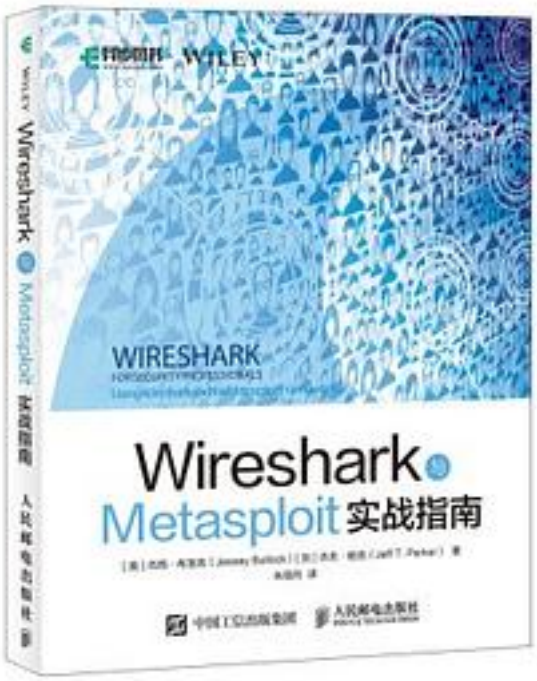
# Wireshark与Metasploit实战指南




Wireshark与Metasploit实战指南_下载链接1_

著者:[美]杰西·布洛克 [加]杰夫·帕克

出版者:人民邮电出版社

出版时间:2019-3

装帧:平装

isbn:9787115506573

Wireshark是流行的网络嗅探软件，对于数据包的抓取和分析，以及网络故障的分析和修复来说都是一个非常好的工具。本书的主题是关于Wireshark和网络安全的，全书共计8章，融合了网络安全、渗透测试、虚拟系统、Wireshark、Kali Linux、Metasploit套装和Lua等多个技术点。除此之外，本书还结合虚拟环境，对各类网络攻击进行了模拟，帮助读者深入把握网络分析技术。本书内容实用性较强，案例也非常丰富，适合读者边学边尝试，在实践中掌握分析技能。本书适合所有对网络安全感兴趣的读者阅读，也适合想要学习Wireshark这一强大工具的读者参考使用。

作者介绍:

杰西·布洛克（Jessey
Bullock）是一位拥有多种不同行业背景的安全工程师，他既做过安全顾问担任过机构内的安全团队成员。杰西是从网络支持管理领域逐渐进入安全行业的，Wireshark一直是他的随身工具集。他丰富的技术才华在各个领域都广受认可，例如能源和金融圈，包括游戏界。

杰夫·T·帕克（Jeff T.
Parker）是一位安全专家和技术撰稿人。他在DEC公司有20年的工作经验，然后服务过康柏和惠普两家公司。杰夫的工作主要是为复杂的企业环境提供咨询，在惠普工作期间，杰夫的兴趣逐渐从系统转向安全，因为安全更需要学习和持续的分享。

目录: 第 1章 Wireshark入门介绍 1
1．1 Wireshark是什么 1
1．1．1 什么时候该用Wireshark 2
1．1．2 避免被大量数据吓到 3
1．2 用户界面 3
1．2．1 分组列表面板 5
1．2．2 分组详情面板 6
1．2．3 分组字节流面板 8
1．3 过滤器 9
1．3．1 捕获过滤器 9
1．3．2 展示过滤器 13
1．4 小结 18
1．5 练习 18
第 2章 搭建实验环境 19
2．1 Kali Linux操作系统 20
2．2 虚拟化技术 21
2．2．1 基本术语和概念 22
2．2．2 虚拟化的好处 22
2．3 VirtualBox 23
2．3．1 安装VirtualBox 23
2．3．2 安装VirtualBox扩展软件包 30
2．3．3 创建一个Kali Linux虚拟机 32
2．3．4 安装Kali Linux 39
2．4 W4SP Lab实验环境 45
2．4．1 W4SP Lab的环境需求 45
2．4．2 关于Docker的几句话 46
2．4．3 什么是GitHub 47
2．4．4 创建实验环境用户 48
2．4．5 在Kali虚拟机里安装W4SP Lab实验环境 49
2．4．6 设置 W4SP Lab 51
2．4．7 Lab网络 53
2．5 小结 54
2．6 练习 54
第3章 基础知识 55
3．1 网络基础知识 55
3．1．1 OSI层级 56
3．1．2 虚拟机之间的联网 59
3．2 安全 61
3．2．1 安全三要素 61
3．2．2 入侵检测和防护系统 61

