

图书基本信息

书名：《Kali Linux & BackTrack渗透测试实战》

13位ISBN编号：9787115370583

出版时间：2014-11

作者：[韩] 赵涎元 等

页数：510

译者：金光爱

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

内容概要

渗透测试业务整体流程理解
咨询业务经验、技巧及项目经理必备知识
Kali Linux Live CD与BackTrack工具分析简易方法
利用Kali Linux与BackTrack的诊断业务高效强化方案
攻击者角度的技术技巧与实际管理业务中的有效应对方案
利用BackTrack进行渗透测试的基础知识
Kali Linux与BackTrack的比较
利用Kali Linux进行渗透测试深化诊断的方法

书籍目录

第1章 认识渗透测试的业务流程	1
1.1 渗透测试的定义	1
1.2 执行访问的方法	2
1.3 进行渗透测试的业务范围	3
1.4 检查清单	12
1.5 项目投标阶段	13
1.6 范围和对象选定阶段	15
1.7 环境信息收集阶段	17
1.8 深化渗透测试攻击和编写报告阶段	18
1.9 小结	19
第2章 认识BackTrack	20
2.1 BackTrack的定义	20
2.2 BackTrack V5的变化	21
2.3 Kali Linux登场	21
2.4 安装BackTrack	31
2.5 安装Kali Linux	38
2.5.1 安装到虚拟机	39
2.5.2 安装到硬盘	41
2.5.3 安装Windows和双启动模式	47
2.6 在智能手机上安装BackTrack	60
2.6.1 准备安装	60
2.6.2 安装	62
2.6.3 BackTrack的启动和结束	64
2.7 构建检测对象环境	70
2.7.1 应用Metasploitable V2	70
2.7.2 DVL	73
2.7.3 云测试环境服务	74
2.7.4 其他测试环境	74
2.8 小结	75
第3章 信息收集阶段	76
3.1 主机查看过程	76
3.1.1 收集DNS信息	76
3.1.2 查看真实主机	88
3.2 网络扫描过程	102
3.2.1 Netifera：查看网络/服务信息	102
3.2.2 autoscan：查看详细服务信息	106
3.2.3 Unicornscan：收集网络信息	110
3.2.4 scapy：网络数据包操作	113
3.3 小结	119
第4章 信息收集详细阶段	120
4.1 收集服务信息	120
4.1.1 Nmap：查看服务漏洞信息	120
4.1.2 利用Nmap NSE深化诊断	125
4.1.3 Dnmap：分布式Nmap	151
4.1.4 httpprint：收集网络服务信息	155
4.1.5 dmitry：收集主机信息	159
4.2 查看IDS/IPS是否已启用	160

4.2.1	Waffit : 查看网络应用防火墙是否已启用	161
4.2.2	UA-tester : 收集网络服务信息	162
4.3	利用搜索服务收集信息	165
4.3.1	GHDB : 谷歌搜索工具	165
4.3.2	Metagoofil : 利用谷歌搜索收集文件	169
4.3.3	goofile : 利用谷歌搜索收集文件	179
4.3.4	goohost : 利用谷歌搜索收集服务信息	181
4.3.5	fimap : 利用谷歌搜索收集信息并攻击	182
4.3.6	利用谷歌搜索进行防御	185
4.4	小结	186
第5章	漏洞评估阶段	187
5.1	收集服务漏洞	187
5.1.1	DirBuster : 查看目录结构	187
5.1.2	mantra : 利用网络浏览器插件收集信息	192
5.1.3	Nessus : 收集和评估服务漏洞	195
5.1.4	Nikto : 收集和评估服务漏洞	208
5.2	诊断CMS服务漏洞	211
5.2.1	joomscan : 收集服务漏洞信息	211
5.2.2	WPScan : 收集服务漏洞信息	213
5.2.3	WordPress安全设置	216
5.2.4	WhatWeb : 收集服务信息	238
5.3	小结	240
第6章	漏洞诊断阶段	241
6.1	深化攻击工具	241
6.1.1	Metasploit : 诊断框架	241
6.1.2	Fasttrack : 自动攻击工具	290
6.1.3	Fasttrack GUI : 自动攻击工具	297
6.1.4	Exploit-DB : 收集最新漏洞信息	297
6.2	查看是否为已获认证的通信	299
6.2.1	SSLScan : 查看通信是否已加密	299
6.2.2	digicert : 查看是否已适用SSL认证书	301
6.3	数据库漏洞诊断	302
6.3.1	SQLmap : 获取数据库信息	302
6.3.2	sqlsus : 把握数据库结构	317
6.4	社会工程学攻击技术	320
6.4.1	SET : 社会工程学	321
6.4.2	BeEF XSS框架 : 获取用户权限	332
6.5	小结	345
第7章	深化渗透攻击阶段	346
7.1	认识文件上传漏洞	346
7.2	网络后门攻击	348
7.2.1	简单分析Web shell	348
7.2.2	利用weevely制作后门	349
7.3	防御网络后门攻击	352
7.3.1	防御源代码级	352
7.3.2	考虑使用Web shell检测功能	353
7.4	攻击OS后门	358
7.4.1	cymothoa : 后门shellcode插入工具	358
7.4.2	Cryptcat : 传送加密通信数据	361

7.5	小结	365
第8章	密码破解诊断	366
8.1	脱机密码破解工具	366
8.1.1	John the Ripper：破解密码	366
8.1.2	hashcat：密码恢复工具	368
8.1.3	crunch：生成字典文件	375
8.1.4	cupp：生成字典文件	376
8.1.5	hash-identifier：识别算法类型	378
8.1.6	dictstat：把握密码结构	381
8.1.7	ophcrack：破解密码	385
8.2	联机密码破解工具	389
8.2.1	hydra：登录密码破解工具	389
8.2.2	medusa：登录密码破解工具	395
8.2.3	findmyhash：联机破解数据库	397
8.3	获取网络嗅探信息	400
8.3.1	ettercap：创建网络嗅探环境	400
8.3.2	SSLStrip：SSL通信绕过攻击	408
8.3.3	ferret：网络嗅探攻击	411
8.3.4	hamster：通过网络嗅探收集信息	413
8.3.5	TShark：分析网络数据包	417
8.4	小结	428
第9章	无线网络诊断	429
9.1	认识无线网络诊断	429
9.2	破解技术	430
9.2.1	破解WEP密钥	431
9.2.2	WEP密钥破解安全对策	435
9.2.3	破解WPA密钥	436
9.2.4	WPA密钥破解安全对策	440
9.3	会话劫持攻击	441
9.4	运用其他工具	445
9.4.1	GERIX-GUI：Aircrack-ng GUI版本	445
9.4.2	reaver：无线破解工具	450
9.4.3	easy-creds：自动化综合工具	452
9.5	无线AP固件和应用程序漏洞增加	460
9.6	小结	460
第10章	编写报告阶段	462
10.1	RecordMyDesktop：录制视频	462
10.2	Magictree：管理诊断结果	468
10.3	制定报告编写框架	473
10.4	服务影响度评估	476
10.5	小结	479
附录	渗透测试和系统安全初学者须知	480
索引		504

精彩短评

- 1、kali linux backtrack渗透测试实战
- 2、挺好的一本书，适合有一定网络基础的读者进一步实战。
- 3、基本上是一本实用手册类型的图书，按照kali/BackTrack系统的菜单目录划分，对各个目录中的主要工具进行了简介，可以作为入门读物学习和验证使用。

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