# <<渗透测试实践指南>>

## 图书基本信息

书名：<<渗透测试实践指南>>

13位ISBN编号：9787111401414

10位ISBN编号：7111401417

出版时间：2012-11-20

出版时间：机械工业出版社华章公司

作者：Patrick Engebretson

页数：169

译者：缪纶,只莹莹,蔡金栋

## 前言

当你打算阅读本书时，我想会有几个问题萦绕在你的脑海中：本书读者对象是谁？
这本书与其他书（在这里插入你最喜爱的书名）有什么不同？
我为什么要买这本书？
这些都是很平常的问题，而且我正在让读者为其支付他们辛辛苦苦赚来的现金，所以为这些问题提供一些答案是很重要的。
对于有兴趣学习黑客技能和渗透测试的人来说，进入一个琳琅满目的书店就如同在amazon.com搜索关于“ 黑客 ”的书籍那样让人迷惑。
最初，似乎是有无尽的选择让人从中挑选。
最大的书店都会为计算机安全书籍设立几个书架，包括编程安全、Web应用安全、rootkit和恶意软件、渗透测试方面，当然，还有黑客方面的书籍。
然而，即使是关于黑客的书籍,它们在内容和题材上似乎也各不相同。
有的书侧重于使用工具，但不讨论如何将这些工具结合在一起。
其他书籍侧重于黑客领域中的某个特定主题，却缺乏对大局的论述。
本书旨在解决上述问题，它是任何对黑客活动或渗透测试知识感兴趣的人的起点。
本书会涉及具体的工具和知识点，并且还将研究如何将这些工具结合在一起，探讨如何利用这些工具成功地完成任务。
本书读者对象本书是关于黑客活动和渗透测试的一个非常易懂但却很彻底的指南。
它特别注重帮助读者掌握完成一次黑客攻击或渗透测试所需的基本步骤，而且不会让你感到不知所措。
当你阅读本书后，将会对渗透测试过程有一个扎实的理解，并且能自如地运用所需要的基本工具来完成工作。
需要强调的是，本书面向从事黑客活动和渗透测试的新手和那些很少或根本没有经验的人们，也面向那些因无法顾全大局（各种工具和各个阶段是如何结合在一起的）而感到沮丧的人们，或那些希望学习到更多有关威慑安全相关知识的人们。
总之，本书是为所有对计算机安全、黑客活动或渗透测试感兴趣，但没有经验、不知道从哪里开始的人们撰写的。
我和一位同事称这个概念为“ 黑客入门 ”（Zero Entry Hacking，ZEH），就像现在的游泳池，入门级游泳池由浅到深逐渐倾斜，初学者涉水时不会有被淹没的感觉，也不用担心溺水。
“ 入门 ”这一概念允许每个人都能够使用这个“ 游泳池 ”，不论年龄或能力。
本书采用了类似的技术。
ZEH旨在揭示基本概念而不会令人感到不知所措。
掌握ZEH将为你将来学习更高级的课程和阅读更深入的书籍打下坚实的基础。
本书与其他书有什么不同当不与我的家人共度时光时，我喜欢做两件事情：阅读和从事与黑客相关的活动。
大部分时间，我通过阅读有关黑客方面的书籍来将这两个爱好结合起来。
可以想象，作为一名教授和渗透测试者，我书架上排列着许多有关黑客、安全和渗透测试方面的书籍。
如同生活中大多数事情一样，每本书的质量和价值是不一样的。
有些书是非常优秀的资源，书读百遍以至于这些书籍的封面差不多都破碎了。
另外一些书籍提供的帮助则比较少，一直崭新如一。
一本能够很好地解释细节且没有失去读者的书，如同金子般珍贵。
遗憾的是，大多数我喜爱的书籍都已经磨损和破碎，它们要么特别厚（500页），要么内容针对性强（单一主题的深入指南）。
这并不是什么坏事，事实上，正好相反，它们内容详尽且清晰，因此它们都是非常棒的书籍。
但同时，侧重详细安全性主题的大型巨著似乎会使新手不知所措。

