信息安全
技术大讲堂

从实践中学习
Kali Linux
渗透测试

大学霸IT达人◎编著

从理论、应用和实践三个维度讲解Kali Linux渗透测试的相关知识

通过145个操作实例手把手带领读者从实践中学习Kali Linux渗透测试技术

涵盖环境搭建、信息收集、漏洞扫描与利用、嗅探欺骗、密码攻击、无线渗透……

机械工业出版社
China Machine Press

信息安全
技术大讲堂

从实践中学习
Kali Linux
渗透测试

大学霸IT达人◎编著

机械工业出版社
China Machine Press

图书在版编目（CIP）数据

从实践中学习Kali Linux渗透测试 / 大学霸IT达人编著. —北京：机械工业出版社，2019.8

（信息安全技术大讲堂）

ISBN 978-7-111-63258-0

Ⅰ. 从… Ⅱ. 大… Ⅲ. Linux操作系统－安全技术 Ⅳ. TP316.85

中国版本图书馆CIP数据核字(2019)第151571号

从实践中学习 Kali Linux 渗透测试

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：欧振旭 李华君 责任校对：姚志娟

印 刷：中国电影出版社印刷厂 版 次：2019 年 8 月第 1 版第 1 次印刷

开 本：186mm × 240mm 1/16 印 张：24.25

书 号：ISBN 978-7-111-63258-0 定 价：119.00 元

客服电话：（010）88361066 88379833 68326294 投稿热线：（010）88379604

华章网站：www.hzbook.com 读者信箱：hzit@hzbook.com

前言

渗透测试是一种通过模拟黑客攻击的方式来检查和评估网络安全的方法。由于它贴近实际，所以被安全机构广泛采用。渗透测试过程中需要使用大量的软件工具。为了方便使用，很多安全专家将这些工具集成到一个操作系统中，从而形成了多个专业的测试系统。在国际上，最知名的渗透测试系统就是 Kali Linux。

本书基于 Kali Linux，详细讲解渗透测试的各项理论和技术。书中首先介绍了渗透测试的准备知识，如渗透测试的概念、Kali Linux 系统的安装和配置、靶机环境的准备；然后详细地讲解了渗透测试的各个流程，包括信息收集、漏洞扫描、漏洞利用；最后着重讲解了常用的渗透技术，如嗅探欺骗、密码攻击和无线网络渗透等。

本书有何特色

1. 内容实用，可操作性强

在实际应用中，渗透测试是一项操作性极强的技术。本书秉承这个特点，合理安排内容，从第 2 章开始就详细讲解了扫描环境的搭建和靶机建立。在后续的内容讲解中，对每个扫描技术都配以操作实例，带领读者动手练习。

2. 充分讲透渗透测试的相关流程

渗透测试的基本流程包括三大环节，分别为信息收集、漏洞扫描和漏洞利用。其中，每个环节又包括多个流程。例如，信息收集包括主机发现、域名发现、端口扫描、识别系统与服务、信息分析。本书详细讲解了每个环节，帮助读者建立正确的操作顺序，从而避免盲目操作。

3. 由浅入深，容易上手

本书充分考虑初学者的学习规律，首先从概念讲起，帮助读者明确渗透测试的目的和操作思路，然后详细讲解实验环境的准备，例如需要用到的软件环境、靶机和网络环境等。这些内容可以帮助读者更快上手，从而理解渗透测试的本质。

4．环环相扣，逐步深入

渗透测试是一个理论、应用和实践三者紧密结合的技术。任何一个有效的渗透策略都由对应的理论衍生应用，并结合实际情况而产生。本书力求对每个重点内容都按照这个思路进行讲解，帮助读者能够在学习中举一反三。

5．提供完善的技术支持和售后服务

本书提供 QQ 交流群（343867787）供读者交流和讨论学习中遇到的各种问题。另外，本书还提供了服务邮箱 hzbook2017@163.com。读者在阅读本书的过程中若有疑问，可以通过 QQ 群或邮箱获得帮助。

本书内容

第 1 章渗透测试概述，主要介绍了渗透测试和 Kali 系统的基础知识，如渗透测试的类型、渗透测试流程、使用 Kali Linux 的原因、Kali Linux 的发展史，以及法律边界问题等。

第 2～4 章为测试环境的准备，主要介绍了 Kali Linux 系统的使用和靶机环境的搭建。这 3 章涵盖的主要内容有 Kali Linux 镜像获取、虚拟机安装、实体机安装、网络配置、软件源配置、软件安装、驱动安装和靶机构建等。

