

《渗透测试实践指南：必知必会的工尽

图书基本信息

书名：《渗透测试实践指南：必知必会的工具与方法(原书第2版)》

13位ISBN编号：9787111473442

出版时间：2014-8-12

作者：Patrick Engebretson

页数：182

译者：姚军,姚明

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

《渗透测试实践指南：必知必会的工尽》

内容概要

美国国家安全局主管Keith B.Alexander将军鼎力推荐；以独特性的ZEH方法，结合前沿、实用的开源工具，采用科学、有序的方法，高级渗透测试专家为你呈现渗透测试和黑客活动的领域全景。

书籍目录

《渗透测试实践指南：必知必会的工具与方法(原书第2版)》

译者序

前言

致谢

第1章 什么是渗透测试 1

1.1 简介 1

1.2 搭建平台 2

1.3 kali和backtrack linux工具简介 4

1.4 使用backtrack：启动引擎 8

1.5 黑客实验环境的搭建与使用 11

1.6 渗透测试的步骤 13

1.7 接下来该做什么 16

1.8 本章小结 17

第2章 侦察 18

2.1 简介 19

2.2 htrack：网站复制机 22

2.3 google指令——google搜索实践 25

2.4 the harvester：挖掘并利用邮箱地址 30

2.5 whois 33

2.6 netcraft 35

2.7 host工具 36

2.8 从dns中提取信息 37

2.8.1 ns lookup 38

2.8.2 dig 40

2.8.3 fierce：在区域传输失败时该做什么 40

2.9 从电子邮件服务器提取信息 41

2.10 metagoofil 42

2.11 threatagent drone攻击 43

2.12 社会工程 45

2.13 筛选信息寻找可攻击的目标 46

2.14 如何实践 47

2.15 接下来该做什么 47

2.16 本章小结 48

第3章 扫描 49

3.1 简介 49

3.2 ping和ping扫描 52

3.3 端口扫描 54

3.3.1 三次握手 56

3.3.2 使用nmap进行tcp连接扫描 56

3.3.3 使用nmap进行syn扫描 58

3.3.4 使用nmap进行udp扫描 59

3.3.5 使用nmap执行xmas扫描 61

3.3.6 使用nmap执行null扫描 62

3.3.7 nmap脚本引擎：化蛹成蝶 63

3.3.8 端口扫描总结 65

3.4 漏洞扫描 66

3.5 如何实践 70

- 3.6 接下来该做什么 71
- 3.7 本章小结 72
- 第4章 漏洞利用 73
 - 4.1 简介 74
 - 4.2 利用medusa获得远程服务的访问权限 75
 - 4.3 metasploit：用hugh jackman的方式进行入侵 78
 - 4.4 john the ripper：密码破解之王 90
 - 4.4.1 本地密码破解 92
 - 4.4.2 远程密码破解 99
 - 4.4.3 linux密码破解和权限提升的一个简单例子 99
 - 4.5 密码重置：破墙而入 100
 - 4.6 wireshark：嗅探流量 103
 - 4.7 macof：巧妇能为无米之炊 104
 - 4.8 armitage：入侵工具中的超级明星 107
 - 4.9 为什么要学习五个工具 110
 - 4.10 如何实践 112
 - 4.11 接下来该做什么 114
 - 4.12 本章小结 116
- 第5章 社会工程 117
 - 5.1 简介 117
 - 5.2 set基础知识 118
 - 5.3 网站攻击向量 120
 - 5.4 凭据采集器 125
 - 5.5 set中的其他选项 127
 - 5.6 本章小结 128
- 第6章 基于web的漏洞利用 129
 - 6.1 简介 130
 - 6.2 web入侵基础知识 130
 - 6.3 扫描web服务器：nikto 132
 - 6.4 w3af：不是徒有其表 132
 - 6.5 网络爬虫：抓取目标网站 135
 - 6.6 使用webscarab拦截请求 138
 - 6.7 代码注入攻击 140
 - 6.8 跨站脚本：轻信网站的浏览器 144
 - 6.9 zed attack proxy：一网打尽 146
 - 6.9.1 在zap中拦截 147
 - 6.9.2 zap中的爬虫功能 148
 - 6.9.3 zap中的扫描功能 149
 - 6.10 如何实践 149
 - 6.11 接下来该做什么 150
 - 6.12 其他相关资源 151
 - 6.13 本章小结 152
- 第7章 维持访问 153
 - 7.1 简介 154
 - 7.2 netcat：瑞士军刀 154
 - 7.3 netcat神秘的家族成员：cryptcat 160
 - 7.4 rootkit 160
 - 7.5 rootkit的检测与防御 166
 - 7.6 meterpreter：无所不能 167

- 7.7 如何实践 169
- 7.8 接下来该做什么 170
- 7.9 本章小结 171
- 第8章 渗透测试总结 172
 - 8.1 简介 172
 - 8.2 编写渗透测试报告 173
 - 8.2.1 综合报告 174
 - 8.2.2 详细报告 174
 - 8.2.3 原始输出 176
 - 8.3 不应到此为止 178
 - 8.4 接下来该做什么 180
 - 8.5 回顾 181
 - 8.6 学无止境 182
 - 8.7 本章小结 182

《渗透测试实践指南：必知必会的工尽

精彩短评

- 1、比上一版本更新了一些软件，适合入门阅读
 - 2、很好的入门书 架构清晰
 - 3、简单易懂清晰的入门书
 - 4、上一版翻翻可以丢了，还好我是买盗版的。
- （还写向奥巴马汇报，我去）
<script>alert("别看了，关了吧！烂书一本")</script>

《渗透测试实践指南：必知必会的工尽

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