信息安全
技术大讲堂

从实践中学习
Kali Linux
无线网络渗透测试

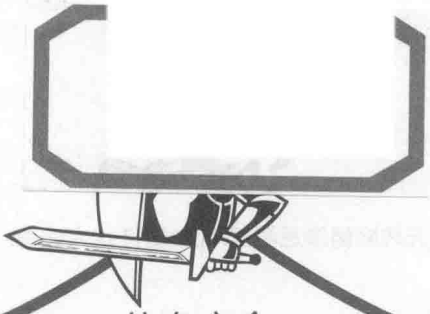
大学霸IT达人◎编著

从理论、应用和实践三个维度讲解Kali Linux无线网络渗透测试的相关知识

通过108个操作实例手把手带领读者从实践中学习Kali Linux无线网络渗透测试技术

涵盖环境搭建、网络监听、网络扫描、数据分析、加密破解、网络攻击……

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
无线网络渗透测试

大学霸IT达人◎编著

RFID

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无线网络渗透测试/大学霸IT达人编著. —北京：机械工业出版社，2019.9

（信息安全技术大讲堂）

ISBN 978-7-111-63674-8

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204733号

从实践中学习 Kali Linux 无线网络渗透测试

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 10 月第 1 版第 1 次印刷

开 本：186mm × 240mm 1/16 印 张：17.25

书 号：ISBN 978-7-111-63674-8 定 价：89.00 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

内容简介

无线网络是现在最常用的网络连接方式。由于其架设容易、实施成本低、连接方便，成为了家庭及中小企业联网的首选模式。由于无线网络数据公开传播，其安全性较差，也成为了黑客关注的重点。渗透测试是通过模拟黑客攻击的方式来检查和评估网络安全的一种方法。通过渗透测试，可以验证无线网络的安全性，发现潜在的风险，如信息泄漏等问题。

本书共11章，内容包括渗透测试基础知识、搭建渗透测试环境、无线网络监听模式、扫描无线网络、捕获数据包、获取信息、WPS加密模式、WEP加密模式、WPA/WPA2加密模式、攻击无线AP和攻击客户端。

本书适合渗透测试人员、网络维护人员和信息安全爱好者阅读。通过本书，可以帮助读者了解和掌握Kali Linux无线渗透测试的相关知识，熟悉无线渗透测试的各个技术要点，并掌握规范的操作流程，从而提高工作效率。

本书特色

- 基于Kali Linux滚动更新（Kali Rolling）版本写作
- 涵盖无线渗透测的四大应用领域：网络监听、数据分析、加密破解和网络攻击
- 明确给出无线渗透测试的目的和操作思路
- 涉及数十种主流渗透测试工具和命令的使用
- 详解软硬件环境的准备，以及无线网卡的使用方式
- 详解无线渗透测试每个流程的操作步骤和实施要点
- 每个技术要点都结合实例讲解，带领读者动手练习
- 提供后续的内容更新服务和完善的工具获取方式
- 提供QQ群和E-mail互动交流方式，答疑解惑

