HZ BOOKS
华章科技

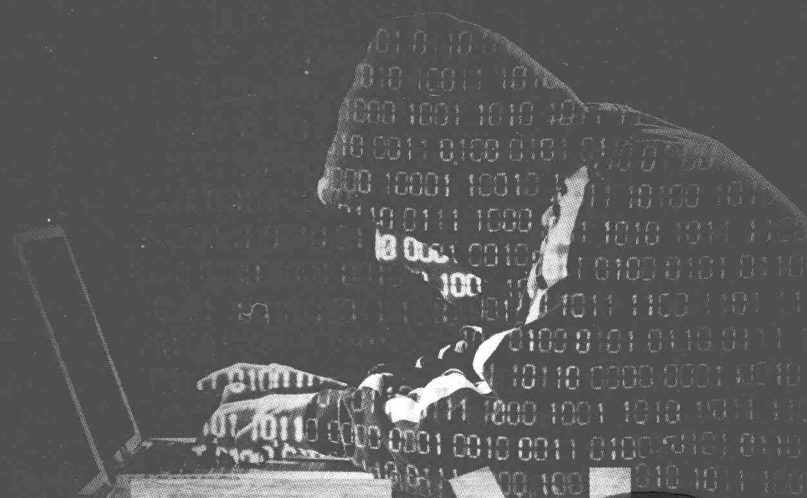
网站渗透测试实战入门

以最有效的方式测试网站漏洞/构筑完备的网站信息安全

- 实例引导佐以工具介绍，降低学习门槛
- 应用工具皆为免费软件，信息安全防护不求人
- 专注网站安全检测，目标明确，事半功倍
- 辅以完整的操作图例，强化渗透概念

陈明照 编著

机械工业出版社
China Machine Press



网站渗透测试实战入门

陈明照 编著

机械工业出版社
China Machine Press

图书在版编目（CIP）数据

网站渗透测试实战入门/陈明照编著.—北京:机械工业出版社, 2015.11

ISBN 978-7-111-51906-5

Ⅰ. ①网… Ⅱ. ①陈… 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252951号

本书版权登记号：图字：01-2015-1586

本书从实战的角度出发，通过网站渗透测试工具的介绍，详述如何建立系统安全防范意识，强化渗透测试的概念，如何防范新的安全弱点等，以保证从业者能够保护网络系统的信息安全；也尽可能降低新手的学习门槛。

本书主要包括渗透测试的基本程序、渗透测试的练习环境、网站弱点、信息搜集、网站探测及弱点评估、网站渗透、离线密码破解、渗透测试报告等内容。

本书内容全面，用浅显的文字让读者在短时间内，以最有效的方式一窥渗透测试的全貌，适合广大渗透测试的入门者阅读，也可供大中专院校信息安全及相关专业的师生学习参考。

网站渗透测试实战入门

出版发行：机械工业出版社（北京市西城区百万庄大街22号　邮政编码：100037）
责任编辑：夏非彼　迟振春
印　　刷：中国电影出版社印刷厂
开　　本：180mm×230mm　1/16
书　　号：ISBN 978-7-111-51906-5
版　　次：2016年1月第1版第1次印刷
印　　张：11.25
定　　价：39.00元

凡购本书，如有缺页、倒页、脱页，由本社发行部调换
客服热线：（010）88379426　88361066
购书热线：（010）68326294　88379649　68995259
投稿热线：（010）88379604
读者信箱：hzit@hzbook.com

序

我的主管对信息通信安全非常重视，除了定期委托其他专业机构对各系统进行安全检测外，也主导成立了自己的渗透测试及数字鉴别团队，笔者有幸受主管指派参与到这个团队中来。

因参与渗透测试及数字鉴别团队的缘故，多次受到指派参加其他专业机构举办的相关教育培训，因缘际会，曾受张裕敏、吴肯尼及洪光钧等老师的指导，老师们的教学方式生动有趣，让我了解到实施黑客技术也可以提升单位的防御能力，黑客技巧可以是建设，而不是破坏，故而对渗透测试产生莫大的兴趣，也纠正了我对系统入侵的偏执想法。

笔者是信息从业人员，虽然也受过相当程度的白帽黑客课程训练，并执行过很多次渗透测试操作，但渗透测试领域博大精深，涉及的专业知识不知凡几，到目前仍觉得无法参透渗透测试操作的精髓。

刚踏入渗透测试这道门时，我曾努力自学，寻找相关的书籍及网络信息，但心中一直有个缺憾——为什么找不到几本有参考性的操作性强一些的专业书籍呢？因此我想抛砖引玉，编写一本渗透测试方面的入门书，为想进入渗透测试领域的人提供更有价值、观念正确的学习教材。

