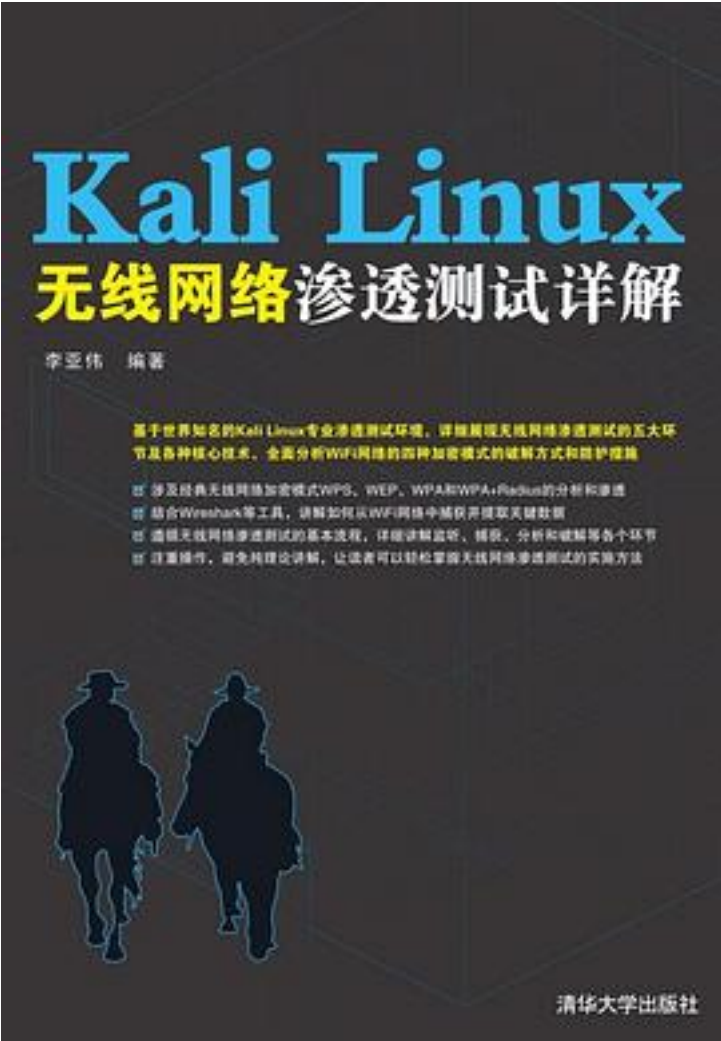


Kali Linux无线网络渗透测试详解



[Kali Linux无线网络渗透测试详解_下载链接1](#)

著者:李亚伟

出版者:清华大学出版社

出版时间:2016-2-1

装帧:平装

isbn:9787302420835

本书是国内第一本无线网络安全渗透测试图书。本书基于Kali Linux操作系统，由浅入深，全面而系统地介绍了无线网络渗透技术。本书针对不同的加密方式的工作原理及存在的漏洞进行了详细介绍，并根据每种加密方式存在的漏洞介绍了实施渗透测试的方法。另外，本书最后还特意介绍了针对每种加密方法漏洞的应对措施。

本书共10章，分为3篇。第1篇为基础篇，涵盖的主要内容有搭建渗透测试环境和WiFi网络的构成。第2篇为无线数据篇，涵盖的主要内容有监听WiFi网络、捕获数据包、分析数据包和获取信息。第3篇为无线网络加密篇，涵盖的主要内容有WPS加密模式、WEP加密模式、WPA加密模式和WPA+RADIUS加密模式。

本书涉及面广，从基本环境搭建到数据包的捕获，再到数据包的分析及信息获取，最后对WiFi网络中的各种加密模式进行了分析和渗透测试。本书不仅适合想全面学习WiFi网络渗透测试技术的人员阅读，同样适合网络维护人员和各类信息安全从业人员阅读。

作者简介:

