TURING 图灵程序设计丛书

i!i 에이콘

Kali Linux & BackTrack 渗透测试实战

【韩】赵涎元等 著　金光爱 译

BackTrack

人民邮电出版社
POSTS & TELECOM PRESS

TURING 图灵程序设计丛书

Kali Linux & BackTrack 渗透测试实战

【韩】赵涎元等 著　金光爱 译

BackTrack

人民邮电出版社
北京

图书在版编目（CIP）数据

Kali Linux & BackTrack渗透测试实战 / （韩）赵涎元等著 ; 金光爱译. -- 北京 : 人民邮电出版社, 2014.11
（图灵程序设计丛书）
ISBN 978-7-115-37058-7

Ⅰ. ①K… Ⅱ. ①赵… ②金… Ⅲ. ①Linux操作系统 Ⅳ. ①TP316.89

中国版本图书馆CIP数据核字(2014)第212734号

内 容 提 要

本书基于编写团队的实际经验，围绕渗透测试进行了全面介绍，并选择“Kali Linux (包含 BackTrack)” Live CD 作为讲解工具。下载 BackTrack Live CD 和 Kali Linux Live CD 后根据书中讲解逐步实践，可有效提高漏洞诊断效率，迎合市场对于计算机安全技术的要求。本书多次介绍 BackTrack 在实际业务中对渗透测试的影响，通过 BackTrack 工具实操让读者了解各流程中应用到的主要工具。书中不仅讲解了攻击者立场上的技术和方法，而且对实际管理业务中可以有效应用的部分以及攻击应对策略也做了说明。

无论是刚刚接触渗透测试、想要把握渗透测试业务流程的读者，还是需要全面掌握 BackTrack 工具、希望了解后续版本 Kali Linux 工具的变化和使用方法的读者，都能从中获益。

◆ 著　[韩] 赵涎元　等
译　金光爱
责任编辑　傅志红
执行编辑　陈　曦
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
三河市海波印务有限公司印刷

◆ 开本：800×1000　1/16
印张：33
字数：780千字　2014年11月第1版
印数：1-3 000册　2014年11月河北第1次印刷
著作权合同登记号　图字：01-2013-8802号

定价：99.00元

读者服务热线：(010)51095186转600　印装质量热线：(010)81055316
反盗版热线：(010)81055315
广告经营许可证：京崇工商广字第 0021 号

版权声明

作 者 序

赵涎元

执笔写这本书的时候，我回忆起了第一次出书的往事。因为是突如其来的机会，所以我毫无准备，只能在一片空白的状态下开始。也许是因为没有经验，仅拟定目录这一项工作就花去了好几个月的时间，半年后才开始填充内容。经过无数次的编辑过程后，我深刻地体会到了其他作者们经常在书的开头所说的“削骨之痛”。当时我就下定决心，此生不再写书。不过当书编成册出版时，那份感动至今令我难以忘怀。不管怎样，我写完一本书之后反而信心倍增，给后辈们传授知识时也会经常用到它。但遗憾的是，由于经验不足，第一本书没能全部记录我的所思所想。

准确地说，应该是过了整整一年以后，我才完全忘却当时的痛苦而重拾写书的念头。如果要写新的主题，一切都要重头开始，这样沉重的负担让我考虑了很久究竟应该写什么。渗透测试业务的初学者最感兴趣的、最想知道的内容是什么，我对此进行了反复思考。另外，我还通过网络社区活动，以导师的身份与后辈们聊了很多。

最终，我决定写一本涵盖当时未能向后辈们公开的、有关渗透测试业务全部内容的书，其中介绍可以应用到渗透测试业务的技术。事实上，执行渗透测试业务并不需要那么多工具。讲解业务时，也许“手动检测”反而是理所当然的过程，因为渗透测试能采用自动方式的部分极少。不过，“如果真有那么好的工具呢？如果有能够充分应用到业务中的工具呢？如果存在可以有效管理无数诊断对象的方案呢？”这样的疑问一直萦绕在我的脑海中。恍然间我想起，虽然BackTrack Live CD很早就广为人知，却没有人认真研究过其内部的众多工具。