第 5～7 章为渗透测试的流程，主要介绍了渗透测试的三大核心环节：信息收集、漏洞扫描和漏洞利用。这 3 章涵盖的主要内容有发现主机、扫描端口、识别操作系统与服务、收集服务信息、分析信息、漏洞扫描和漏洞利用等。

第 8～10 章主要介绍了渗透测试中常见的几项技术，如嗅探欺骗、密码攻击和无线网络渗透等。这些技术可以帮助安全人员更好地完成渗透测试任务。

本书配套资源获取方式

本书涉及的工具和软件需要读者自行下载。下载途径有以下几种：

- 根据图书中对应章节给出的网址自行下载；
- 加入技术讨论 QQ 群（343867787）获取；
- 登录华章公司网站 www.hzbook.com，在该网站上搜索到本书，然后单击“资料下载”按钮，即可在页面上找到“配书资源”下载链接。

本书内容更新文档获取方式

为了让本书内容紧跟技术的发展和软件更新，我们会对书中的相关内容进行不定期更新，并发布对应的电子文档。需要的读者可以加入 QQ 交流群（343867787）获取，也可

以通过华章公司网站上的本书配套资源链接进行下载。

本书读者对象

- 学习渗透测试的入门人员；
- 渗透测试技术人员；
- 网络安全和维护人员；
- 信息安全技术爱好者；
- 计算机安全技术自学者；
- 高校相关专业的学生；
- 专业培训机构的学员。

本书阅读建议

- 由于网络稳定性的原因，下载镜像后，建议读者一定要校验镜像，避免因为文件损坏而导致系统安装失败。
- 学习阶段建议多使用靶机进行练习，避免因为错误操作而影响实际的网络环境。
- 由于安全工具经常会更新，以增补不同的功能，因此在学习的时候，建议定期更新工具，以获取更稳定和更强大的环境。

本书作者

本书由大学霸 IT 达人技术团队编写。感谢在本书编写和出版过程中给予了作者大量帮助的各位编辑！由于作者水平所限，加之写作时间较为仓促，书中可能还存在一些疏漏和不足之处，敬请各位读者批评指正。

编著者

目录

第 1 章　渗透测试概述

渗透测试是对用户信息安全措施积极评估的过程。它通过系统化的操作和分析，积极发现系统和网络中存在的各种缺陷和弱点，如设计缺陷和技术缺陷。在渗透测试之前，本章将介绍渗透测试的一些相关概念。

1.1　什么是渗透测试

渗透测试是通过模拟恶意黑客的攻击方法，来评估计算机网络系统安全的一种安全测试与评估方法。通过实施渗透测试，可以发现一个主机中潜在却未被披露的安全性问题。然后，用户可以根据测试结果对系统中的不足和安全弱点进行加固及改善，从而使用户的系统变得更加安全，减少其风险。当用户实施渗透测试时，可以使用黑盒测试、白盒测试和灰盒测试 3 种方式。本节将分别介绍这 3 种测试方法。

1.1.1　黑盒测试

黑盒测试（Black-box Testing）也称为外部测试（External Testing）。采用这种方式时，渗透测试者将从一个远程网络位置来评估目标网络基础设施，并没有任何目标网络内部拓扑等相关信息。他们完全模拟真实网络环境中的外部攻击者，采用流行的攻击技术与工具，有组织、有步骤地对目标组织进行逐步渗透和入侵，揭示目标网络中一些已知或未知的安全漏洞，并评估这些漏洞能否被利用，以获取控制权或者操作业务造成资产损失等。

黑盒测试的缺点是测试较为费时和费力，同时需要渗透测试者具备较高的技术能力。优点在于，这种类型的测试更有利于挖掘出系统潜在的漏洞，以及脆弱环节和薄弱点等。

1.1.2　白盒测试

白盒测试（White-box Testing）也称为内部测试（Internal Testing）。进行白盒测试的渗透测试者可以了解到关于目标环境的所有内部和底层信息。这可以让渗透测试人员以最小的代价发现和验证系统中最严重的漏洞。白盒测试的实施流程与黑盒测试类似，不同之处在于无须进行目标定位和情报收集。渗透测试人员可以通过正常渠道从被测试机构取得

