在为客户执行这些测试，将有助于在坏人有机会利用安全漏洞之前修补它们。

本书提供的信息可以帮助大家在这场安全游戏中占据先机，让大家享受帮助组织和客户防止信息受危害所赢得的声誉和荣耀。

关于本书　　本书是通过攻击系统以提高安全性的参考指南。
这些道德黑客攻击技术都基于计算机系统渗透测试、漏洞测试和信息安全最佳做法中各种成文和不成文的规则。
本书涵盖了各种内容，从制订黑客攻击计划，到对系统进行测试，再到修复漏洞，直至维持长期的道德黑客攻击计划。
实际上，对很多网络、操作系统和应用而言，可能存在几千种黑客攻击。
我要介绍的是多种平台和系统中的主要攻击。
不管是需要评估小型家庭办公室网络，还是要评估中等规模的企业网络，抑或是为大型企业系统进行评估，本书都能为大家提供所需的信息。

如何利用本书　　本书具有以下特性。

· 多种技术上的和非技术的黑客攻击，及其详细方法； · 来自知名信息安全专家的信息安全测试案例研究； · 应对黑客攻击的具体保护对策。

在开始攻击自己的系统之前，要熟悉第一部分中介绍的信息，让自己对这些任务成竹在胸。“如果不做计划，那就等着失败”（if you fail to plan， you plan to fail），这在道德黑客攻击过程中特别正确。

如果大家想要取得成功，就必须获得授权，并且制订可靠的测试计划。

请不要将这些资料用于不文明或非法的黑客攻击，不要依靠这些内容让自己实现从脚本小子到大黑客的飞跃。

本书只是为了让大家了解以文明且合法的方式对自己或客户的系统进行黑客攻击所需的知识，以增强信息安全。

不需要阅读的内容 根据自己的计算机和网络配置的不同，大家可以跳过某些章节。例如，如果大家没有使用Linux系统或无线网络，那么就可以跳过相关章节。

傻瓜假设 我在这里对你们这些有抱负的安全专业人员作出了一些假设： · 熟悉与计算机安全、网络安全和信息安全相关的基本概念和术语； · 对黑客和恶意用户的行为有基本的了解； · 可以访问使用这些技术的计算机和网络； · 可以访问互联网，获取用于道德黑客攻击过程的各种工具； · 有权执行本书中描述的道德黑客技术。