以前，我们在业务中经常会使用到BackTrack工具。不过在我的记忆中，并没有多少人尝试进一步应用此工具，更别说研究它会为业务带来哪些效用价值。韩国国内尤其如此。因大部分BackTrack由开源（特别由基于Python、Ruby、Perl脚本的工具）构成，其优点在于通过分析、修改就可以变成个性化的工具。另外，BackTrack Live CD并非单纯的工具集合，它还包括渗透测试（Penetration）的步骤和方法。

在这种想法和长期目标的指引下，我发布了“分析BackTrack工具”的主题，开始寻找共同研究的人。而且，我还打算把共同的研究成果中那些整理好的部分编辑成书，与大家分享。虽然我作为负责人在代表所有成员写这段作者序，不过，这本书是所有成员努力的结晶。目前，安全防范项目（www.boanproject.com）一直在整理成员们利用业余时间不断调查研究、更新的内容。

BackTrack后续版本Kali Linux发行后，虽然部分服务已中断，但Live CD内部的大部分工具仍可以独立运行，所以不会有太大问题。更新到Kali Linux后，部分有用的工具已消失，所以我平时会把

BackTrack与其一同使用。而且Ubuntu与Debian环境也存在较大差异，所以有必要考虑其使用环境。

本书不可能包含渗透测试相关的所有内容，其他内容可参见我的《什么是渗透测试？》《Nmap NSE安全漏洞诊断实战》等书。此外，我还在努力涉及其他领域的写作。本书内容基于无数次的授课经验和培训内容开发经验，因此，我相信对从事渗透测试的读者大有裨益。本书出版后，我计划在自己管理的博客（bolg.naver.com/chogar）和网络社区（www.boanproject.com）中上传Kali Linux的其他应用方法和视频教程等最新信息，并努力将之打造为最佳指南、最佳安全资讯。

首先感谢给予我们极大帮助的Acorn出版社金喜贞副总经理和出版社的所有相关人士。另外，还要感谢为本书编写和出版给予支持的所有作者，以及所有安全防范项目的幕后成员。也向写作期间一直在旁默默鼓励和帮助我的妻子金慧真和儿子虎英，以及在妻子肚子里健康成长的夏莹说声："我爱你们。"

朴炳旭

大家应该都听说过BackTrack和Kali Linux，但能有几个人真正见识过其中的工具呢？我虽然从很早就开始逐步使用BackTrack中的工具，不过从来都没有仔细观察过。因此，我将这个目的树立为长期目标，开始研究和分析BackTrack及Kali Linux中包含的工具。

我在研究和分析这些工具的过程中发现，除了经常使用的工具外，对其他工具的认识基本接近空白，所以首先袭来的是茫然和恐惧。不过后来我不止一次地发现，自己在研究工具的时候，事先会想到"这工具有何用途"等问题，然后就沉浸于学到新知识的快乐了。

有些人只把BackTrack和Kali Linux视为用于入侵行为的工具集。这么想其实也没错，不过我想重新定义。BackTrack和Kali Linux中的大部分工具是开源的，随着对工具的深入分析，以及根据当前环境进行修改的程度，其应用价值会大幅提升。希望各位阅读此书时能够想到，BackTrack和Kali Linux工具集不仅用于入侵行为，还可以应用于漏洞诊断业务。我想，各位一定是因为对安全和渗透测试感兴趣才选择了本书。通过研究和分析BackTrack以及Kali Linux，我在这方面的知识更上了一层楼。希望各位也能像我一样，通过本书跃上一个新的台阶。

这本书是几位合著者共同的劳动成果，所有成员确立了"BackTrack & Kali Linux工具分析"为主题的长期目标后，共同研究分析，讨论是否有助于实际业务，并为了获得更好的信息而付出了共同努力。无论研究和分析任务多么有趣，如果没有大家的并肩奋斗，不可能获得如此好的结果，研究、分析的乐趣也会转瞬即逝，甚至可能中途放弃。确立长期目标去研究、分析完全陌生的工具时，有时会感到疲倦和郁闷。每当此时，叫做"放弃"的怪物就会在内心深处慢慢滋生。如果没有成员们的共同合作，我很有可能早就被这只怪物给吞噬掉了。所有成员现在依然不惜投入个人时间进行调查研究，努力更新安全防范项目（www.boanproject.com）的内容。

