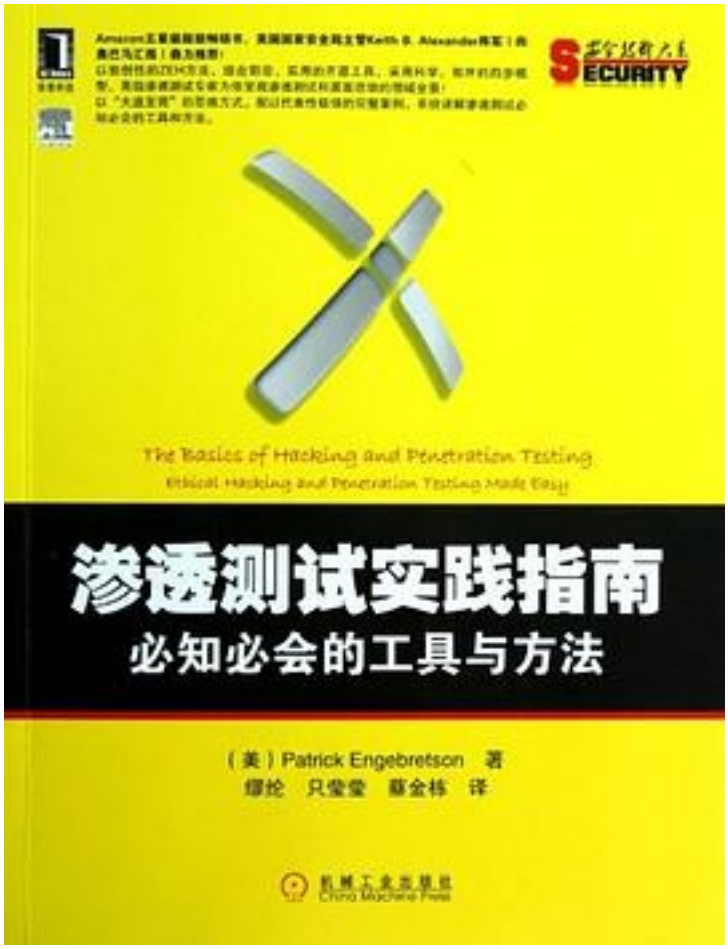
渗透测试实践指南



渗透测试实践指南_下载链接1_

著者:Patrick Engebretson

出版者:机械工业出版社华章公司

出版时间:2012-11-20

装帧:平装

isbn:9787111401414

“你是否听说过渗透测试但不知道它包含哪些内容？本书就是你步入渗透测试领域的良好开端，它简单易读，也不需要什么先验知识，而且其内容也是当前最流行的。我诚挚向你推荐Pat的最新力作。”——Jared Demott，Crucial

Security股份有限公司首席安全研究员

本书以“大道至简”的方式阐述了高深的“道德黑客”和“渗透测试”的知识，通过讲解操作案例和技术细节（涵盖四个阶段，其间穿插多种实用、前沿的热点工具和技巧），让你了解通用知识和真正的渗透测试工作；令人期待的是，部分案例为你真实再现好莱坞大片中的神秘“黑客”情景。

本书结合大量可操作性极强的实例和步骤图解，通过输出结果将渗透测试四个阶段和所用工具巧妙关联，使你不再为只知其一而踌躇不前，从而真正掌握渗透测试精髓，余下的提升问题也迎刃而解。

本书主要内容：

□ 搭建渗透测试环境技巧及注意事项；

□ 侦察阶段的各种可利用工具及其参数设置，包括HTTrack、Google搜索指令、The Harvester、DNS和电子邮件服务器信息提取、MetaGooFil等；

□
扫描系统和网络漏洞的切实可用工具和方法，ping命令和ping扫描、端口扫描（如Nmap、Nessus等）；

□
漏洞利用过程涉及的常用黑客工具和技巧，如密码重置和破解、嗅探网络流量、自动化漏洞攻击和Web漏洞扫描、Web服务器扫描、拦截请求、代码注入、跨站脚本等；

□ 后门和rootkit的利用方法及rootkit的检测和防御，涵盖
Netcat、Cryptcat、Netbus等实用工具；

□ 如何编写渗透测试报告为你赢得回头客。

作者介绍:

Patrick
Engebretson，高级渗透测试专家，达科他州立大学信息安全专业博士。专注于渗透测试、黑客活动、入侵检测、漏洞利用、蜜罐技术和恶意软件的研究和实践，于多个领域发表了多篇颇负盛名的专业论文。曾受国土安全部的邀请，在华盛顿特区软件保障论坛上介绍其研究成果，并在拉斯维加斯黑帽大会上发表演讲。活跃于高级开发人员社区和渗透测试社区，同时拥有多种认证证书。