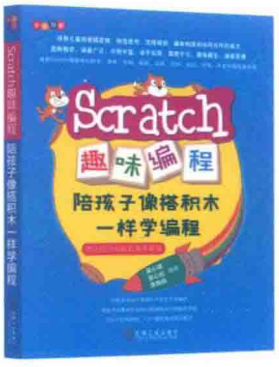
配套资源获取方式

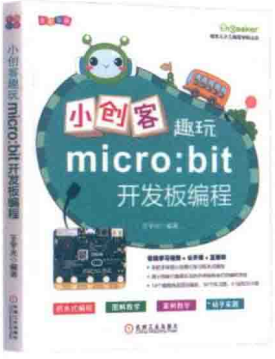
本书配套资源需要读者自行下载，请参考前言中的详细说明进行获取。

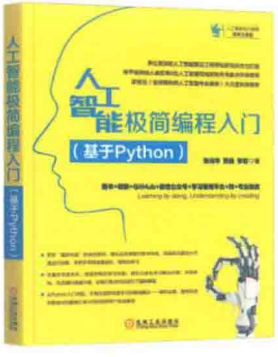
作者简介

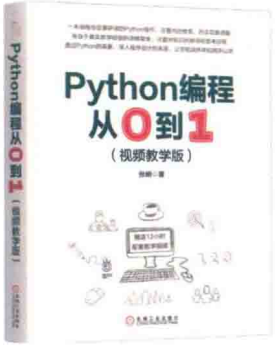
大学霸IT达人 信息安全技术研究团队。熟悉Kali Linux、Metasploit、Xamarin等相关技术。长期从事技术研究和推广工作。专注于网络安全、渗透测试、移动开发和游戏开发等领域。曾经参与编写了多本相关技术图书。

推荐阅读









欢迎IT领域的各位技术专家洽谈出版事宜。如果有写书或投稿意向，请加QQ或者微信具体商谈。

QQ：627173439　　微信：oyzx_xp

前言

无线网络是目前搭建网络最为简单的方式。用户只需要安装一个无线路由器，就可以让周边几十米范围内的无线设备进行连接，如手机、笔记本、平板电脑。由于其成本低廉、架设方便，因此广泛应用于中小网络环境，如家庭、小规模办公场所、公共空间等。

无线网络通过无线电信号传播数据，周边的设备都可以接收和发送数据。所以无线网络的安全性较差，也成为了网络安全防护的重点。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。

本书基于 Kali Linux 详细讲解无线渗透测试的各项理论和技术。书中首先介绍了无线渗透测试的准备知识，如渗透测试的概念、Wi-Fi 网络构成、Wi-Fi 网络协议标准、Kali Linux 系统的安装和配置、无线网卡设备的准备，然后详细地讲解了无线渗透测试的应用场景，包括网络监听、数据分析、加密破解和无线网络攻击等。

本书有何特色

1. 内容可操作性强

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搭建、靶机建立等相关内容。在后续章节中，每个技术要点都配以操作实例，带领读者动手练习。

2. 充分讲解无线渗透测试的四大应用

无线渗透测试包括四大领域的应用，分别为网络监听、数据分析、加密破解和网络攻击。其中，每个应用又划分为不同的技术分支。例如，根据 AP 所使用的加密策略，加密破解分为 WPS、WEP、WPA/WPA2 三个分支。本书详细讲解了每个分支，帮助读者理解每个分支所依赖的背景知识、应用场景和实施手段。

3. 由浅入深，容易上手

本书充分考虑了初学者的实际情况，从概念讲起，帮助读者明确无线渗透测试的目的和操作思路。同时，本书详细讲解了如何准备实验环境，如需要用到的软件环境、硬件环

境和无线网卡使用方式等。这些内容可以让读者更快上手，理解无线渗透测试的实施方式。

4．环环相扣，逐步讲解

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。本书力求对每个重要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

本书提供了对应的 QQ 群（343867787）供大家交流和讨论学习中遇到的各种问题。同时，本书还提供了专门的售后服务邮箱 hzbook2017@163.com。读者在阅读本书的过程中若有疑问，可以通过该邮箱获得帮助。

本书内容

第 1、2 章为无线渗透测试的准备工作，主要介绍了渗透测试基础知识和如何搭建渗透测试环境，如渗透测试的概念、Wi-Fi 网络构成、Wi-Fi 网络协议标准、安装 Kali Linux 操作系统、软件需求、硬件需求和设置无线网卡。

第 3、4 章为无线网络扫描，主要介绍了如何设置网络监听和探测无线网络结构，如网络监听原理、设置网络监听、扫描方式、扫描 AP、扫描客户端和扫描地理位置等。

第 5、6 章为数据分析，主要介绍了如何捕获数据包并进行分析，如 Wi-Fi 数据包格式、捕获数据包、分析数据包、解密数据包、分析客户端行为和提取信息等。

第 7~9 章为 Wi-Fi 加密模式，主要介绍了 Wi-Fi 常用加密方案的实施方式和破解技巧，如设置 WPS/WEP /WPA/WPA2 加密、破解 WPS/WEP/WPA/WPA2 加密、防止锁 PIN、创建密码字典和使用 PIN 获取密码等。