再次感谢与我共同经历时间磨练的所有成员。

林钟旻

最近经常可以听到"个人信息泄露"或"黑客入侵"等术语，而且几乎每天都能接触到"个人信息泄露事件"或企业安全事故频繁发生等类似新闻。就算不是安全方面的专家，也能听到很

多有关黑客入侵的故事。另外，很多人也出于对黑客入侵的好奇而想要学习相关知识。虽然有很多“黑客入侵工具”方便大家跟着学习，但是介绍各工具的原理和攻击核心内容的书却不多。本书整理了BackTrack OS和2013年03月发布的Kali Linux中添加的功能，介绍了Kali Linux相关概念和各种内置工具的应用及原理。

如果你刚涉足安全相关业务，那我建议你不要仅停留在利用工具的层面上，而要学习工具原理和所有基础知识。如果你是实操人员，那我建议你有必要考虑如何应用于实际业务。实际上，与利用自动化工具进行的检查相比，渗透测试执行的大部分业务更多的是服务障碍或服务器过载引起的“手动检查”。不过，如果能在不造成问题的前提下应用各种工具有效管理诊断对象和公司的资产，就能大大提高工作效率。

本书还完整记录了我们的技巧和经验，全面而详细。我们还会在安全防范项目（www.boanproject.com）社区继续研究和整理新的内容。

希望本书不负您的期待。

李庆喆

老实说，我实在想不起来当时选择学习安全以及黑客领域知识的契机是什么了。当时误打误撞进入这一领域，毫无基础可言。学习各种内容的过程中，我首先了解到的就是BackTrack。可我事先并没有系统学习过BackTrack，而是急着乱用。在此过程中我发现需要更多信息，这样就接触到了“安全防范项目”（www.boanproject.com）的网络社区。现在，安全防范项目已成为我再熟悉不过的地方，熟悉得都让我忘记了自己是何时加入安全防范项目的。通过这个社区，我获得了BackTrack以及各种安全、黑客相关信息，也自然而然地参加了“分析BackTrack工具”的项目。借此机会，我得以从BackTrack的基础知识逐一学起，并有了深入了解。

关注安全防范的人都知道，BackTrack是基于开源的Linux公开发行版，它是很多人喜欢用的工具。尽管人们非常关心BackTrack，但是，如果要集中研究并分析庞大的BackTrack功能，还是相当困难的。

所以我们编写了这本《Kali Linux & BackTrack渗透测试实战》，本书并不仅限于介绍工具，还讲解了渗透测试的步骤和方法。通过集中研究和分析BackTrack中的工具，编写了数量庞大的信息。这些都是成员们亲自研究分析的结果，所以渗透测试业务的初学者或普通读者会感到易于理解。当然，正因为BackTrack是基于开源的Linux公开发行版，所以包含于其中的工具也是开源的，是由多个脚本构成的工具，它们都是全新的。不过刚开始分析时，工具相关信息可能包括在相关文件夹中，也可能不包括。如果不包括，就要通过搜索查找资料，并且需要通过各种测试来编辑内容。当然也有容易分析的工具，可还有很多工具信息不足，甚至会让你质疑为什么非要放进来不可。我通过比较其他会员的内容和自己的内容来修改分析环境，并努力使分析更详细。多亏了会员朋友们的宝贵意见，才让我弥补了不足的部分。

成员们也不是时刻都能顺利地进行项目研究，包括我在内。工具种类多样，还有很多工具是我们从未接触过的，所以我曾对此失去兴趣，也遇到了不少困难。我最清楚自己的分析能力，所以并没有满足于现状，而是时刻准备进行不一样的分析。我相信，即使这变化来得比较慢，也一

定可以得出令人满意的结果。这对于学习设计的我来说是一次崭新的挑战，但我从未想过放弃。

我们排除万难终于出版了这本书，小组成员们也因此学习和经历了不少东西。目前BackTrack服务虽已中断，不过同时讲解了Kali Linux工具，所以有助于各位提早了解Kali Linux和更多技术点。本书不仅有助于应用BackTrack，更有助于应用Kali Linux。