李亚伟

就职于大学霸网站，任技术研究员。熟悉Apache、Tomcat、Oracle、MySQL、集群、RAC、SAN和容灾等IT业界中流行的系统集成技术。长期从事Linux和网络安全最新技术的研究，以及Linux服务器维护工作。拥有多年的服务器维护经验。曾经参与编写并出版了《Wireshark数据包分析实战详解》一书。

目录: 第1篇 基础篇

第1章 搭建渗透测试环境

1.1 什么是渗透测试

1.2 安装Kali Linux操作系统

1.2.1 在物理机上安装Kali Linux

1.2.2 在VMware Workstation上安装Kali Linux

1.2.3 安装VMware Tools

1.2.4 升级操作系统

1.3 Kali Linux的基本配置

1.3.1 配置软件源

1.3.2 安装中文输入法

1.3.3 虚拟机中使用USB设备

第2章 WiFi网络的构成

2.1 WiFi网络概述

2.1.1 什么是WiFi网络

2.1.2 WiFi网络结构

2.1.3 WiFi工作原理

2.1.4 AP常用术语概述

2.2 802.11协议概述

2.2.1 频段

2.2.2 使用WirelessMon规划频段

2.2.3 带宽

2.3 配置无线AP

2.3.1 在路由器上设置AP

2.3.2 在随身WiFi上设置AP

第2篇 无线数据篇

第3章 监听WiFi网络

3.1 网络监听原理

3.1.1 网卡的工作模式

- 3.1.2 工作原理
- 3.2 配置管理无线网卡
 - 3.2.1 Linux支持的无线网卡
 - 3.2.2 虚拟机使用无线网卡
 - 3.2.3 设置无线网卡
- 3.3 设置监听模式
 - 3.3.1 Aircrack-ng工具介绍
 - 3.3.2 Aircrack-ng支持的网卡
 - 3.3.3 启动监听模式
- 3.4 扫描网络范围
 - 3.4.1 使用airodump-ng扫描
 - 3.4.2 使用Kismet扫描
- 第4章 捕获数据包
 - 4.1 数据包简介
 - 4.1.1 握手包
 - 4.1.2 非加密包
 - 4.1.3 加密包
 - 4.2 使用Wireshark捕获数据包
 - 4.2.1 捕获非加密模式的数据包
 - 4.2.2 捕获WEP加密模式的数据包
 - 4.2.3 捕获WPA-PSK/WPA2-PSK加密模式的数据包
 - 4.3 使用伪AP
 - 4.3.1 AP的工作模式
 - 4.3.2 创建伪AP
 - 4.3.3 强制客户端下线
 - 4.3.4 捕获数据包
- 第5章 分析数据包
 - 5.1 Wireshark简介
 - 5.1.1 捕获过滤器
 - 5.1.2 显示过滤器
 - 5.1.3 数据包导出
 - 5.1.4 在Packet List面板增加无线专用列
 - 5.2 使用Wireshark
 - 5.2.1 802.11数据包结构
 - 5.2.2 分析特定BSSID包
 - 5.2.3 分析特定的包类型
 - 5.2.4 分析特定频率的包
 - 5.3 分析无线AP认证包
 - 5.3.1 分析WEP认证包
 - 5.3.2 分析WPA认证包
- 第6章 获取信息
 - 6.1 AP的信息
 - 6.1.1 AP的SSID名称
 - 6.1.2 AP的Mac地址
 - 6.1.3 AP工作的信道
 - 6.1.4 AP使用的加密方式
 - 6.2 客户端的信息
 - 6.2.1 客户端连接的AP
 - 6.2.2 判断是否有客户端蹭网
 - 6.2.3 查看客户端使用的QQ号
 - 6.2.4 查看手机客户端是否有流量产生
- 第3篇 无线网络加密篇
- 第7章 WPS加密模式
 - 7.1 WPS简介

