异步图书
www.epubit.com.cn

信息安全技术丛书

THE HACKER PLAYBOOK 2

Practical Guide To Penetration Testing

黑客秘笈

——渗透测试实用指南（第2版）

[美] Peter Kim 著
孙勇 译

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

（第2版）

[美] Peter Kim 著
孙勇 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 : 第2版 / (美) 皮特·基姆 (Peter Kim) 著 ; 孙勇译. -- 北京 : 人民邮电出版社, 2017.2
ISBN 978-7-115-44245-1

Ⅰ. ①黑… Ⅱ. ①皮… ②孙… Ⅲ. ①计算机网络－网络安全－指南 Ⅳ. ①TP393.08-62

中国版本图书馆CIP数据核字(2017)第005798号

版权声明

◆ 著　[美] Peter Kim
译　孙　勇
责任编辑　傅道坤
责任印制　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
北京艺辉印刷有限公司印刷

◆ 开本：800×1000　1/16
印张：23.5
字数：402 千字　2017 年 2 月第 1 版
印数：1 – 3 000 册　2017 年 2 月北京第 1 次印刷

著作权合同登记号　图字：01-2015-7466 号

定价：79.00 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

本书是畅销书《黑客秘笈——渗透测试实用指南》的全新升级版，对上一版内容进行了全面更新，并补充了大量的新知识。本书采用大量真实案例和极有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 12 章，涵盖了攻击机器/工具的安装配置，网络扫描，漏洞利用，网站应用程序的人工检测技术，渗透内网，社会工程学方面的技巧，物理访问攻击，规避杀毒软件检测的方法，破解密码相关的小技巧和分析报告、继续教育等知识。

本书编排有序，章节之间相互独立，读者既可以按需阅读，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《黑客秘笈》的第 2 版。有些读者已经阅读过第 1 版。当前版本是第 1 版的扩充。下面简要地介绍书中新增的漏洞和攻击技术。除了增加这些新的内容，当前版本中也包括第 1 版涉及的攻击技术和方法。这些技术和方法在当前依然具有应用价值，读者不需要查阅本书第 1 版就可以了解和掌握相关内容。那么，哪些是新增加的内容？最近一年半以来出现的一些新攻击技术包括：

- 心脏出血；
- ShellShock；
- Kerberos 问题（金票据/万能钥匙）；
- Postgres 数据库的哈希传递攻击；
- 新型网络钓鱼攻击；
- 性价比高的渗透便携设备；
- 快速/智能密码破解；
- 新型 WIFI 攻击；
- 大量 PowerShell 脚本；
- 提升权限攻击；
- 大规模网络突破；
- 横向渗透；
- Burp 模块；

- 打印机漏洞利用；
- 后门工厂；
- ZAP 代理；
- 粘滞键攻击；
- NoSQL 注入；
- 商业工具（Cobalt Strike、Canvas 和 Core Impact）；
- 实验部分。

除了介绍最近两年攻击技术的变化，我也尝试将第一本书读者的评论和反馈加入到新书中。本书深入地讨论如何搭建攻击技术的实验室测试环境，以及渗透测试最新的技巧和诀窍。最后，由于很多学校已经将我的书作为教科书，所以我尽量使得新版本的内容更加易于理解和掌握。为了帮助读者掌握测试脆弱点或漏洞的方法，我已经尽可能增加实验测试的章节。

本书有什么是不变的呢？从写第 1 版时，我的一个目标就是尽可能地模拟真实的渗透环境。我尽可能不讨论理论攻击技术，而重点介绍实践证明的攻击技术和现实世界应用的攻击技术。我的第二个目标是强化您对渗透测试人员价值的深入了解。换句话，我想鼓励您用不同的方法提升您的价值，从而为您现在的公司、未来的公司或客户带来收益。如果仅仅是提交漏洞扫描工具和扫描生成的报告，那么这样的报告对于一个公司来说并没有什么真正的价值。同样，如果只对非常小的领域开展渗透测试，那么测试的结果会使渗透测试人员和用户对系统的安全造成错误的认识。对于阅读过第 1 版的读者来说，您尽管放心，虽然可能在第 2 版中看到相似的内容，但是第 2 版中确实有大量新的内容，第 2 版有第 1 版两倍的内容。另外，为了满足读者的需求，我创建了大量的脚本和工具，用来帮助您开始黑客冒险历程。这可能是读者提出最多的需求之一，因此我创建了大量的脚本在我的 Github（https://github.com/cheetz）上，尽可能使读者都能掌握课程的内容。

对于没有读过本书第 1 版的读者，您可能很疑惑，我作为渗透测试人员，有什么样的经历。我有 8 年的渗透测试经验，测试的对象包括大型的金融机构、大型的公用事业公司、财富 500 强企业和政府机构。多年来我也讲授攻击网络安全课程，在 Toorcon/Derbycon/BayThreat 等安全会议上做过主题发言，在多个安全杂志上发表论文，目前在南加州经营