各种资料，如网络拓扑、员工资料甚至网站程序的代码片段等，也可以和单位其他员工进行面对面沟通。

白盒测试的缺点是无法有效地测试客户组织的应急响应程序，也无法判断出他们的安全防护计划对特定攻击的检测效率。这种测试的优点是发现和解决安全漏洞所花费的时间和代价要比黑盒测试少很多。

1.1.3 灰盒测试

灰盒测试（Grey-box Testing）是白盒测试和黑盒测试基本类型的组合，它可以提供对目标系统更加深入和全面的安全审查。组合之后的好处就是能够同时发挥这两种渗透测试方法的优势。在采用灰盒测试方法的外部渗透攻击场景中，渗透测试者也类似地需要从外部逐步渗透进目标网络，但他所拥有的目标网络底层拓扑与架构将有助于更好地选择攻击途径与方法，从而达到更好的渗透测试效果。

1.2 渗透测试流程

当用户对渗透测试的概念了解清楚后，就可以开始对一个目标实施渗透了。在实施渗透之前，将先介绍一下其工作流程，如图 1.1 所示。

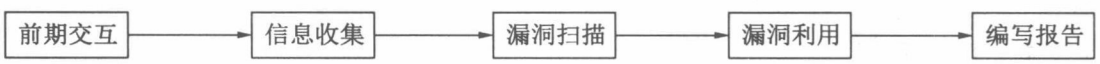

图 1.1 渗透测试流程

这里共包括 5 个阶段，分别是前期交互、信息收集、漏洞扫描、漏洞利用和编写报告。为了方便用户对每个阶段获取的信息更清楚，这里将介绍每个阶段的作用。

1. 前期交互

在进行渗透测试之前，渗透测试者需要与渗透测试目标、渗透测试范围、渗透测试方式、服务合同等细节进行商议，以达成一致协议。该阶段是之后进行渗透测试的基础和关键。

2. 信息收集

在确定了渗透测试目标及范围以后，接下来就进入信息收集阶段。在这个阶段，渗透测试者需要使用各种公开的资源尽可能地获取与测试目标相关的信息。此时，渗透测试者可以借助互联网进行信息收集，如官方网站、论坛、博客等。同时，也可以借助各大搜索引擎来获取相关信息，如 Baidu 和 Google 等。还可以借助 Kali Linux 中的一些工具来对

DNS 信息、注册人信息、服务信息、WAF 信息等进行收集。这个阶段收集的信息越充分，对之后的渗透测试越有利，渗透测试的成功率也会大大提高。

3．漏洞扫描

当渗透测试者收集到足够多的信息之后，就可以对目标实施漏洞扫描了。在该阶段，渗透测试者通过网络对目标系统进行探测，向目标系统发送数据，并将反馈数据与自带的漏洞特征库进行匹配，进而列举出目标系统上存在的安全漏洞。

4．漏洞利用

当渗透测试者探测到目标主机存在漏洞之后，就可以通过已有的漏洞利用程序对目标系统进行渗透。但是，在一般情况下，渗透测试者都需要考虑到目标系统的环境对漏洞利用程序进行修改和额外的研究，否则它无法正常工作。同时，在该阶段也要考虑到对目标系统的安全机制的逃逸，从而避免让目标系统发现。

5．编写报告

在完成渗透测试之后，需要对这次渗透测试编写测试报告。在编写的报告中需要包括获取到的各种有价值的信息，以及探测和挖掘出来的安全漏洞、成功攻击过程及对业务造成的影响和后果分析等。同时，还要明确地写出目标系统中存在的漏洞及漏洞的修补方法。这样，目标用户就可以根据渗透测试者提供的报告修补这些漏洞和风险，以防止被黑客攻击。

1.3　Kali Linux 系统概述

Kali Linux 是一个基于 Debian 的 Linux 发行版，包括很多安全和取证方面的相关工具。它由 Offensive Security Ltd 维护和资助。最先由 Offensive Security 的 MatiAharoni 和 Devon Kearns 通过重写 Back Track 来完成。而 Back Track 是基于 Ubuntu 的 Linux 发行版。本节将介绍书中使用 Kali Linux 的原因及该系统的发展史。

