

《Kali Linux渗透测试技术详解》

图书基本信息

书名：《Kali Linux渗透测试技术详解》

13位ISBN编号：9787302389640

出版时间：2015-3-1

作者：杨波

页数：310

版权说明：本站所提供下载的PDF图书仅提供预览和简介以及在线试读，请支持正版图书。

更多资源请访问：www.tushu000.com

《Kali Linux渗透测试技术详解》

内容概要

编辑推荐

《Kali Linux渗透测试技术详解》由浅入深地介绍了Kali Linux的各种渗透测试技术。书中选取了最核心和最基础的内容进行讲解，让读者能够掌握渗透测试的流程，而不会被高难度的内容所淹没。《Kali Linux渗透测试技术详解》适合使用Linux各个层次的人员作为学习渗透测试技术的基础读物，也适合对安全、渗透感兴趣的人、网络管理员及专门从事搞安全的人员等阅读。

《Kali Linux渗透测试技术详解》

作者简介

作者简介

杨波 现就职于兰州文理学院电子信息工程学院，副教授。从事计算机教学与科研工作16年。熟悉Linux操作系统及相关开发，长期从事计算机网络及信息安全的研究。参编教材3部，在国内外发表学术论文10余篇，其中SCI论文1篇。

书籍目录

目录

第1篇Linux安全渗透测试基础

第1章Linux安全渗透简介

1.1什么是安全渗透

1.2安全渗透所需的工具

1.3Kali Linux简介

1.4安装Kali Linux

1.4.1安装至硬盘

1.4.2安装至USB驱动器

1.4.3安装至树莓派

1.4.4安装至VMware Workstation

1.4.5安装VMware Tools

1.5Kali更新与升级

1.6基本设置

1.6.1启动默认的服务

1.6.2设置无线网络

第2章配置Kali Linux

2.1准备内核头文件

2.2安装并配置NVIDIA显卡驱动

2.3应用更新和配置额外安全工具

2.4设置ProxyChains

2.5目录加密

2.5.1创建加密目录

2.5.2文件夹解密

第3章高级测试实验室

3.1使用VMwareWorkstation

3.2攻击WordPress和其他应用程序

3.2.1获取WordPress应用程序

3.2.2安装WordPress Turnkey Linux

3.2.3攻击WordPress应用程序

第2篇信息的收集及利用

第4章信息收集

4.1枚举服务

4.1.1DNS枚举工具DNSenum

4.1.2DNS枚举工具fierce

4.1.3SNMP枚举工具Snmpwalk

4.1.4SNMP枚举工具Snmpcheck

4.1.5SMTP枚举工具smtp—user—enum

4.2测试网络范围

4.2.1域名查询工具DMitry

4.2.2跟踪路由工具Scapy

4.3识别活跃的主机

4.3.1网络映射器工具Nmap

4.3.2使用Nmap识别活跃主机

4.4查看打开的端口

4.4.1TCP端口扫描工具Nmap

4.4.2图形化TCP端口扫描工具Zenmap

4.5系统指纹识别

4.5.1使用Nmap工具识别系统指纹信息

4.5.2指纹识别工具pOf

4.6服务的指纹识别

4.6.1使用Nmap工具识别服务指纹信息

4.6.2服务枚举工具Amap

4.7其他信息收集手段

4.7.1Recon—NG框架

4.7.2ARP侦查工具Netdiscover

4.7.3搜索引擎工具Shodan

4.8使用Maltego收集信息

4.8.1准备工作

4.8.2使用Maltego工具

4.9绘制网络结构图

第5章漏洞扫描

5.1使用Nessus

5.1.1安装和配置Nessus

5.1.2扫描本地漏洞

5.1.3扫描网络漏洞

5.1.4扫描指定Linux的系统漏洞

5.1.5扫描指定Windows的系统漏洞

5.2使用OpenVAS

5.2.1配置OpenVAS

5.2.2创建Scan Config和扫描任务

5.2.3扫描本地漏洞

5.2.4扫描网络漏洞

5.2.5扫描指定Linux系统漏洞

5.2.6扫描指定Windows系统漏洞

第6章漏洞利用

6.1Metasploitable操作系统

6.2Metasploit基础

6.2.1Metasploit的图形管理工具Armitage

6.2.2控制Metasploit终端 (MSFCONSOLE)