目录: 译者序
前言
致谢
第1章 渗透测试1
1.1 内容简介1
1.2 Backtrack Linux介绍3
1.3 使用Backtrack：启动引擎7
1.4 黑客实验环境的搭建与使用10
1.5 渗透测试的步骤11
1.6 本章回顾15
1.7 小结15
第2章 侦察17

2.1 内容简介17
2.2 HTTrack：网站复制机21
2.3 Google指令—Google搜索实践24
2.4 The Harvester：挖掘并利用邮箱地址29
2.5 Whois31
2.6 Netcraft34
2.7 host工具35
2.8 从DNS中提取信息36
2.8.1 NS Lookup 37
2.8.2 Dig 39
2.9 从电子邮件服务器提取信息39
2.10 MetaGooFil40
2.11 社会工程学42
2.12 筛选信息以寻找可攻击的目标43
2.13 如何实践44
2.14 接下来该做什么44
2.15 小结45
第3章 扫描47
3.1 内容简介47
3.2 ping和ping扫描50
3.3 端口扫描52
3.3.1 三次握手 53
3.3.2 使用Nmap进行TCP连接扫描 54
3.3.3 使用Nmap进行SYN扫描 55
3.3.4 使用Nmap进行UDP扫描 57
3.3.5 使用Nmap执行Xmas扫描 60
3.3.6 使用Nmap执行Null扫描 61
3.3.7 端口扫描总结 62
3.4 漏洞扫描63
3.5 如何实践66
3.6 接下来该做什么68
3.7 小结68
第4章 漏洞利用69
4.1 内容简介69
4.2 利用Medusa获得远程服务的访问权限71
4.3 Metasploit74
4.4 John the Ripper：密码破解之王87
4.5 密码重置：破墙而入96
4.6 嗅探网络流量99
4.7 macof：泛洪攻击交换机100
4.8 Fast-Track Autopwn：自动化漏洞攻击104
4.9 如何实践108
4.10 接下来该做什么110
4.11 小结112
第5章 基于Web的漏洞利用115
5.1 内容简介115
5.2 扫描Web服务器：Nikto116
5.3 Websecurify: 自动化的Web漏洞扫描117
5.4 网络爬虫：抓取目标网站119
5.5 使用WebScarab拦截请求122
5.6 代码注入攻击125
5.7 跨站脚本：轻信网站的浏览器 129
5.8 如何实践133
5.9 接下来该做什么134

5.10 小结135
第6章 使用后门和rootkit维持访问137
6.1 内容简介137
6.2 Netcat：瑞士军刀138
6.3 Netcat神秘的家族成员：Cryptcat144
6.4 Netbus：一款经典的工具145
6.5 rootkit146
6.6 rootkit的检测与防御152
6.7 如何实践154
6.8 接下来该做什么155
6.9 小结156
第7章 渗透测试总结157
7.1 内容简介157
7.2 编写渗透测试报告158
7.2.1 综合报告 159
7.2.2 详细报告 159
7.2.3 原始输出 161
7.3 继续前行164
7.4 接下来该做什么166
7.5 结束语168
7.6 学无止境169
7.7 小结169
・・・・・・(收起)

渗透测试实践指南_下载链接1_

标签

渗透测试

渗透

黑客

信息安全

网络安全

计算机安全

安全

计算机

评论

黑的框架 整体感很强 练习资源很丰富

2小时刷完…了解了好多工具……真是可怕的网络…读到后来真是心惊胆战…要是能更专注于背后的原理和理论就更好了…

半天翻完，比研究生网络安全课程好太多

挺有趣的书，适合我这种入门的人看看。尤其是google的使用部分和加facebook好友来获取目标信息的例子更是让人印象深刻。

---
clean

ZEH的好书

系统

被低估的好书 豆瓣很多时候评分真的只是参考。

入门

值得一看的书， 特别是想转Linux运维的伙计。

极简入门推荐读物。

二刷了，作为入门书不错，挺喜欢的。在图书馆借的，新的一本书被我翻得皱皱的。反正我是一点基础都没有的，还是很有可操作性的，就是。。。里面的技术不会过时了吧。。。？

真是贵死了

渗透测试实践指南_下载链接1_

书评

说的工具都是BT5里面有的，还只是挑几个常用的工具简单地说一下，唯一的好处是对BT50基础的还可以看看！ 里面的方法论有一定渗透经验的都懂好不! 不值这个价啊！抱歉，你的评论太短了抱歉，你的评论太短了抱歉，你的评论太短了抱歉，你的评论太短了抱歉，你的评论太短了抱...

渗透测试实践指南_下载链接1_