相信有许多人跟我初学渗透测试时一样，老师大多都是蜻蜓点水带过，教了一堆工具软件，听的时候好像懂了，实际操作时又不知要用在什么地方，再者，每个老师都有自己惯用的工具组，虽然工具不同，但大部分都功能重叠，我们真的要学那么多工具吗？本书是从一个刚刚踏入渗透测试领域者的视角出发，希望用浅显的文字让初学者在短时间内以最有效的方式一窥渗透测试的全貌。

这本书并非我个人独力完成，要感谢我的好朋友陈庆龙、陈右龙在工作之余且身心俱疲的情况下，愿意为我校稿，并提供诸多建设性的修改意见；感谢我的主管，让我参与渗透测试操作，我的实力才能得以快速提升；还要感谢我的太太，时时鼓励我，在我有新的发现时，愿意倾听我的“高谈阔论”，纵然她不明白我说的内容，也能耐心听我描述，让我有继续提笔的动力。

笔者自认为还没有完全学会渗透测试，毕竟信息技术博大精深，个人才疏学浅，书中所述方法、观念或有偏误，敬请各位不吝指正。

编者

2015 年 6 月

改编说明

“信息安全”是信息化和网络化的核心话题之一，理论教科书枚不胜举，涉及“黑客技术”的书也铺天盖地。但是，像本书以“红客”视角写作的书却并不多见。

区分“黑客”(Hacker)和“红客”(Honker)不是看他们是否掌握了黑客技术，而且看他们用黑客技术来做什么。从另外一个方面来说，其实就是看“黑客”和“红客”对“矛”和“盾”专研的角度和深度。“黑客”更关注目标系统“盾”的漏洞——一点漏洞就够了，之后就研发或者使用专用的“矛”攻击“盾”的这个弱点，黑客往往在暗处，所以防不胜防。“红客”则更关注来自暗处的各种各样的“矛”，考虑如何构筑起完备的“盾”来抵御这些“矛”对目标系统或者网站的攻击。

本书就是一本为“红客”而著的“红客实战手册”，书中深入探讨了各种各样的“矛”，并运用它们进行实际的网站攻击，而后可以根据攻击的特点、特征和结果，重新构筑起网站“盾”的防御体系和防御策略。实战中的网站渗透测试就是为了检验用于保护网站安全的“盾”的坚固性和可靠性，因此“网站渗透测试”是评估、构筑和验收网站防御系统与策略的核心步骤。

本书从一个初踏入网站渗透测试领域的初学者出发，在较短的时间内，以最有效的方式让初学者一窥渗透测试的全貌。让读者学习到在真实的网络环境中，如何运用黑客技术和工具的“矛”进行“渗透”和“入侵”，以便发现网站的漏洞和防御弱点，将黑客技术用于网站“盾”的检测和检验，最终为构筑完备的“盾”提供思路和方向。

作者在书中介绍“渗透”和“入侵”的各种手段时，都列出了相应工具软件的来源，并配备了图文来详细说明这些工具的使用方法和步骤，即使是初学者也完全可以依照本书的说明，依葫芦画瓢地运用到自己的网站渗透测试的实际工作中。作者还细心地在附录中为读者提供了《渗透测试足迹搜集检查表》，读者可以参照运用于自己的网站渗透测试工作中。

赵军

2015 年 9 月

目 录

第 1 章
关于渗透测试

本章重点

- 渗透测试的目的
- 理论中的渗透测试
- 我眼中的渗透测试
- 渗透测试的入门知识
- 为什么只在网站中进行渗透测试
- 本书的目的
- 重点提示

当我们将系统部署到网站上时，系统就要面对成千上万的测试，其中不乏来自有心人士的“恶意”攻击，系统提供的服务越多，遭受攻击的概率就越高。虽然就“安全系统开发生命周期（SSDLC）”问题而言，系统从一开始规划就必须注重相关的安全防护，但一组系统的成型要经过多少人之手，如何保证每个人都尽到安全防护的责任呢？我们又该怎么验证呢？况且每天都有新的弱点、漏洞被发现，要如何得知我们原本安全的系统，是否也存在新的漏洞呢？要发现这些漏洞，就需要依靠测试来完成——良性的测试，也就是所谓的渗透测试。

为了让文字读起来不至于太饶舌，有些用语会交替使用，为了避免读者混淆或误解，现说明如下。

- 受测方、客户、委托方、雇主：都是指请（叫）我们进行渗透测试的人、单位或机关，当然也可以是你自己，以下用“甲方”表示。
- 标靶、受测系统、受测目标：都是指将要进行渗透测试的网站。
- 测试方、测试端：实际执行渗透测试的人，也就是我们自己！以下用“乙方”表示。
- 埠、通信端口、连接端口、端口：Port，个人觉得端口的用词比较接近于网络通信领域里“Port”的实际功用，所以大多场合都会称为“端口”，但有时为了句子顺口，也会采用“埠”、“通信端口”或“连接端口”。