我经常强调自己是机械工程专业出身。无论哪个领域，只要是自己关心的，都会喜欢尝试。虽然并没有专业人士那样的实力，可还是希望自己的热情能够获得大家的好评。我写这篇文字的时候，很多成员可能仍在埋头研究。我想一如继往地支持他们高涨的热情，也很想变成像他们那样的人。另外，向总是为我们着想的赵涎元（nicky）先生表示衷心感谢，我会一直支持您的。

崔祐硕

我第一次接触计算机是在小学时上过的电脑培训班。那时使用5.1英寸的软盘或1.44英寸的软盘启动DOS以运行其他程序，Windows3.1还未普及。从Windows95起，韩国很多国内企业都开始大量生产电脑，之后才逐渐普及到百姓家中。当时我虽然已经听说过病毒和V3，不过在那个年纪，根本没想到与信息安全有关。而且当时网络也不够发达，所以只关注幸运到手的DOS专用游戏。初中一年级时，我考取了信息处理执业资格证，之后就再也没有碰过电脑，一直在复习高考。

考入大学后服兵役，退伍之后我才开始正式学习计算机知识。主要的学习方向为编程，有段时间感觉很有意思，但没有坚持到底。在此过程中，我到首尔参加了信息安全培训班，首次接触到BackTrack 5。还通过短期项目调查和学习了BackTrack的Metasploit相关信息，借此对BackTrack有了更加深入的了解。

我目前从事的工作与恶意代码有关，各位可能会认为与Kali Linux等渗透测试操作系统没什么关系。甚至可能认为，用于分析恶意代码的Windows专用虚拟机和测试平台的构建、基于REMnux等Linux构筑的恶意代码逆向工程操作系统会更适合。

但我认为，现在的IT技术很多，如想探讨某项技术衍生的信息安全问题，需要多种技术上的基本原理。我们需要以这些基本原理为基础，自然地在攻击者或防御者的立场间转换。此时，最容易获得的工具就是Kali Linux。如果能够应用好Kali Linux中的无数个开源工具，就能产生巨大的效果。

下面举几个例子。假设分析恶意代码时需使用arp spoofing技术，为了编写分析报告书以及教导后辈，需要进行arp spoofing实操。此时，如果是普通Linux系统，就需要从repository中查找相关工具，否则需要上网查找。

而Kali Linux提供了这些工具，所以利用起来很方便。再举一个例子。2012年夏天，人们发现了IE浏览器的远程代码执行漏洞，但微软公司只提供了相关Fix it，未能提供紧急安全补丁。发现漏洞后的一周时间内，BackTrack（当时为Kali Linux之前版本BackTrack 5 R3）的相关漏洞代码泄漏到Metasploit，无数攻击者开始在零日攻击（zeroday）期间大量散布恶意代码。技术分析家可以用Kali Linux从BackTrack中轻松获取并分析PoC代码。

由此可见，Kali Linux对于研究安全的人而言是非常不错的素材。另外，如果研究Kali Linux包括的多种开源工具，通过运营Kali Linux以视觉效果表现发生的结果或日志，将新工具应用于业务，就能建立自己的个性化操作系统。希望各位不要局限于渗透测试，而是以本书为起点，拓

宽视野，更广泛地利用此工具。

感谢让我参与写作的赵涎元前辈，还要感谢全力支持各种技术活动的南锡宇组长以及（株）tricubelab的同事们，感谢安全防范项目成员与我分享未能在公司经历的各种安全领域的故事和技术。最后向在远方一直支持我的家人们说声："我爱你们。"

致　谢

我们5人为编写本书付出了大量努力，向我们提供各种帮助的人——安全防范项目经理及各小组骨干成员——也对本书出版功不可没，他们也可算得上是合著者。如果没有他们的帮助，整个编写及出版过程能否顺利完成都将成为疑问。在此，我们向为本书出版鞠躬尽瘁的所有人致以深深的谢意。