遗憾的是，对于进入安全领域的初学者和想学习道德黑客的人来说，那些向他们介绍黑客知识基本原理的书籍，既令人望而却步又使人困惑。
本书在两个方面与其他书籍有所不同。
首先，它适合初学者（运用“ 入门 ”的概念）。
如果你从来没有执行过任何类型的黑客活动，或已经使用了一些工具但不是很确定下一步要做什么（或不知道如何解释工具的输出结果），那么本书是为你准备的。
我们的目标不是让你迷失在细节中，而是为你呈现整个领域的全景。
当然，本书仍然会介绍每一个用于完成渗透测试步骤所需要的主要工具，它不仅会深入地探究每一个工具，并且还会详细讲解它们的附加功能。
从这个观点来看，这样的讲解有助于本书将重点集中到基本知识介绍上，而且在很大程度上，可以使我们避免陷入由工具版本的高级功能或细微差别所带来的困惑中。
例如，3.3节将介绍如何使用常用的端口扫描器Nmap来运行基本扫描。
因为本书侧重于基础知识，所以到底运行哪个版本的Nmap就变得不那么重要了。
不管你使用的是Nmap版本2或版本5，执行SYN扫描是完全一样的，没有什么不同。
我们将尽可能地采用这个技巧，这样读者可以在学习Nmap（或任何工具）过程中不必担心功能的变化，因为往往由于版本的改变，会随之带来一些高级特性。
本书旨在介绍通用的知识，这有助于读者将来理解更前沿的主题。
请记住，一旦扎实地掌握了基础知识，就可以随时回过头来学习具体的细节并掌握工具的高级功能。
此外，每章结尾都会建议性地介绍一些工具和深入的主题，这些工具和主题超出了本书的范围，但你可以做进一步研究从而增进知识层次。
本书不仅仅是为初学者编写的，实际上它以一种非常独特的方式呈现信息。
我们在书中使用的所有工具和技术将会以少量的机器作为目标，并以一种特定的顺序进行实践。
（所有目标机器将属于同一子网，读者将能够轻松地重建这个“ 目标 ”网络。
）读者将会了解如何解释工具的输出，以及如何利用输出继续后续的攻击。
本书使用了一个贯穿全书且有先后次序的例子来帮助读者了解渗透测试的全景，而且这个例子可以使读者更好地理解各种工具和各个阶段是如何结合在一起的。
这与如今市场上的许多其他书籍不同，这些书籍通常会讨论各种工具和不同的攻击手段，但未能解释如何有效地将这些工具衔接在一起。
本书为读者清楚地解释了渗透测试的某个阶段是如何向另一个阶段过渡的。
以这种方式呈现信息，可以为读者提供宝贵的经验，并可让他们通过简单地模仿书中的例子完成整个渗透测试过程。
这种方法可以帮助读者清楚地理解基础知识，同时了解各种工具和各个阶段是如何相互关联的。
为什么要购买本书对于这个问题，我们在前面已经给出了直接的回答，下面我们将这一问题的答案以列表的形式呈现出来：你想了解更多有关黑客活动和渗透测试方面的知识，但不确定从哪里开始。
你已涉足黑客活动和渗透测试，但不知道如何将各部分结合在一起。
你想了解更多有关黑客和渗透测试者为获得网络和系统的访问控制权限所使用的工具以及实现的过程。
你在寻找学习威慑安全知识的理想入手点。
你喜欢挑战。

# <<渗透测试实践指南>>

## 内容概要

这是一本权威而实用的渗透测试实践指南，Amazon超五星畅销书，美国国家安全局主管鼎力推荐，被誉为学习渗透测试必读的书之一。
以独创性的ZEH方法，结合前沿、实用的开源工具，采用科学、有序的四步模型，全面讲解了渗透测试的技术、工具和方法，同时结合大量的演示实例，配以详细的操作步骤和图文解说，适合作为系统学习渗透测试的参考书。