渗透测试的目的

❖ 了解入侵者可能利用的途径

- 信息不当
- 网络架构之设计问题
- 防火墙之设置问题
- 系统及应用程序的漏洞

- 系统及应用程序的设置问题

了解系统及网络的安全强度

- 评估具同等能力的入侵者大约需花费多久的时间才能入侵成功
- 评估遭到入侵后可能造成的影响
- 评估信息通信安全政策的落实程度

了解弱点、强化安全

- 强化系统及网络的安全
- 降低遭到入侵后的损失

理论中的渗透测试

维基（WiKi）对于渗透测试（penetration test，或缩写为 pentest）的说法是：通过对计算机系统的攻击，发现系统可能的安全弱点，进而取得系统、程序功能或敏感数据的存取权。一般的说法是：利用黑客的观点、技术、工具对目标系统仿照黑客的攻击手法，以便找出系统的弱点或漏洞，并提供客户修补建议，以作为系统强化的手段。

所以渗透测试不是要击垮系统，而是找出弱点作为改善的依据，进行渗透测试时，依照甲方与乙方对此次测试操作内容的熟悉程度，可分为下列几种。

- 黑箱：甲方只提供受测目标的名称或 URL，乙方必须在测试活动期间自行搜集其他相关信息。感觉上，除了知道敌人是谁外，其他如敌人的部署、配备、数量全部未知，就像拿到一只看不透的黑箱子。使用黑箱测试，是在考验乙方的黑客技巧，因为这种模式最接近实际黑客攻击的情况。

- 白箱：甲方会尽可能提供标靶的信息，让乙方尽可能将精力放在找出受测系统的弱点（漏洞）上，因为乙方知晓受测目标的部署情形，可以事先拟好策略。就像拿到一只透明的箱子，可以知道箱子里放的是什么东西。使用白箱测试，是在考验系统的安全防护能力。
- 灰箱：当然有的时候甲方并不是那么清楚受测系统的信息（例如外包开发的系统），若无法主动提供完整的受测目标信息，乙方就无法事先取得系统信息，不过甲方还是尽可能协助乙方了解取得相当多的信息，所以灰箱是指介于黑箱与白箱之间的测试方法。
- 双黑箱：有时甲方想尽可能以模拟黑客攻击的情景进行测试，不仅要测验系统的防护能力，同时也要测试乙方人员的警觉性或应变能力，在对内部人员保密的情况下，暗地委托乙方进行渗透操作，相关人员并不知晓渗透测试的进行，而乙方亦无法得到详细的受测系统信息，因此，攻防双方都在暗地里较劲，故称之双黑箱（或双盲）测试。
- 双白箱：跟双黑箱相对，双方都知道彼此的存在，最主要的目的是乙方协助甲方找出并确认系统漏洞。

我眼中的渗透测试

实际上黑客的攻击没有时间、地点、目标、工具、手法的限制，为了达到目的，可以不择手段、持续不断、用尽任何可能的方法（APT 攻击）。但渗透测试却必须在有限的时间内（一般是 7～14 日），在双方（委托者与测试者）确定的目标范围、作业时间（例如晚上 8:00 至凌晨 6:00）及攻击手法（如可否进行社交工程）的限制下进行，故渗透测试无法完全反应黑客的攻击强度，就连攻击的手法也大有不同，譬如：渗透测试大多不会进行社交工程、阻断服务（DoS：Denial-of-service）攻击，不会（也不该）对受攻击系统注入木马或留下后门。因为测试操作有所限制，不要期望渗透测试可以帮我们找到所有的系统弱点，除非甲方自身持续进行渗透测试。

就我个人看来，渗透测试应该：

- 是“健康检查”，而不是攻击：渗透测试是为了提升甲方系统的安全性，尽早挖掘现存的弱点，作为改善的依据，而执行渗透测试必须兼顾系统服务的持续进行，要事先拟妥因进行测试造成系统停止服务的处理对策。
- 是稽查，而不是窃取：渗透测试可以印证甲方在信息通信安全政策方面的落实程度，是一种稽查行为，渗透测试结束后，相关信息必须完全交给甲方，作为甲方持续改进信息通信安全的策略参考，除非经甲方同意，否则乙方不该私自留存副本。
- 防护是测试的目的：渗透测试发现的弱点，必须提出相应的防护对策，以供甲方参考。

渗透测试是 POC（Proof of Concepts），只要证明有弱点、漏洞存在即可，不一定要对目标系统进行致命的攻击，就这一点看来，渗透测试对系统的危害比黑客攻击来得轻，相对的，渗透的深度也来得浅些。