- 7.1.1 什么是WPS加密
- 7.1.2 WPS工作原理
- 7.1.3 WPS的漏洞
- 7.1.4 WPS的优点和缺点
- 7.2 设置WPS
 - 7.2.1 开启WPS功能
 - 7.2.2 在无线网卡上设置WPS加密
 - 7.2.3 在移动客户端上设置WPS加密
- 7.3 破解WPS加密
 - 7.3.1 使用Reaver工具
 - 7.3.2 使用Wifite工具
 - 7.3.3 使用Fern WiFi Cracker工具
- 第8章 WEP加密模式
 - 8.1 WEP加密简介
 - 8.1.1 什么是WEP加密
 - 8.1.2 WEP工作原理
 - 8.1.3 WEP漏洞分析
 - 8.2 设置WEP加密
 - 8.2.1 WEP加密认证类
 - 8.2.2 在AP中设置WEP加密模式
 - 8.3 破解WEP加密
 - 8.3.1 使用Aircrack-ng工具
 - 8.3.2 使用Wifite工具破解WEP加密
 - 8.3.3 使用Gerix WiFi Cracker工具破解WEP加密
 - 8.4 应对措施
- 第9章 WPA加密模式
 - 9.1 WPA加密简介
 - 9.1.1 什么是WPA加密
 - 9.1.2 WPA加密工作原理
 - 9.1.3 WPA弥补了WEP的安全问题
 - 9.2 设置WPA加密模式
 - 9.2.1 WPA认证类型
 - 9.2.2 加密算法
 - 9.2.3 设置AP为WPA加密模式
 - 9.3 创建密码字典
 - 9.3.1 使用Crunch工具
 - 9.3.2 使用pwgen工具
 - 9.3.3 创建彩虹表
 - 9.4 破解WPA加密
 - 9.4.1 使用Aircrack-ng工具
 - 9.4.2 使用Wifite工具破解WPA加密
 - 9.4.3 不指定字典破解WPA加密
 - 9.5 WPA的安全措施
- 第10章 WPA+RADIUS加密模式
 - 10.1 RADIUS简介
 - 10.1.1 什么是RADIUS协议
 - 10.1.2 RADIUS的工作原理
 - 10.2 搭建RADIUS服务
 - 10.2.1 安装RADIUS服务
 - 10.2.2 配置文件介绍
 - 10.3 设置WPA+RADIUS加密
 - 10.3.1 配置RADIUS服务
 - 10.3.2 配置MySQL数据库服务
 - 10.3.3 配置WiFi网络

10.4 连接RADIUS加密的WiFi网络
10.4.1 在Windows下连接RADIUS加密的WiFi网络
10.4.2 在Linux下连接RADIUS加密的WiFi网络
10.4.3 移动客户端连接RADIUS加密的WiFi网络
10.5 破解RADIUS加密的WiFi网络
10.5.1 使用hostapd-wpe创建伪AP
10.5.2 Kali Linux的问题处理
10.5.3 使用asleap破解密码
10.6 WPA+RADIUS的安全措施
• • • • • (收起)

[Kali Linux无线网络渗透测试详解_下载链接1](#)

标签

无线网络

网络安全

安全

kali

计算机科学

计算机安全

技术

web安全

评论

内容比较水。

干货较少。很多截图、命令输出结果有拼凑篇幅之嫌。

入门

内容不算特别详细，但该有的都有了

这本书仅仅是kali泛泛之谈，里面对kali做了最基本的讲解，等同于一本入门指南。如果想从这本书中得到什么破解无线密码的手段的话，还不如上网找点类似的文章。因为本书只是简单的介绍一些命令和工具，没有太复杂的具有实际操作意义的东西。当然基于本书面向的对象和网络安全的敏感性，也不可能会写得很具有操作性，一切都在于读者自己去挖掘。不过里面过多的截图和不必要的命令输出结果，占用了不小的篇幅，感觉是把读者当成一窍不通的外行人了。所以这本书对于有兴趣了解kali的人来说还是有些可看性的。对于专业的，还是看kali的文档吧。

[Kali Linux无线网络渗透测试详解_下载链接1](#)

书评

[Kali Linux无线网络渗透测试详解_下载链接1](#)