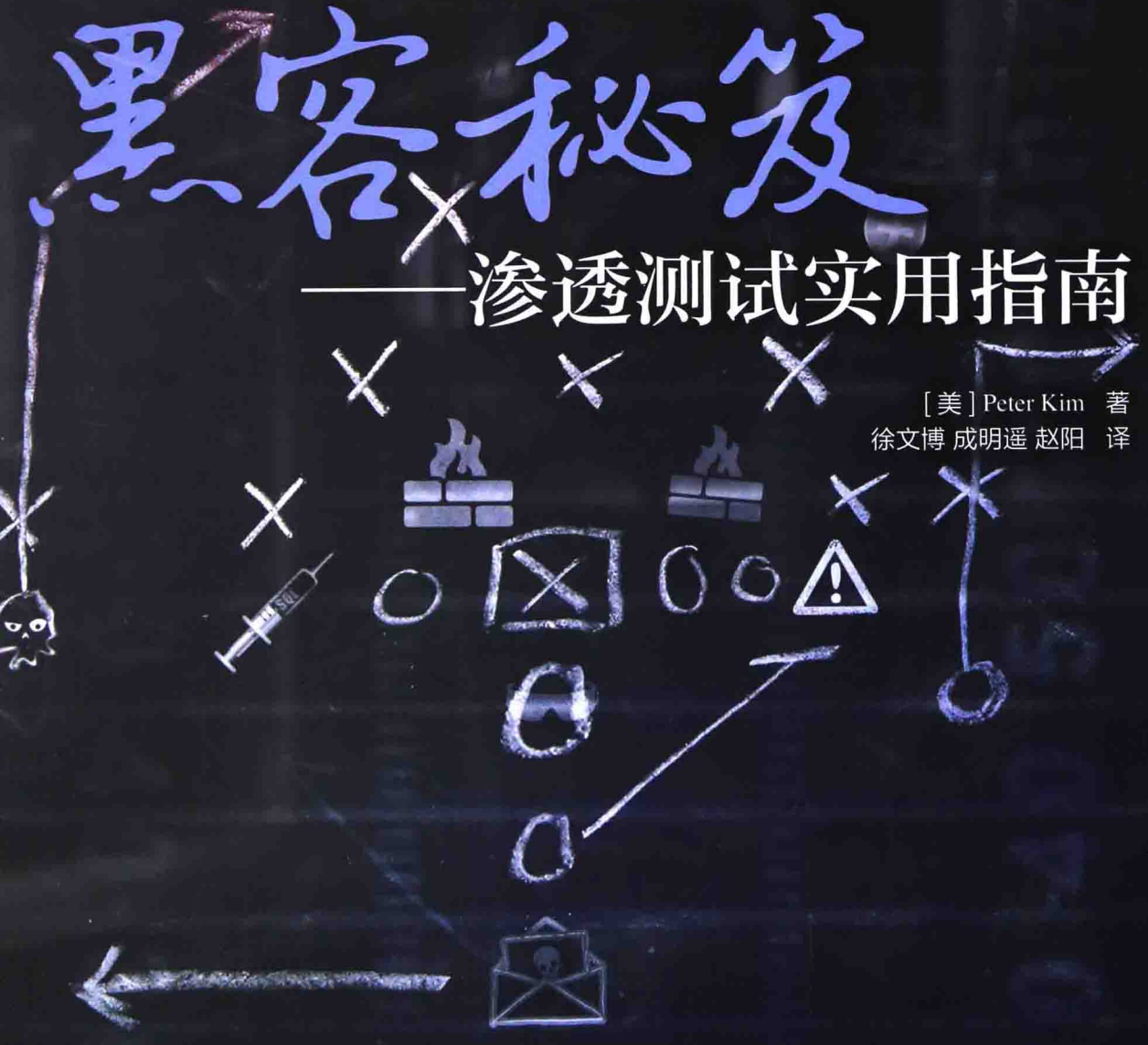
信息安全技术丛书

黑客秘笈

——渗透测试实用指南

[美] Peter Kim 著
徐文博 成明遥 赵阳 译



THE HACKER PLAYBOOK

Practical Guide To Penetration Testing

中国工信出版集团
人民邮电出版社
POSTS & TELECOM PRESS

黑客秘笈

——渗透测试实用指南

[美] Peter Kim 著
徐文博 成明遥 赵阳 译

人民邮电出版社
北京

图书在版编目（CIP）数据

黑客秘笈 : 渗透测试实用指南 / (美) 基姆(Kim,P.) 著 ; 徐文博, 成明遥, 赵阳译. -- 北京 : 人民邮电出版社, 2015.7
ISBN 978-7-115-39368-5