第 10、11 章为 Wi-Fi 攻击，主要介绍了常见的 AP 和客户端攻击方式，如破解 AP 的默认账户、认证洪水攻击、取消认证洪水攻击、假信标洪水攻击、使用伪 AP 和监听数据等。

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；
- 通过 bbs.daxueba.net 论坛获取；

- 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的脚步，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书资源链接下载。

本书读者对象

- 无线渗透测试入门人员；
- 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，下载镜像文件后，建议读者一定要校验镜像文件，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，避免因为错误的操作而影响实际的网络环境。
- 由于安全工具经常会更新、增补不同的功能，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团队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　渗透测试基础知识

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评估方法。这种方法会对系统的任何弱点、技术缺陷或漏洞进行主动分析。分析的时候，渗透测试人员会从攻击者可能存在的任何位置进行实施，并且主动利用安全漏洞。本章将介绍渗透测试的相关基础知识。

1.1　什么是渗透测试

简单地说，渗透测试是指渗透人员在不同的位置（如从内网、外网等位置）利用各种手段对某个特定网络进行测试，以期待发现和挖掘系统中存在的漏洞。然后，制定渗透测试报告，并提及给网络所有者。网络所有者根据渗透人员提供的渗透测试报告，可以清晰知晓系统中存在的安全隐患和问题。本节将介绍渗透测试的流程和特点。

1.1.1　渗透测试的流程

渗透测试的流程共包括 5 个阶段，分别是网络扫描、信息收集、漏洞扫描、漏洞利用和编写报告。在第一个阶段，通过实施网络扫描以确定目标主机的范围，如 IP、域名和内外网等；然后，针对目标进行信息收集，如主机开放的端口、服务、操作系统类型和域名 whois 信息等；接着，利用收集到的信息实施漏洞扫描，以找出可以利用的漏洞；最后，利用扫描出的漏洞对目标实施渗透。当实施完渗透测试之后，渗透测试者可以将渗透过程中获取到的有价值信息，以及探测和挖掘出来的相关安全漏洞、成功攻击过程、对业务造成的影响和后果分析等编写成测试报告。

1.1.2　无线渗透的特点

无线网络渗透相比较有线渗透更容易，不需要必须入侵目标主机才可以获取控制权和目标主机的信息。由于无线网络是公共传播，所以渗透测试者可以直接监听，以发现活动主机或者截获数据。同时，渗透测试人员可以构建大功率伪 AP（Access Point，无线接入

点），诱骗目标用户进行连接。目标主机一旦接入伪 AP，就很容易被控制。

1.2 Wi-Fi 网络构成

Wi-Fi（Wireless Fidelity，无线保真）是一种可以将笔记本电脑、手持设备（如手机、平板）等终端以无线方式互相连接的技术。简单地说，它就是一个高频无线电信号。如果要实施无线渗透，则必须对其网络结构及工作原理有所了解。本节将介绍 Wi-Fi 网络构成。

1.2.1 Wi-Fi 网络结构

Wi-Fi 网络的组成非常简单，只需要一个 AP 和一个客户端即可构成一个 Wi-Fi 网络。但是在 Wi-Fi 网络中，并不是只可以有一个客户端，而是可以连接多个客户端。下面将分别介绍这两个组成部分的作用。