渗透测试的入门知识

渗透测试是技术，也是艺术，必须要有创意，更需要耐力，不能只具备常规的想法，不按常理出牌也是很必要的，弱点常常不是一个步骤就可以找出来的，收集到的数据需要依靠经验仔细地交叉分析，测试的程序也需要反复执行，这些都是弱点扫描工具所不能涉及的地方，千万不要以为用工具扫描没问题，就认为系统没有漏洞了，漏洞往往是由“创意”制造出来的！

本书仅就渗透测试操作的步骤及常用的工具提供给读者参考，但在测试过程中所得到的信息如何解读，必须依靠读者对系统操作原理的了解程度及想象力了，渗透测试过程中涉及的每一项技术都是一门专业，其内容可以说是包罗万象，会得越多，能使用的渗透手法就越丰富，如 JavaScript、http/https 的运行原理、AJAX、SQL 等，这方面的技能只能请读者自我充实了！

这不是一本教你做黑客的书，本书的内容只是带你跨进渗透测试这道门，不要期待

看完本书就能成为专家。孙中山说：“知难行易”，因此本书不会传递太多的学术理论，而是以实战的角度看待入门学习，从实战攻击中得到的成果，会增强成就感。相信我，如果先叙述各种渗透测试的理论，大部分的初学者在学完第 1 章就萌生退意了，毕竟实战比说教更有趣！

虽然本书是以实战的角度切入，但信息通信安全终究不同于一般的程序设计或系统操作，有些基本知识还是必备的，书中不会详细介绍这些知识细节，有关下列的议题尚请读者自我学习：

- HTML 语法与网页运行原理
- JavaScript
- Command Line Interface（命令行界面）的操作（Windows、Linux）
- SQL 语法
- 有关网络操作指令（Telnet、Ping、nslookup、Tracert）
- 程序的下载及安装
- 脚本语言（Python、Ruby、Perl）的部署与执行

为什么只在网站中进行渗透测试

渗透测试涵盖的领域非常广，平台、网络、防火墙，甚至实体环境，一个人的能力实难面面俱到，笔者自认为不是渗透测试方面的专家，实在无法写出兼顾各种情景的测试教学文件，诚如书名《网站渗透测试实战入门》所言，笔者只打算聚焦于网站的渗透测试。

另一方面，网站是开放的，以供不特定人使用的，也就是说每个人都可以对你的系统进行攻击，而网站的弱点或漏洞往往来自于应用程序设计不良，或系统设置不完善，平台的漏洞必须等待供货商发布补丁程序（如 Windows 的漏洞要靠微软的 Hot Fix 发布），但网站的漏洞却是需要由我们自己负责，也是我们可以掌控的部分。简单地说，网站就是站在被攻击的第一线，如果有漏洞该由我们自己修补，在一般的渗透测试操作

中，网站测试大多自成一格，而且网站的弱点比较容易衡量，初学者可从中得到成就感，进而持续精进其他部分的测试技巧。

通常情况下，只要懂得开发网页应用程序者，都能进行网页渗透测试，相较其他领域，网页渗透技术门槛低，入门相对简单，对初学者来说容易有成就感，可以激起学习兴趣，学习成果较显著。

目前很多公司（或机构）都有自己的网站，委托外部专业公司进行渗透测试所费不赀，无法恒常办理，如果自己能执行渗透测试，那么一些浅显的漏洞就可以及早发现，让专业公司专注较具深度的信息策略即可。

本书的目的

这是一本入门书，目的在于引起更多人对网站安全的关注，并以实际渗透来验证网站的安全性，或许您的网站应用程序都经过黑、白箱的弱点扫描，但自动化扫描程序是依照特定的规则（Policy）来解读回应的结果，经常有误判或漏判的状况，我们可通过智慧判断响应的结果，再进一步做细微的攻击策略调整，通过实际的测试操作，可以弥补自动化扫描程序的不足，亦可作为弱点扫描的结果验证程序。

渗透测试的技术并无止境，施测者通常会整理自己惯用的工具组，有关书中介绍的工具均是笔者个人的偏好，不表示只有这些工具可以用，如果读者有心走渗透测试这条路，应该整理出属于自己的工具组，笔者会在介绍工具时提供下载网址，为避免版权纠纷，无法将工具整理成光盘随书发行。

安全不能只靠政策、设备，不是装了防火墙，使用账号、密码机制，就能说系统够安全，必须经过实际检验，才能做出安全等级评断，应让更多人了解弱点、挖掘安全漏洞，才能有效地修补漏洞，真正强化系统的安全，不然大家都以为系统有多么牢靠！

警 告

渗透测试的手法如同黑客攻击，没有得到雇主授权之前千万不要擅自进行，以免触犯刑法。