Ⅰ. ①黑… Ⅱ. ①基… ②徐… ③成… ④赵… Ⅲ. ①计算机网络－安全技术 Ⅳ. ①TP393.08

中国版本图书馆CIP数据核字(2015)第124307号

版权声明

◆ 著 [美]Peter Kim
译 徐文博 成明遥 赵 阳
责任编辑 傅道坤
责任印制 张佳莹 焦志炜

◆ 人民邮电出版社出版发行 北京市丰台区成寿寺路 11 号
邮编 100164 电子邮件 315@ptpress.com.cn
网址 http://www.ptpress.com.cn
三河市海波印务有限公司印刷

◆ 开本：800×1000 1/16
印张：13.25
字数：252 千字 2015 年 7 月第 1 版
印数：1－2 500 册 2015 年 7 月河北第 1 次印刷

著作权合同登记号 图号：01-2014-4189 号

定价：45.00 元

读者服务热线：(010)81055410 印装质量热线：(010)81055316
反盗版热线：(010)81055315

内容提要

所谓的渗透测试，就是借助各种漏洞扫描工具，通过模拟黑客的攻击方法，来对网络安全进行评估。

本书采用大量真实案例和集邮帮助的建议讲解了在渗透测试期间会面临的一些障碍，以及相应的解决方法。本书共分为 10 章，其内容涵盖了本书所涉的攻击机器/工具的安装配置，网络扫描，漏洞利用，人工地查找和搜索 Web 应用程序的漏洞，攻陷系统后如何获取更重要的信息，社工方面的技巧，物理访问攻击，规避杀毒软件的方法，破解密码相关的小技巧和最终的成果汇总等知识。

本书编排有序，章节直接相互独立，读者可以按需阅读，也可以逐章阅读。本书不要求读者具备渗透测试的相关背景，但是如果具有相关的经验，对理解本书的内容会更有帮助。

序

这是一本有关渗透测试方面的技术书籍。不过在起笔之前，我并没有打算撰写这样一本书。最初，我只是将日常的渗透测试、安全会议、安全性文章、有关研究和上手经验等整理为文字。没想到随着笔记的日积月累，我也逐渐整理出可重复完成渗透测试的工作方法，慢慢领悟到哪些操作有用，哪些没有用。

后来我开始从事教学工作，并应邀在会议上做演讲，逐步涉足信息安全行业。这些工作经验使我相信，我的经验和教训同样会对业内的朋友有所帮助。于是，我将个人的知识、经验和教学凝聚为此书。需要着重指出的是：我不是一个职业的作家，只是出于爱好写了这本书。您可能有个人喜欢的其他工具、技术和使用的技巧，正因如此，渗透测试的工作才会变得如此精彩纷呈。同一个问题的答案常常不止一个，我邀请您逐一探索。此外，本书不可能一步一步地详细介绍每种类型的攻击，不过，不断地研究、摸索各种不同的方法，寻求适合实际情况的各种方案——这本来就是渗透测试工作的特点。

如果您大体了解常用的安全工具，接触过 Metasploit，并在一定程度上跟得上安全行业的变化，那么您适合阅读本书。本书不仅面向渗透测试的从业人员，而且同样适合对信息安全感兴趣的行业爱好者阅读。

本书主要阐述了一种简单实用的渗透测试方法。确实有很多安全相关的图书详尽地介绍了各种工具和每种类型的安全漏洞，但是对于一般的渗透测试人员而言，那些书的指导意义并不大。我希望我写的这本书能够丰富您的安全知识，深入理解安全防范措施。

本书由真实的渗透技术以及典型的渗透测试的过程组成。虽然书中介绍的每种技术和操作过程不可能都与读者实际的渗透工作相吻合，但是这些知识无疑能够为您的渗透测试工作奠定良好的基础。