本书结构 本书分为七个部分，所以大家可以按照自己的需要跳过某个部分直接阅读其他部分。

每一章都提供了可用于道德黑客攻击过程的可行方法，包括可使用工具的清单和来源，以及互联网上的资源。

第一部分：打下道德黑客攻击的基础 本部分涵盖了道德黑客攻击的基础知识。

首先概述了道德黑客攻击的价值，以及在道德黑客攻击过程中该做和不该做的事。

接着带大家深入了解恶意心态，并告诉大家如何计划自己的道德黑客攻击测试。

最后，本部分介绍了道德黑客攻击的步骤，其中包括如何选择合适的工具。

第二部分：发动道德黑客攻击 本部分开启了道德黑客攻击的过程。

首先介绍了数种广泛使用的知名黑客攻击，包括社会工程学攻击和破解密码，作为这场道德黑客攻击大戏的开始。

接着介绍了信息安全中的人员要素和物理安全因素，这二者可能是信息安全计划中最脆弱的环节。

在阅读这些主题之后，大家将了解对系统执行常见的一般性黑客攻击所需要的奇技赢巧，以及保障信息系统安全的具体对策。

第三部分：攻击网络 从较大的网络开始，本部分介绍了为系统测试各种知名网络基础设施漏洞的方法。

从TCP/IP协议组的弱点，到无线网络的不安全性，大家可以学习如何借助特定手段和有缺陷网络通信去攻陷网络，并了解避免自己受其危害的对策。

本部分还包括一些有关网络黑客攻击的案例研究。

第四部分：攻击操作系统 几乎所有的操作系统都具有黑客经常利用的知名漏洞。

本部分介绍了如何对三种广泛使用的操作系统（Windows、Linux和NetWare）进行黑客攻击。

这些黑客攻击方法包括对操作系统进行漏洞扫描并对特定主机进行枚举，从而获得详细的信息。

本部分还介绍了如果利用这些操作系统中的知名漏洞进行攻击和远程攻占系统，以及让操作系统更加安全的具体对策。

本部分还含有操作系统黑客攻击的案例研究。

第五部分：攻击应用程序 如今应用程序的安全在信息安全领域也越来越不可小视了。

直接瞄准各种应用的攻击不断增多，这些攻击往往能绕过防火墙、入侵监测系统和杀毒软件。

本部分讨论了对特定应用和数据库（包括电子邮件系统、即时消息系统、IP电话系统和存储系统）的黑客攻击，并介绍了让系统可以更加安全的实用对策。

针对Web应用的攻击是特别常见的网络攻击。

几乎所有防火墙都允许Web流量进出网络，所以大多数攻击是针对几乎任何人都可以下载的数百

万Web应用展开的。
本部分还介绍了Web应用黑客攻击相应对策，以及一些现实安全测试中的应用程序黑客攻击案例研究。
　　第六部分：道德黑客攻击的结果　　在执行了道德黑客攻击之后，应该如何处理收集到的数据？是束之高阁还是四处炫耀？
该如何往前推进？
本部分就回答了这些问题，并介绍了更多内容。
从制订要提交给高管的报告，到修复自己发现的安全漏洞，再到为自己继续进行的道德黑客测试制定一套程序，本部分将整个道德黑客攻击过程结成了一个完整的循环。
这些信息不仅能确保大家的精力和时间得其所用，而且可以证明信息安全是依靠计算机和信息技术的企业取得成功的基本要素。
　　第七部分：三个十项　　本部分包含了一些有助于道德黑客攻击计划取得成功的提示。
大家会了解到如何让自己的道德黑客攻击计划得到高管的支持，以使自己可以行动起来，保护自己的系统。
本部分还介绍了大家必须避免的十大道德黑客攻击错误。
　　本部分还包含了附录，附录中提供了道德黑客工具和资源参考清单。
大家可以在本书在线小抄的附录中找到这些链接。
　　本书中使用的图标　　本图标指代有趣但对理解正讨论的主题来说不太重要的技术信息。
　　本图标指代值得记住的信息。
　　本图标指代可能对道德黑客攻击测试造成负面影响的信息，所以请仔细阅读！
　　本图标指代有助于突出或澄清要点的建议。
　　作者寄语　　对外部黑客和内部不法人员的行为方式以及该如何对系统进行测试了解得越多，就越能更好地保障计算机系统的安全。
本书提供了为自己的组织和客户制订并维护成功道德黑客攻击计划所需的基础知识。
　　要记住，道德黑客的高层级概念不会像自己要防范的具体信息安全漏洞那样经常变化。
道德黑客攻击是这个不断变化的领域中一门恒久不变的艺术和科学。
大家必须了解最新的硬件和软件技术，以及日复一日、年复一年不断出现的各种新漏洞。
没有一种一劳永逸的最佳攻击方法，所以要不断更新自己所掌握的信息。
（道德）黑客攻击，其乐无穷！

<<黑客达人迷>>

内容概要

《黑客达人迷(第3版)》以别具一格的视角、幽默生动的语言详尽地介绍了道德黑客攻击的全过程，旨在帮助读者在网络安全战争中知己知彼，百战不殆。

《黑客达人迷(第3版)》以道德黑客攻击计划为主线，系统讲述了常见黑客攻击方法及防御对策，并辅之以知名信息安全专家的安全测试案例，结构清晰，内容全面，是企业和个人进行计算机系统安全测试与评估的参考指南。

作为“达人迷”系列书之一，《黑客达人迷(第3版)》不仅适用于对计算机系统测试评估和IT安全感兴趣的初学者，而且对于网络管理员、信息安全经理、信息安全顾问、安全审计人员等专业人士也具有很大的参考价值。

作者简介

Kevin Beaver是位于亚特兰大的Principle Logic有限责任公司的独立信息安全咨询师、鉴定人和专业讲师。
他有着逾20年的从业经验，专门为《财富》1000强企业、安全产品供应商、独立软件开发商、大学、政府机构、非营利组织和小型企业进行信息安全评估。
在2001年开始信息安全咨询工作之前，曾在多家医疗保健、电子商务、金融和教育机构从事过信息技术和安全工作。