全书共分7章：第1章介绍了渗透测试的概念、常用工具（Backtrack等）、测试环境的搭建，以及四步模型法；第2章讲解了HTTrack、Google搜索指令、The Harvester（邮箱地址侦察）、DNS和电子邮件服务器信息提取、MetaGooFil、筛选信息技巧等侦察工具和手段；第3章讲解了ping命令、ping扫描、端口扫描涉及的切实可用的工具及参数设置，如Nmap、Nessus等；第4～5章解读了漏洞利用的过程、工具和技巧，包括获得远程服务访问权限、密码重置和破解、嗅探网络流量、自动化漏洞攻击和Web漏洞扫描、Web服务器扫描、拦截请求、代码注入、跨站脚本等流行的黑客技术及工具；第6章介绍了使用后门和rootkit的方法及注意事项，侧重讲解Netcat、Cryptcat、Netbus工具和常用rootkit的使用、检测和防御技术；第7章着重介绍了如何编写渗透测试报告。
每一章的结尾都有扩展阅读，包括对一些工具的介绍和相关深入主题的讲解，使有兴趣的读者可以找到自我提升的方向。

# <<渗透测试实践指南>>

## 作者简介

Patrick
Engebretson，高级渗透测试专家，达科他州立大学信息安全专业博士。
专注于渗透测试、黑客活动、入侵检测、漏洞利用、蜜罐技术和恶意软件的研究和实践，于多个领域发表了多篇颇负盛名的专业论文。
曾受国土安全部的邀请，在华盛顿特区软件保障论坛上介绍其研究成果，并在拉斯维加斯黑帽大会上发表演讲。
活跃于高级开发人员社区和渗透测试社区，同时拥有多种认证证书。

# <<渗透测试实践指南>>

## 书籍目录

## 章节摘录

第1章渗透测试本章知识点Backtrack Linux介绍使用Backtrack：启动引擎黑客实验环境的搭建与使用渗透测试的步骤1.1内容简介渗透测试是一种合法且授权定位计算机系统，并对其成功实施漏洞攻击的方法，其目的是为了使这些受测系统更加安全。
测试过程包括漏洞探测和提供概念证明（Proof of Concept，POC）攻击，以证明系统漏洞确实存在。
一个恰当的渗透测试会在完成之后，标明发现的系统漏洞并给出明确的修补意见。
总之，渗透测试用于加强计算机和网络系统的安全性，让它们在未来的使用中免遭攻击。
渗透测试（Penetration Testing或者Pen Testing，PT）也称为：黑客活动（Hacking）道德黑客（Ethical Hacking）白帽黑客（White Hat Hacking）我们有必要花些时间讨论一下渗透测试和漏洞评估（vulnerability assessment）之间的区别。
许多安全领域中的人士（还有厂商）在使用时都会混淆这两个术语。
所谓漏洞评估是检查系统和服务是否存在潜在安全问题的过程，而渗透测试则是通过执行漏洞利用和概念证明（POC）攻击来证明系统确实存在安全隐患。
渗透测试能够模拟黑客行为并提供攻击载荷（payload），它比漏洞评估更进一步。
本书将把漏洞评估的全过程作为完成渗透测试众多步骤之一进行介绍。

## 媒体关注与评论

“ 你是否听说过渗透测试但不知道它包含哪些内容？
本书就是你步入渗透测试领域的良好开端，它简单易读，也不需要什么先验知识，而且其内容也是当前最流行的。
我诚挚向你推荐Pat的最新力作。
”——Jared Demott，Crucial Security股份有限公司首席安全研究员

# <<渗透测试实践指南>>

## 编辑推荐

《渗透测试实践指南:必知必会的工具与方法》编辑推荐：Amazon五星级超级畅销书，美国国家安全局主管Keith B. Alexander将军（向奥巴马汇报）鼎力推荐！

## 名人推荐

你是否听说过渗透测试但不知道它包含哪些内容？
本书就是你步入渗透测试领域的良好开端，它简单易读，也不需要什么先验知识，而且其内容也是当前最流行的。
我诚挚向你推荐Pat的最新力作。
——Jared Demott，Crucial Security股份有限公司首席安全研究员

# <<渗透测试实践指南>>

## 版权说明