一个安全社区，成员超过 300 人。希望您能够学会我所掌握的技能，并融入到自己的安全研究工作中。

从技术角度看，很多工具和攻击方法在过去的几年中已经发生变化。随着哈希传递和组策略首选项等攻击漏洞被打上补丁，攻击者的过程和方法也发生了变化。

一个重要提示是我同时使用商用工具和开源工具。对于每一个商用工具，我都会尽可能找到对应的开源工具。偶尔会遇到某些渗透测试人员，他们表示只使用开源工具。作为渗透测试人员，我发现很难发表这样的声明。“坏小子”没有仅使用开源工具的限制，因此如果要模拟“真实世界”的攻击，您需要使用任何有助于任务完成的工具。

谁是这本书的读者？您可能需要具备微软活动目录的一些操作经验，深入地了解 Linux，掌握一些网络背景知识和编码经验（Bash、Python、Perl、Ruby、PHP、C 或者其他编程语言），以及使用过漏洞扫描器和漏洞利用工具（例如 Metasploit）。如果您没有相关领域的知识专业背景，但是对于从事渗透测试工作有兴趣，我建议一定要掌握上述基本知识。如果不事先掌握系统工作原理等基本知识，您不可能很快胜任渗透测试工作。

这本书不仅仅适用于那些准备进入或正在从事网络渗透的人员，同时为应急响应人员提供宝贵的知识和经验，因为他们需要知道攻击者是怎么想的以及他们使用什么样的攻击方法。

最后，我想讨论一下研究人员与渗透测试人员的区别。很多时候，这两个职业混为一谈，因为两个职业在各自的工作领域都需要知识渊博。然而，在这本书中，我简单区分两个领域，重点关注渗透测试领域。在本书中，要澄清两者的区别。研究者关注单个或有限的领域，花费大量时间逆向应用程序/协议/操作系统。他们的目标是针对特定的脆弱点发现未知的漏洞。另一方面（记住这是一般情况）渗透测试人员利用公开的漏洞利用程序渗透突破系统和应用程序。这当中也有一些重叠的地方——渗透测试人员同样也使用模糊测试方法测试脆弱点（例如 Web 参数），查找 0-day 漏洞，但是他不会像研究人员那样花费大量时间查找所有的脆弱点和漏洞，而研究人员可能要这样做。

声明和责任

本书不是要将您变成某一种类型的超级黑客。要成为超级黑客需要在这个领域进行大量的练习、研究探索和始终痴迷。希望通过阅读本书，您能够打破常规，更有创意，对于各种系统漏洞的产生有更深入的了解。请记住，您只有操作测试系统的权利。请在 Google 搜索关键词“hacker jailed（黑客监禁）”，您会看到大量不同的案例，某些青少年由于做了他们认为“很好玩”的事情而被入狱多年。网络上很多免费的平台允许对其使用合法的技术，并且能够帮助您提高能力。

前言

您已经被一家大的安全行业公司（Secure Universal Cyber Kittens, SUCK）聘为渗透测试人员。公司开发新型武器，这些武器提供给出价最高者使用，您已经被授权杀死……好的，或者不杀死，只是授权攻击。您已经被完全授权，允许使用工具箱中的任何工具和策略，突破目标网络，窃取公司的商业秘密。

当您带上笔记本电脑、潜伏设备（故意遗失在目标网络周围，用于跳板代理）、橡皮鸭子（USB 接口物理渗透工具）、Proxmarks（RFID 破解设备）和连接线，您几乎忘了最重要的事情——黑客秘笈第 2 版。您应该知道本书可以帮助摆脱最困难的情况。您的思绪回到上一次任务。在复制一些胸卡，并在网络设备附近部署潜伏设备后，您跑出办公室，几乎潜行绕过安全保卫人员。潜伏设备回联到 SSH 设备，您已经进入目标网络。您想安静地潜伏在网络中，不想触发任何入侵检测设备发出警报。您想寻找什么呢？您翻到书中第 3 章中打印机的相关内容。您探测周围的多功能打印机，查看是否设置为默认密码。太棒了！您重新配置打印机的轻量目录访问协议，设置了 netcat 监听程序，获得了活动目录的凭证。因为不知道这些凭证具备什么权限，您尝试设置 SMBexec 净荷，使用 psexec 程序，访问 Windows 主机。由于凭证是有效的，因此您已经是普通用户了。通过使用第 5 章中 PowerTools 的一些小技巧，您成为本地管理员，并且使用 Mimikatz 工具获得内存密码。哎……您叹息……这太简单了。在获得一些账户密码后，您找到域管理员所在的主机，登录主机后又获得一些密码。获得域管理员凭证后，使用 psexec_ntdsgrab 工具可以非常直接地从域控服务器导出哈希值，然后清除您的痕迹……