6.2.3控制Metasploit命令行接口 (MSFCLI)

6.3控制Meterpreter

6.4渗透攻击应用

6.4.1渗透攻击：MySQL数据库服务

6.4.2渗透攻击PostgreSQL数据库服务

6.4.3渗透攻击Tomcat服务

6.4.4渗透攻击Telnet服务

6.4.5渗透攻击Samba服务

6.4.6PDF文件攻击

6.4.7使用browser_autopwn模块渗透攻击浏览器

6.4.8在Metasploit中捕获包

6.5免杀Payload生成工具Veil

第3篇各种渗透测试

第7章权限提升

7.1使用假冒令牌

7.1.1工作机制

- 7.1.2使用假冒令牌
- 7.2本地权限提升
- 7.3使用社会工程学工具包 (SET)
 - 7.3.1启动社会工程学工具包
 - 7.3.2传递攻击载荷给目标系统
 - 7.3.3收集目标系统数据
 - 7.3.4清除踪迹
 - 7.3.5创建持久后门
 - 7.3.6中间人攻击 (MITM)
- 7.4使用SET实施攻击
 - 7.4.1针对性钓鱼攻击向量
 - 7.4.2Web攻击向量
 - 7.4.3PowerShell攻击向量
 - 7.4.4自动化中间人攻击工具Subterfuge

第8章密码攻击

- 8.1密码在线破解
 - 8.1.1Hydra工具
 - 8.1.2Medusa工具
- 8.2分析密码
 - 8.2.1Ettercap工具
 - 8.2.2使用MSFCONSOLE分析密码
 - 8.2.3哈希值识别工具Hash Identifier
- 8.3破解LM Hashes密码
- 8.4绕过Utilman登录
- 8.5破解纯文本密码工具mimikatz
- 8.6破解操作系统用户密码
 - 8.6.1破解Windows用户密码
 - 8.6.2破解Linux用户密码
- 8.7创建密码字典
 - 8.7.1Crunch工具
 - 8.7.2rtgen工具
- 8.8使用NVIDIA计算机统一设备架构 (CUDA)

8.9物理访问攻击

第9章无线网络渗透测试

- 9.1无线网络嗅探工具Kismet
- 9.2使用Aircrack-ng工具破解无线网络
 - 9.2.1破解WEP加密的无线网络
 - 9.2.2破解WPA / WPA2无线网络
 - 9.2.3攻击WPS (Wi-Fi Protected Setup)
- 9.3Gerix Wifi Cracker破解无线网络
 - 9.3.1Gerix破解WEP加密的无线网络
 - 9.3.2使用Gerix创建假的接入点
- 9.4使用Wifite破解无线网络
- 9.5使用Easy-Creds工具攻击无线网络
- 9.6在树莓派上破解无线网络
- 9.7攻击路由器
- 9.8Arpspoof工具
 - 9.8.1URL流量操纵攻击
 - 9.8.2端口重定向攻击

9.8.3捕获并监视无线网络数据

《Kali Linux渗透测试技术详解》

精彩短评

- 1、安装就花了N多篇幅来讲，大段大段的截图，真是醉了。show options 这种命令有必要把结果都截图下来吗？不推荐。
- 2、安装系统就啰啰嗦嗦讲了一大堆，最后的工具就是一个一个介绍，以及把man的内容。全书基本上就是把文档用中文写了一遍 + 英文的文档就复制粘贴 + 配了很多截图凑页数，书名叫做《渗透测试技术详解》，实难苟同
- 3、还不如乌云wiki好用。
- 4、同事买了一本，大体浏览过一遍，一个个工具的累积，恕我浅薄，读完了感觉不知道讲了些什么....认识了几个新工具，后期也没用过....
- 5、很明显是本攒出来的书，通篇不知所云。
如今的人急功近利，为了名利真是啥都不顾了。
- 6、当初看的。。。乌云也狗带了。o()o
- 7、比说明书略微好点的感觉，感觉各个章节之间并不连贯，而且讲述的软件还有重复现象，对于一位学者来说，这样的书未免是不严谨。不过照着书看下来，同时实践一下下，还是有些收获的。

《Kali Linux渗透测试技术详解》

版权说明

本站所提供下载的PDF图书仅提供预览和简介，请支持正版图书。

更多资源请访问:www.tushu000.com