李俊珩

CodeGate2013考试命题委员（数字取证），著有《数字取证的世界》，多次参加Bug Hunting并受邀演讲。

向为本书出版而奔波的所有项目组成员表示衷心感谢。

徐俊锡

任职于韩国信息安全教育中心（2012~至今）。

虽然没能为本书出版提供很大帮助，可我的绵薄之力能够有所助力的话，我就已非常满足了。真心希望各位能够通过本书获得宝贵经验和知识。

金男玄

曾任职于Inca网络公司（2009~2010），现就职于Igloo Security（2011~至今）。

安全防范项目研究的不仅是系统安全，更是梦想，它点燃了我心中的激情。各种系统安全技术并不只是技巧，而是我寻找梦想的关键词，对此我表示十分感谢。

金敬卓

曾负责国家机关安全咨询（2002.01.01~2010.12.27），现兼任认证审计（ISMS/PIMS/GISMS/开发安全诊断员）（2010.12.28~至今）。

安全防范项目每天都在发生有趣的新鲜事！

安全防范项目总能超乎你的想象，让你享受挑战！

很长时间没遇到这样充满生机的网络社区了，它每天都能激发我的学习热情。我非常高兴能与各位成员热烈探讨并研究系统安全。真心感谢社区为我提供了这样的机会。

全永宰

曾就职于陆军信息体系管理团（2001.03~2012.02），历任（株）CAS安全事业部组长（2011.11~2012.06）、（株）NETKTI SD事业组部长（2012.06~至今）、韩国防黑安全协会技术专员（2011.12~至今）、OWASP Korea Chapter组长（2012.06~至今）、新一代安全专家论坛负责人（2013.01~至今）。

我运营安全防范项目已有两年，起初还对它的前途充满担忧，而如今已硕果累累。各位成员，大家辛苦了！希望安全防范项目能够借此机会迈上新的一个台阶。谢谢！

金松斌

任职于Trinitysoft（2011.02.23~至今）。

能够通过“安全防范项目”社区获取更多信息和知识，这于我真是莫大荣幸。管理员nicky先生为首的各位组长、PM以及全体项目成员激发了我的学习热情和动力，非常感谢大家！以后还请多多关照！

金元基

任职于INCOMS（2009年7月~至今）。

能够遇到安全防范项目是我的福气，非常感谢一向恩威并施的赵涎元先生。

吴权泽

曾任职于韩国信息安全教育中心（2009~2011）、A3 Security（2011~2012），现兼任信息安全专员（2012~至今）。

BackTrack提供的工具非常多，与其掌握所有工具的使用方法，不如在具有相同功能的工具中选择一个灵活运用。重点并不在于掌握了多少工具，而在于是否正确掌握原理，能否在需要的时候随时应用。本书适合学习，更适合研究。最后，请允许我再次向安全防范项目表示感谢。

前　言

2014年频繁发生重大黑客事件，金融圈发生多起信用卡个人信息泄露事故，通信公司的用户个人信息也被大量攻击。之前就连媒体也不会公开的黑客事件逐渐被世人熟知，并使人们愈发关注安全市场。期盼已久的《个人信息保护法》终于在韩国国内开始施行，为从根本上消除常用网络服务的脆弱性，“开发阶段安全编码”成为韩国公民法定义务。由此足以看出人们对应对黑客事件的关注。

如果要制造不错的盾牌，首先就要研究对方的长矛。同理，为了进行防御，首先要学习有关攻击的知识。多听取他人经验是很有必要的，对于进行管理的人群来说，可以借此了解黑客们通过哪些技术和流程进行访问；而对于诊断者来说，可以借此形成自己的方法。

本书基于编写团队的实际经验，围绕渗透测试进行了全面的介绍，并选择“Kali Linux（包含BackTrack）”Live CD作为讲解工具。选择该工具的理由非常明显。利用开源工具或免费版本进行渗透测试时，可以使用的工具很多，因为我在使用Kali Linux之前，也把所有工具都放在文件夹中管理并使用。不过，Kali Linux确实有很多有助于业务的工具。而且这些工具根据渗透测试步骤区分了项目，所以诊断时还可以了解其访问方法。由于大部分开源工具都以Python、Ruby编程为中心，因此，即使不符合环境，只要稍作修改就很好用。