1. AP基站

AP 也称为基站。平常人们都说是 Wi-Fi 热点，更通俗地说就是家里的无线路由器。它的作用相当于一个转发器，将互联网上其他服务器上的数据转发到客户端。

2. STA站点

STA（Station）称为站点，就是所谓的客户端。站点是指具有 Wi-Fi 通信功能并且连接到无线网络中的终端设备，如手机、平板和笔记本电脑等。

1.2.2 工作原理

Wi-Fi 网络的工作原理如图 1.1 所示。

在 Wi-Fi 网络中，数据传输共包括 4 个过程，分别是 AP 广播、AP 探测、身份认证和数据传输。下面将分别介绍这 4 个过程的作用。

1. AP广播

如果在无线路由器中开启 SSID 广播功能的话，AP 将自动广播自己的 SSID 名称。其中，SSID 是 Service Set Identifier 的缩写，意思是服务集标识，简单地说，就是用户在无线客户端搜索到的无线信号。用户可以自己设置 AP 的 SSID。下面将以 TP-LINK 路由器为例，介绍 SSID 名称的设置方法及是否进行广播。

（1）登录路由器的管理页面。本例中路由器的地址为 http://192.168.0.1/。在浏览器中输入该地址，访问成功后，将弹出一个登录对话框，如图 1.2 所示。