我个人认为，想要成为一个出色的安全行业专业人员，应当注重：

1．学习、研究并了解各种常见的安全漏洞和安全弱点；

2．在受控环境中，不断练习利用安全漏洞及防止漏洞被利用的方法；

3．在真实的环境下进行渗透测试；

4．在信息安全行业内开展教学并参与演讲。

上述 4 点构成了可持续的生命周期，有助于您不断地提高技术熟练度。请允许我再次感谢您能阅读这本书，我希望您能够通过本书体会到渗透测试的乐趣。

前言

在灯光昏暗的房间角落里，您在键盘前缩成一团，一瓶一瓶地喝着提神饮料，却丝毫打不起半点精神，只能百无聊赖地摆弄着手机。您懒得扭头，用眼角的余光瞥了亮得刺眼的液晶屏一眼，勉强看出现在已经是凌晨 3 点。“还没失败”，还在为自己打气。即使还没有找到任何一处关键漏洞，也没搞定任何 exploit，不过现在距离渗透测试的结束时间还有 5 个小时。问题是：虽然扫描工作略有收获，但是也不能期待客户会接受只有 cookie 安全标志问题的安全报告。

这个时候，您随手拾起本书，不禁开始向圣母玛利亚进行祷告“但愿那里有最后的希望”。然后通读了书中第 4 章，并意识到自己没有利用 cookie 来进行 SQL 注入攻击。“网络扫描程序不是万能的，它做不了这种检测”——想到这些，您再次打开 SQLMap，并设置好 cookie 选项重新运行。几分钟后，屏幕开始快速地滚动，最终停了下来。此时屏幕上的内容是：

Web server operating system: Windows 2008

Web application technology: ASP.net, Microsoft IIS 7.5

Back and DBMS: Microsoft SQL Server 2008

太棒了！用 SQLMap 注入获取了一个交互 shell。不过，此时并没有主机的管理权限，您又开始感到沮丧。“下一步该怎么办？要有些锦囊妙计就好啦”。突然想起这本书或许能帮上忙，于是打开到第 5 章阅读起来。这里给出了许多的方法，但首先看看主机是否连到了域中，是否使用了组策略首选项（Group Policy Preference，GPP）来设置本地的管理权限。

用 IEX Power Shell 命令，在服务器上下载了 PowerSploit 的 GPP 脚本，然后执行脚本，并将运行结果保存为文件。脚本运行正常，没有被反病毒软件拦截！您打开脚本程序导

出的文件……瞧，拿到了本地管理密码！

接下来大家都知道了：以管理员权限运行 Meterpreter shell，而后在该主机上运行 SMBexec 程序，导出在域控制器中的所有用户信息。

当然，这是一个渗透流程的粗略介绍而已。不过，本书将围绕这个流程组织内容。全书共分为 11 章，以橄榄球的行话阐述渗透测试的战术。这 11 章内容分别如下所示。

- 第 1 章，赛前准备——安装：关于如何配置本书所用到的攻击机器、工具。
- 第 2 章，发球前——扫描网络：在出招之前，需要进行扫描，了解即将面对的环境。本章将深入探讨寻找目标信息、智能扫描的相关内容。
- 第 3 章，带球——漏洞利用：利用扫描中所发现的漏洞，对系统进行攻击。从现在开始我们就着手行动了。
- 第 4 章，抛传——Web 应用程序的人工检测技术：有时，您需要发挥创意，寻找公开的目标。我们将会看看如何手动地寻找、攻击 Web 应用。
- 第 5 章，横传——渗透内网：攻陷一个系统后，如何通过网络获取更重要的信息。
- 第 6 章，助攻——社会工程学：通过表演来迷惑敌人，本章将解释一些社会工程学方面的技巧。
- 第 7 章，短传——需要物理访问的攻击：一个要求很近距离的漂亮短踢。这里将描述需要物理访问的攻击。
- 第 8 章，四分卫突破——规避反病毒检测：当您距离很近时，偷袭是很棒的。多数情况下，您会面临反病毒软件的阻挠。为解决这一阻碍，本章将介绍规避杀毒系统的方法。
- 第 9 章，特勤组——破解、利用和技巧：破解密码、漏洞利用，以及一些小技巧。
- 第 10 章，赛后——分析报告：比赛过程分析和成果汇报。
- 第 11 章，继续教育：与读者分享为提升渗透测试水平而有必要做的一些事情，如参加安全会议、参加培训课程、阅读相关图书、研究漏洞框架、参加 CTF 比赛等。