Kali Linux中的工具总是发布新版本，为入门者实操提供了最佳工具。没必要到处去寻找各种工具而浪费时间，下载BackTrack Live CD和Kali Linux Live CD后根据书中讲解逐步实践，就可以完全掌握。

本书读者群

本书主要的读者对象为希望了解渗透测试业务的初学者和实操人员。向以下读者推荐本书：

- 希望了解渗透测试业务流程的读者
- 开始渗透测试业务之前需要指导的读者
- 希望全面了解BackTrack工具的读者
- 希望了解后续版本Kali Linux工具的变化和使用方法的读者
- 希望了解BackTrack实操方法的读者

本书特点

(1) 入门者增加基础内容。

(2) 为希望并行使用Kali Linux和BackTrack的读者增加指南。

(3) 为使用Kali Linux深化渗透测试诊断提供指南。

本书的出发点是，为实施渗透测试业务而应用BackTrack诊断工具。BackTrack包含着漏洞诊断流程，因此本书会多次介绍BackTrack在实际业务中对渗透测试的影响。我们致力于在书中涵盖自己在咨询业务中感受到的方方面面、对入门者的期望、成为项目经理（选拔、担任）时需要了解的知识等各项内容。

本书通过BackTrack工具实操让读者了解各流程中应用到的主要工具，并且更加细致地介绍了可能会继续成为热门话题的内容。不仅讲解了攻击者立场上的技术和方法，而且对实际管理业务中可以有效应用的部分以及应对攻击的方法也做了说明。

本书结构

本书便于BackTrack用户以及后续版Kali Linux用户进行实操练习。根据个人经验，即使发行了后续版Kali Linux,只要能很好利用BackTrack提供的驱动器兼容性及工具，也是个不错的选择。我们进行诊断时也会混用两个Live CD。

- **第1章，认识渗透测试的业务流程**介绍应用BackTrack Live CD之前进行渗透测试的流程和概要。能够灵活运用漏洞诊断工具是件好事，不过更重要的是，了解渗透测试的步骤后将工具运用得恰到好处，从而提高业务效率。如不遵守业务流程而进行漏洞诊断，很可能会引发问题，因此理解概念是非常重要的。本书基于经验而成，结构简单有趣，无论初学者还是初级项目经理都能有所收获。
- **第2章，认识BackTrack**介绍BackTrack Live CD。这一章针对入门者介绍BackTrack概念和安装过程，以及在智能手机上安装BackTrack的方法，以增加趣味性。虽然通过虚拟图像的方式提供BackTrack，不过，通过这些安装过程可以了解Ubuntu Linux的特性，也可以观察到BackTrack的变化。
- **第3~9章**介绍BackTrack Live工具。从第3章开始介绍实际工具的使用方法、选项、应用阶段等。根据工具的使用方法，还对应用价值高的工具添加了源代码分析和应用方法的介绍。近来成为热门话题的部分是从安全层面讲解的。
- **第10章，编写报告阶段**介绍结束渗透测试方式的诊断后如何编写结果报告。涉及了在报告编写阶段也可以应用到的BackTrack工具，而且还讲解了应包含在报告中的服务诊断和影响度评价等内容。因所有诊断结果全凭报告进行判断，所以收尾是最重要的部分。
- **附录，渗透测试和系统安全专家须知**部分整理了作者们在对外活动中实施导师计划时获得的经验，并解答了初学者们提出的诸多疑问。这些应该有助于学习每日安全动向收集方法，且有助于考虑渗透测试业务的发展方向；还简单介绍了学习渗透测试时令人好奇

的实操范围，并收录了获取信息的方法，增加了可浏览所有BackTrack后续版本Kali Linux工具的网站目录。最后讲解了BackTrack中的工具版本更新后，安装和设置过程中的问题的解决方法。

注意事项

本书面向刚刚接触渗透测试诊断业务的读者。为了方便读者在本地电脑上进行测试，书中尽可能地介绍了如何构建系统环境，但严禁利用此工具入侵未获得授权的服务。在此郑重声明，因试图进行入侵而发生的全部法律责任由用户承担。

目　录