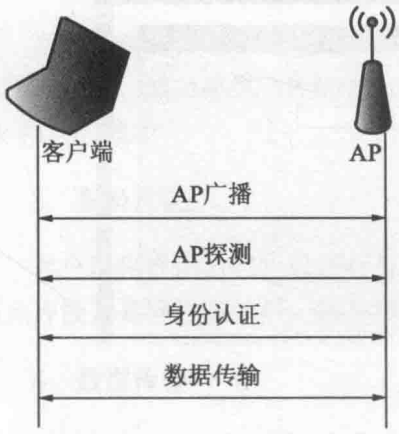


图 1.1　Wi-Fi 工作原理

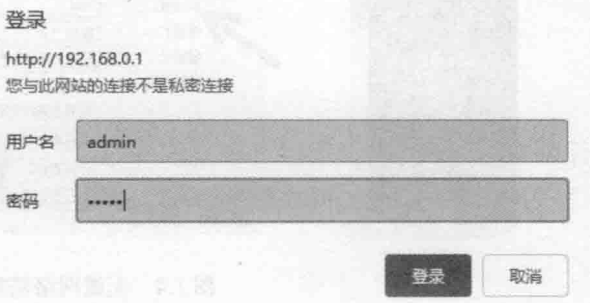


图 1.2　登录对话框

（2）在该对话框中输入登录的用户名和密码，并单击“登录”按钮，将显示路由器的主页面，如图 1.3 所示。

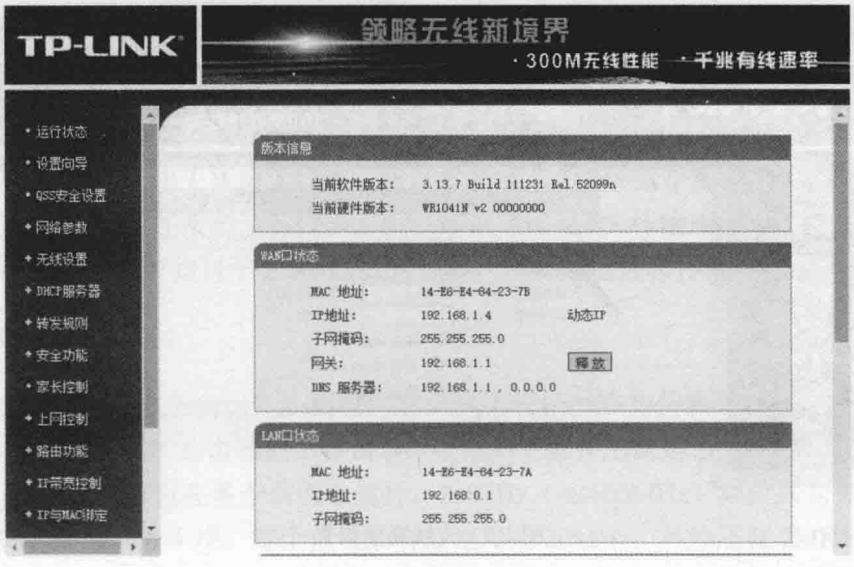


图 1.3　路由器的主页面

（3）在左侧栏中依次选择“无线设置”|“基本设置”选项，将显示无线网络基本设置，如图 1.4 所示。

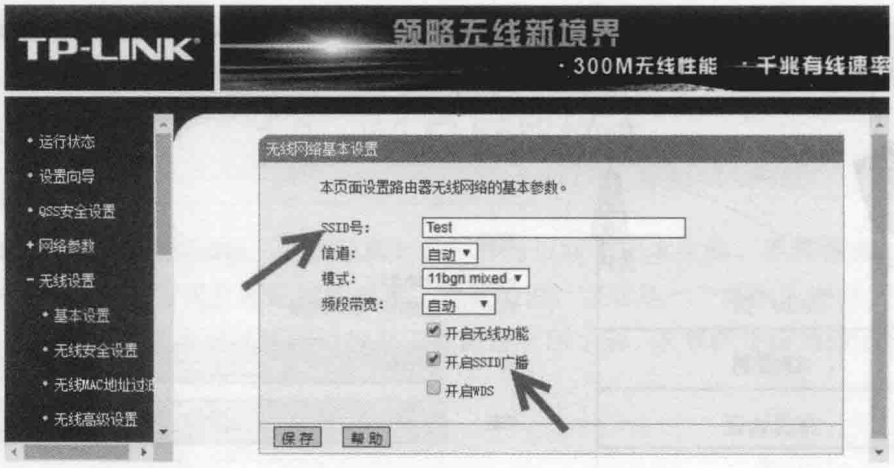


图 1.4　无线网络基本设置

（4）“SSID 号”文本框就是用来设置路由器的 SSID 名称。如果想要广播 SSID，则勾选“开启 SSID 广播”复选框。如果不想要广播 SSID 的话，则取消勾选“开启 SSID 广播”复选框即可。

在该过程中，AP 每隔 100 毫秒将 SSID 经由 beacons 封包广播一次。beacons 就是 AP 广播的信号帧。在路由器的无线高级设置界面即可设置信标间隔，如图 1.5 所示。

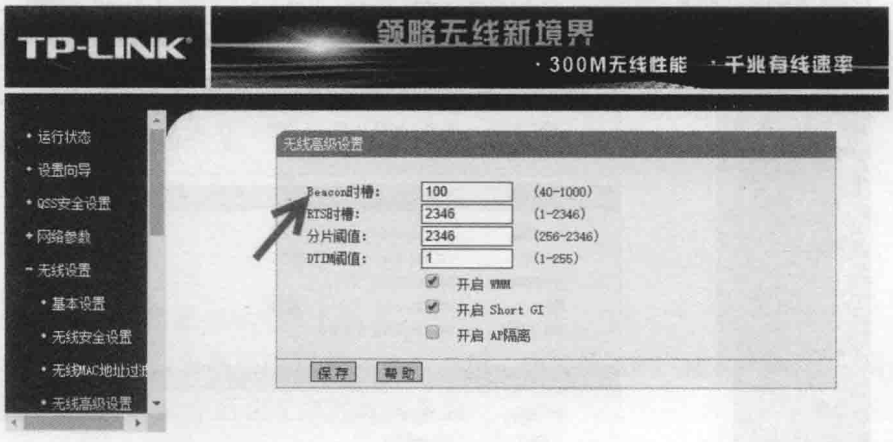


图 1.5　无线高级设置

从图 1.5 中可以看到，“Beacon 时槽”的默认值为 100。此时，用户可以通过修改该值以延长或缩短信标时间间隔。由于 beacons 封包的传输速率是 1Mbit/s，并且长度非常短，所以这个广播动作对网络效能的影响不大。由于 Wi-Fi 规定的最低传输速率是 1Mbit/s，可以满足广播需要，所以所有的 Wi-Fi 客户端都能收到 SSID 广播封包，因此客户端可以