本书将会讨论攻击不同的网络、通过跳板越过安全控制、规避反病毒软件检测的有关策

略。不过在此之前，您应该正确地认识这些概念。如果公司指定您为渗透测试专员，要求您对一家世界 500 强公司的安全进行整体测试，您将从哪着手呢？您的安全测试基线是什么？如何为您所有的客户提供持续的测试呢？什么时候又会偏离基线呢？这正是我想在本书中所传递的信息。

关于本书的附加信息

应当说明的是，本书仅代表我个人的想法、经验。本书内容并不牵扯我先前或当前的雇主，也不针对本书之外的任何人或任何事。如果您发现某些主题、想法的表述方法不当，或者没有按照行业准则提及文献作者的名字，请告诉我。如果发生了这种情况，我会在本书的网站上进行勘误：www.thehackerplaybook.com。

建议读者在学习书中知识的时候，首先使用工具上手练习，然后用其他脚本/编程语言来重新编写这些工具。我通常喜欢用 Python 重新编写一些常见的工具和新的 exploit。这种学习方法不仅可以避免过度依赖现有工具，而且能够帮助您更好地理解漏洞的原理。

最后，我想强调的是“熟能生巧”。人们常说只要功夫深，铁杵磨成针。虽然我不相信有人可以完全掌握渗透测试的所有知识，但我相信，通过不懈的努力，您可以自然而然地领悟到渗透测试的要领。

免责声明

在此，本书像每本道德黑客图书那样强调：不要扫描、攻击或测试那些不归您管理的或者没被授权进行安全评估的系统。还记得这样的案例吗：一个加入匿名组织的家伙进行了 1 分钟的网络攻击，就被处罚了 183 000 美元[1]。在进行渗透测试之前，应当确保您将要做的每件事都获得有关公司、ISP、主机托管服务供应商，或者其他任何可能在测试期间受到影响的人和公司的书面许可。

在测试真实的生产环境之前，首先要在测试环境中进行完整的渗透测试。任何类型的渗透测试都有可能会攻破被测系统，甚至导致严重的后果。

---

[1] http://mashable.com/2013/12/09/anonymous-attack-fine/。

在您阅读正文之前，请注意：本书并没有囊括所有的攻击类型，书中介绍的方法也并不一定都是最好或者最有效的方法，这仅是我挑选出来的很实用的方法。如果您发现任何的错误，或者发现更好的测试方法，请尽管告诉我。

目录

第 1 章　赛前准备——安装

本章将直接探讨攻击系统的配置方法。安全测试最为重要的方面就是有一个可重复的流程。所以，您需要有一套标准化的基准系统、测试工具和测试流程。本章将会讲解配置测试平台的方法，以及本书示例所需的额外工具的安装步骤。只要按照本章的步骤配置测试平台，您就能够重现后续章节中我所提供的案例、演示。好！让我们全力以赴、积极备战吧。

1.1　搭建渗透测试主机

在进行渗透测试的时候，我都会配置两套不同的测试主机。其中一台是 Windows 主机，另外一台则是 Linux 系统的主机。如果您习惯其他操作系统的测试平台，那就用您所习惯的。重要的不是操作系统，而是创建基准测试系统的方法，并且在每次渗透测试任务中应能一直使用这个基准系统。配置好主机以后，我会对这干净、配置好的虚拟机做个快照。这样，在日后进行其他测试时，只要还原虚拟机到快照时的基准状态、安装补丁、进行升级，再安装所需的其他额外工具就可以了。请相信我，对基准系统进行快照备份绝对是磨刀不误砍柴功的工作。在过去的测试里，我在安装工具的过程中就浪费过不计其数的时间。