如果要使用 Kali Linux 系统实施渗透测试，则必须先安装该系统。对于很多初学者来说，安装系统也是一件非常头疼的事。

1.3.1　为什么使用 Kali Linux

Kali Linux 的发布主要是用于数字取证和渗透测试。在本书中使用 Kali Linux 系统来实施渗透测试，主要有以下两个原因。

1. 工具仓库

Kali Linux 系统中提供了一个强大的工具仓库，而且预装了许多渗透测试软件，包括 Nmap（端口扫描器）、Wireshark（数据包分析器）、John the Ripper（密码破解器）及 Aircrack-ng（无线局域网渗透测试软件）等。如果用户使用其他操作系统，则需要自己手动安装相关工具，而渗透测试往往需要用到大量的工具，收集这些工具并不是一件容易的事，也无法保证代码的安全。另外，如果用户手动安装，还可能需要配置复杂的环境。用户想要更容易及快速地实施渗透测试，Kali Linux 系统是最佳选择。

为了方便用户实施渗透测试，这里将列举出常用的工具，如表 1.1 所示。

表 1.1 常用的渗透测试工具

信息收集工具集	嗅探欺骗工具集	密码攻击工具集	漏洞分析工具集	漏洞利用工具集	无线渗透工具集
DNSRecon	EtterCap	Crunch	SQLmap	Msfconsole	Aircrack-ng
Dnsenum	driftnet	CeWL	sqlsus	BeEF	Fern WiFi Cracker
DotDotPwn	dsniff	Hash-Identifier	Sqlninja	SQLmap	Wifite
parsero	ferret-sidjack	findmyhash	BBQSQL	RouterSploit	Reaver
Maltego	0trace	RainbowCrack	jSQL	Yersinia	Bully
Amap	HexInject	John	Oscanner	Social-Engineer Toolkit	PixieWPS
Fping	prettypacket	Ncrack	SidGuesser	exploitdb	Kismet
Sparta	hex2raw	THC-Hydra	Doona	sandi	Cowpatty
Hping3	tcpreplay	Patator	Lynis	shellnoob	MDK3
Ghost Phisher	Wafw00f	Medusa	Powerfuzzer	Backdoor Factory	Wifi Honey
Nmap	DNSChef	acccheck	Yersinia	sandi	Pyrit

2. 不断更新

Kali Linux 系统更新速度比较快，稳定版本大约 3 个月会更新一次；而且每周还会发布周更新版本。所以用户可以随时进行更新，尽早使用新的系统和最新的工具。而且，该操作系统更新非常方便，无须用户手动更新。

1.3.2 Kali Linux 发展史

为了使读者对 Kali Linux 系统有更多的了解，这里将介绍一下它的发展史。

1. 前身BackTrack Linux

BackTrack Linux 是一套专业的计算机安全监测 Linux 操作系统，简称 BT。BackTrack

不仅用来作为侦查平台（WarDriving），它还集成了包括 Metasploit 等 200 多种安全渗透工具；此外，众多的 RFID 工具和对 ARM 平台的支持也是一个亮点。目前，BackTrack 已被 Kali Linux 所代替，不再维护。

2．历史版本

Kali Linux 从发布至今共有 4 个版本代号，分别是 moto、kali、sana 和 kali-rolling。其中，每个版本代号表示 Kali Linux 的不同版本。用户通过修改软件源中的该版本代号，即可更新到对应版本的系统。例如，moto 版本代号对应的 Kali 系统版本是 1.0.X；kali 版本代号对应的 Kali 系统版本是 1.1.X；sana 版本代号对应的 Kali 系统版本是 2.0；kali-rolling 版本代号对应的 Kali 系统版本是 2016 年 1 月之后的版本。为了使用户对 Kali Linux 系统的发展史更清楚，表 1.2 列举出了它的所有版本及对应的发布时间。

表 1.2　Kali Linux所有版本及发布时间

版　本　号	发 布 时 间
1.0.0	2013年3月13日
1.0.1	2013年3月14日
1.0.2	2013年3月27日
1.0.3	2013年4月26日
1.0.4	2013年7月25日
1.0.5	2013年9月5日
1.0.6	2014年1月9日
1.0.7	2014年5月27日
1.0.8	2014年7月22日
1.0.9	2014年8月25日
1.0.9a	2014年10月6日
1.1.0	2015年2月7日
1.1.0a	2015年3月13日
2.0	2015年8月11日
2016.1	2016年1月20日
2016.2	2016年8月30日
2017.1	2017年4月23日
2017.2	2017年9月17日
2017.3	2017年11月9日
2018.1	2018年1月26日
2018.2	2018年4月30日
2018.3	2018年8月27日
2018.3a	2018年9月14日