<<黑客达人迷>>

书籍目录

章节摘录

 这些骇客只是少数，所以不要觉得自己面对着数百万恶棍的威胁。
很多黑客只是喜欢修修补补，而且只是追求对计算机系统工作原理的了解。
我们最大的威胁其实来自于在组织内工作而且拥有有效网络账户的人，所以别忽视了这种内部威胁。
他们为什么这样做 黑客们进行黑客攻击的主要原因是他们有能力那样做。
就这么简单。
好吧，还有比这更深一点的原因。
黑客攻击是某些黑客的休闲爱好，他们攻击系统只是想看看自己能不能攻入系统，通常只是测试他们自己的系统。
这些人不在本书讨论之列。
我要讲的是那些迷恋于获得恶名或击败计算机系统，以及那些有着犯罪意图的黑客。
很多黑客以智斗公司和政府的IT和安全管理员为乐，以制造头条新闻和成为臭名昭著的网络歹徒为荣。
打败某个很少有人打败的实体，或是了解很少有人了解的知识，会让他们自我感觉良好。
很多这种黑客会享受侵入计算机系统带来的即时陕感。
他们会迷恋上这种感觉。
有些黑客无法抗拒攻入别人系统时。
肾上腺素上涌的感觉。
通常情况下，任务越困难，黑客获得的快感就越大。
黑客们通常很推崇个人主义或至少是信息的分散化，因为很多黑客觉得所有信息都应该是自由的。
他们认为网络攻击和现实世界的攻击是不同的。
黑客们可能很容易忽视或误解受害者以及黑客攻击的后果。
很多黑客说他们并不打算通过他们的攻击造成危害或谋取私利，这不过是他们为其行为开脱的借口。
很多黑客不求有形的回报，获得某种证明对他们来说往往就是足够的奖励了。
恶意攻击者获得的知识，以及成功攻击带来的自豪感，都可能会导致他们攻击成瘾并成为一种生活方式。
一些攻击者想把人们的生活弄得苦不堪言，另一些则只是想引起人们的注意。
常见的动机包括报复、获取吹牛资本、好奇心、无聊、寻求挑战、破坏公物、为了经济利益盗窃、阴谋破坏、敲诈、勒索和企业间谍活动。
黑客们经常会引用这些动机来解释他们的所作所为，不过这些动机在经济形势困难的时候往往会被引用得更多。
网络内部的恶意用户可能想要通过获取信息来解决个人经济问题，让他们可以比竞争对手先行一步，报复他们的雇主，满足他们的好奇心，或只是为了解闷。
很多企业所有者和管理者（即便是一些网络和安全管理员）相信，他们没有黑客想要的东西，或者觉得黑客就算侵入系统也不会造成多少损害。
他们真是大错特错。
这种对黑客不屑一顾的思想会助长这些坏人的气焰，促进他们实现目标。
黑客可以利用看似不重要的系统访问网络，并以此作为跳板攻击其他系统。
要记住，黑客经常只是因为他们可以攻击而攻击。
一些黑客会追寻那些引人瞩目的系统，不过攻入任何人的系统都能帮助他们融入黑客圈。
黑客利用很多人虚假的安全感，并会攻击他们觉得可以攻下的任何系统。
电子信息可能同时出现在多个地方，所以如果黑客们只是从他们侵入的系统复制了信息，那么很难证明黑客已经拥有这些信息了。
类似地，黑客们也知道被弄得面目全非的网页（不管有多容易受攻击）对其他人的业务来说是不好的。
要查看一些以前被篡改网页的例子，可以参考http：Hzone · h.or9／archive。

被黑的网站可能经常劝说管理者和其他不信邪的人来处理信息威胁和漏洞。
计算机侵害不断变简单的原因有以下几个：网络和互联网连接的广泛使用；互联网上和（经常有）内部网络中的计算机系统所提供的匿名性（因为很少进行有效地日志记录，特别是日志监控）；黑客工具数量变多，而且更容易取得；大量开发的无线网络可以帮助黑客掩盖他们的踪迹；当下在开发的应用程序和数据库的代码复杂度和规模更大了；计算机神童；攻击者如果被抓住，不大可能被调查或受起诉。
虽然大多数攻击被忽视或未被上报，但是那些被发现的罪犯却往往未受追捕或被起诉。
当黑客被抓住之后，他们往往会为自己的行为开脱，说他们的行为只为利人而且会造福社会：他们只是赶在其他人之前找出漏洞而已。
不管如何，如果黑客被抓获并被起诉，那黑客们所认同的“声望和荣耀”奖励系统就会受威胁。
恶意用户同样如此。
通常情况下，他们的诡计不会被发现，不过如果他们被抓住，那么也可能会以股东价值或不想造成不快的名义不了了之。
不过，最近的信息安全和隐私法律法规正在改变这一情形，因为在大多数情况下必须通报这种违规行为。
有时候，这些人会被解雇或被要求辞职。
虽然内部违规公共案件日益普遍，但这只是冰山一角，并非一般组织的真正全貌。

<<黑客达人迷>>

编辑推荐

《黑客达人迷(第3版)》为计算机信息安全必备；详尽涵盖了最新黑客攻击方法和工具，内容全面；提供了来自知名信息安全专家的安全测试案例；企业进行计算机系统安全测试与评估的参考指南。

版权说明