1.1.1　硬件规格

我们首先要选择一台运行状态良好的电脑，然后再在上面下载虚拟机，安装各种测试工具。下面是些推荐，您可以对此做出自己的判断。不管您是运行 Linux、Windows，还是 OS X 作为基准系统，只要确保基准系统没有被恶意软件感染就可以了。

1. 基本的硬件要求

运行多个虚拟机真的很耗费资源，所以测试平台的硬件要求可能高于一般家用电脑。

- 至少有 8GB 内存的笔记本电脑。
- 500GB 的硬盘空间，最好还是固态硬盘。
- Intel i7 四核处理器。
- VMWare Workstations/Fusion/Player 或者 Virtual Box。
- 外置的 USB 无线网卡——我用的是 Alfa AWUS051NH。

2. 后文演示用到的可选硬件

- 用于密码破解的显卡（这要安装到工作站上）。
- 一些 CD 或者闪存驱动器（用于社工）。
- Dropbox - Odroid U2。

1.1.2 商业软件

如果您要进入渗透测试领域，我强烈推荐您购买下列软件的许可证。您也可以推荐工作的单位购买它们，毕竟这些软件的价格可能很贵。不是说非这些工具不可，但是它们确实可以简化您的操作。特别是下文提到的 Web 应用程序扫描器，虽说它们通常价格昂贵，但是其效能确实很高。下文列举了各种类型的扫描器程序。当然了，我只介绍了那些使用过的觉得容易上手的扫描器。

这些工具各有所长，若要进行功能比较，可以阅读 HackMiami Web Application Scanner 2013 PwnOff（http://hackmiami.org/whitepapers/HackMiami2013PwnOff.pdf）上的白皮书，或者参考 sectooladdict.blogspot.com（http://sectooladdict.blogspot.com/ 2012/07/2012-web-application-scanner-benchmark.html）上的早期文章。

- Nexpose/Nessus 漏洞扫描器（高度推荐）。
  - Nexpose: http://www.rapid7.com/products/nexpose/。
  - Nessus: http://www.tenable.com/products/nessus。

这两款工具都很出色，但它们个人版许可证的价格却相差很多。相比而言，个人版的 Nessus 更便宜一些。它们都是业内普遍使用的漏洞扫描器。

- Burp Suite（http://portswigger.net/burp/）——Web 应用程序扫描器和手动 Web App 测试（高度推荐）。
  - 必备工具。该软件的功能强大，更新速度也很快。Burp Suite 的价格大概是 300 美元左右。如果觉得其价格过高，可以试试 OWASP 的 ZAP 扫描器（http://www.owasp.org/index.php/OWASP_Zed_Attack_Proxy_Project）。ZAP 扫描器的功能和 Burp Suite 相似，而且其作者也在积极进行维护。本书案例使用的是 Burp Suite 专业版，因为我发现这是一款相当高效的工具。
- 自动化的 Web 应用扫描器（下面两个工具都很不错，您可以根据预算进行相应选择）。需要强调的是，因为它们都是非常简单易用的工具，所以本书不再详细介绍其中的任何一款工具。尽管如此，在进行专业的 Web 应用程序测试时，或者给企业提供定期 Web 测试时，这些专业的工具还是非常实用的。
  - IBM AppScan: http://www-03.ibm.com/software/products/en/appscan。
  - HP Web Inspect: http://www8.hp.com/us/en/software-solutions/software.html? comp URI=1341991。

1.1.3　Kali Linux（http://www.kali.org）

Kali 属于渗透测试专用的发行版 Linux，它收录了渗透测试所需的多数常用工具。安全界内的大部分人已经把它当作了一种普遍认可的标准系统，而且还有人在这个框架上进行二次开发。此外，您可以添加一些自己的工具。虽然 Kali 发行版已经自带了像 Windows Credential Editor（WCE）这类工具，但我们在实际过程中最好下载最新版本的 WCE 程序。此外，为了满足规避反病毒软件的常见需求，我们还要对 Kali 的工具进行相应修改。但是，我会把修改后的程序保存在单独的文件夹中，而不是覆盖原来的 Kali 程序。

其实许多的发行版都很不错，推荐读者试试 Pentoo（http://www.pentoo.ch/）。现在，我们一起来深入了解 Kali 吧。