很高兴您没有忘记带上本书！

标准

在开始阅读本书之前，需要理解一些渗透测试使用的基本概念和标准。这是探测、漏洞

挖掘、漏洞利用和撰写渗透测试报告的基础。开展渗透测试工作没有什么标准的方法，但是至少需要掌握如下基本知识。

渗透测试实践标准（PTES，地址 http://www.pentetstandard.org/index.php）：它是目前开展渗透测试的标准。在从事渗透测试工作中，标准中的内容经常被参考引用，并且是核心的部分。由于渗透测试实践标准技术指南包括所有技术细节，因此我强烈推荐您通读一遍。标准收录的模块主要包括以下7个小节：

1．预交互；

2．情报搜集；

3．威胁建模；

4．脆弱点分析；

5．漏洞利用；

6．后漏洞利用；

7．撰写报告。

我鼓励您做的一件事就是充满创造力，找到什么方式最适合您。对我来说，尽管在开展渗透测试时，渗透测试实践标准是一个非常好的模型，但是我在从事渗透测试时喜欢对标准模型做细微的调整。根据经验，我通常喜欢使用下面的流程：

1．情报搜集；

2．最初的立足点；

3．本地/网络枚举；

4．本地权限提升；

5．持续控制；

6．横向渗透；

7．域权限提升；

8．导出哈希值；

9．信息识别/提取；

10．撰写报告。

通过对渗透测试工作进行分解，我掌握要做什么以及重点是什么。通过社会工程，在获得了最初的立足点之后，重点是获得一个高权限账户。为了实现这个目标，需要枚举系统/网络资源，查找错误的配置或者本地主机的脆弱点。同时需要实现持续控制，以防远程终端连接丢失。在获得系统或者提升权限后，需要观察是否能获得域特权账户。为了实现目的，需要渗透其他主机，以便最终获取域管理员权限。登录域控服务器后，渗透测试最重要的一步就是导出域哈希值，休息一会儿跳支舞。渗透测试不应当到此为止。用户最关心的事情是找到敏感的数据，特别是个人身份信息、知识产权或者其他用户指定的信息。最后，正如我们知道的，渗透测试工作要根据报告支付薪酬，拥有一个好的标准模板和有价值的数据，使您在竞争中脱颖而出。

当然，这只是非常快速和比较抽象的举例，列举了评估过程涉及的内容。为了帮助您了解这个过程，我已经尝试开发了一个模板，帮助您开展渗透测试。本书包括 12 章，布局是按照橄榄球的战术编排的。但是，请不要担心，您在读这本书时，没有必要知道橄榄球术语的细节，下面是本书的各个章节介绍。

- 第 1 章，赛前准备——安装：本章介绍如何搭建实验室、攻击主机和整本书中用到的工具。
- 第 2 章，发球前——扫描网络：在开展各种操作前，需要仔细查看环境，了解面对的情况。我们将带您发现和智能扫描目标系统。
- 第 3 章，带球——漏洞利用：基于第 2 章中发现的漏洞，渗透突破目标系统。在本章中，我们需要人工操作实践，渗透突破目标系统。
- 第 4 章，抛传——网站应用程序的人工检测技术：有时候查找互联网公开的目标时，您需要变得具有创造性。我们将深入探讨如何手动搜索和攻击网站应用程序。
- 第 5 章，横传——渗透内网：在已经突破一个系统后，将讨论采用多种方法，横向渗透网络。
- 第 6 章，助攻——社会工程学：通过表演欺骗对手。本章将解释一些社会工程学方面的策略。

- 第 7 章，短传——物理访问攻击：一个精妙的短传需要距离短。在这里，将介绍物理攻击方法。
- 第 8 章，四分卫突破——规避杀毒软件检测：当仅仅距离几码时，四分卫突破是最适合的。有时候您无法摆脱杀毒软件的查杀，本章介绍如何规避杀毒软件，克服上述障碍。
- 第 9 章，特勤组——破解、利用和技巧：破解密码、漏洞利用、NetHunter 和一些技巧。
- 第 10 章，两分钟的操练——从零变成英雄：您只有两分钟的时间，需要从没有访问权限提升到最高域管理员权限。
- 第 11 章，赛后——分析报告：撰写渗透测试报告，汇报成果。
- 第 12 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。

更新

正如大家知道的，安全知识更新速度很快，事情一直在发生变化。我尽量对所有的变化以及您可能有的请求保持更新。您可以从下面找到更新。

本书更新订阅网址：http://thehackerplaybook.com/subscribe

推特：@HackerPlaybook

网址：http://TheHackerPlaybook.com

Github：https://www.github.com/cheetz

邮件：book@thehackerplaybook.com

目录