3．2．3 误报和漏洞 62
3．2．4 恶意软件 62
3．2．5 欺骗和污染 64
3．3 分组数据包和协议分析 64
3．3．1 一个协议分析的故事 65
3．3．2 端口和协议 69
3．4 小结 71
3．5 练习 72
第4章 捕获分组数据包 73
4．1 嗅探 73
4．1．1 混杂模式 74
4．1．2 开始第 一次抓包 75
4．1．3 TShark 80
4．2 各种网络环境下的抓包 84
4．2．1 本地机器 85
4．2．2 对本地环路的嗅探 86
4．2．3 虚拟机的接口上嗅探 90
4．2．4 用集线器做嗅探 93
4．2．5 SPAN端口 95
4．2．6 网络分流器 98
4．2．7 透明Linux网桥 100
4．2．8 无线网络 102
4．3 加载和保存捕获文件 105
4．3．1 文件格式 105
4．3．2 以环形缓冲区和多文件方式保存 108
4．3．3 最近捕获文件列表 113
4．4 解析器 114
4．4．1 W4SP Lab：处理非标准的HTTP 流量 115
4．4．2 过滤SMB文件名 116
4．4．3 用颜色标记数据包 120
4．5 查看他人的捕获文件 123
4．6 小结 124
4．7 练习 125
第5章 攻击分析 126
5．1 攻击类型：中间人攻击 127
5．1．1 为什么中间人攻击能奏效 128
5．1．2 ARP中间人攻击的成因 128
5．1．3 W4SP Lab：执行ARP中间人攻击 130
5．1．4 W4SP Lab：执行DNS中间人攻击 137
5．1．5 如何防范中间人攻击 144
5．2 攻击类型：拒绝服务攻击 145
5．2．1 为什么DoS攻击能奏效 145
5．2．2 DoS攻击是怎么实现的 146
5．2．3 如何防范DoS攻击 151
5．3 攻击类型：APT攻击 152
5．3．1 为什么APT攻击管用 152
5．3．2 APT攻击是怎么实施的 153
5．3．3 APT流量在Wireshark里的例子 153
5．3．4 如何防范APT攻击 157
5．4 小结 158
5．5 练习 158
第6章 Wireshark之攻击相关 159
6．1 攻击套路 159
6．2 用Wireshark协助踩点侦察 161

6．3 规避IPS/IDS的检测 164
6．3．1 会话切割和分片 164
6．3．2 针对主机，而不是IDS 165
6．3．3 掩盖痕迹和放置后门 165
6．4 漏洞利用 166
6．4．1 在W4SP实验环境里增加Metasploitable节点 167
6．4．2 启动Metasploit控制台 167
6．4．3 VSFTP Exploit 168
6．4．4 使用Wireshark协助调试 169
6．4．5 Wireshark里查看shell执行 171
6．4．6 从TCP流里观察正向shell 172
6．4．7 从TCP流里观察反向shell 179
6．4．8 启动ELK 184
6．5 通过SSH远程抓包 186
6．6 小结 187
6．7 练习 187
第7章 解密TLS、USB抓包、键盘记录器和绘制网络拓扑图 188
7．1 解密SSL/TLS 188
7．1．1 用私钥解密SSL/TLS 190
7．1．2 使用SSL/TLS会话密钥解密 194
7．2 USB和Wireshark 196
7．2．1 在Linux下捕获USB流量 197
7．2．2 在Windows下捕获USB流量 201
7．2．3 TShark键盘记录器 202
7．3 绘制网络关系图 206
7．4 小结 212
7．5 练习 213
第8章 Lua编程扩展 214
8．1 为什么选择Lua 214
8．2 Lua编程基础 215
8．2．1 变量 217
8．2．2 函数和代码块 218
8．2．3 循环 220
8．2．4 条件判断 222
8．3 Lua设置 223
8．3．1 检查Lua支持 223
8．3．2 Lua初始化 224
8．3．3 Windows环境下的Lua设置 225
8．3．4 Linux环境下的Lua设置 225
8．4 Lua相关工具 226
8．4．1 TShark里的Hello World 228
8．4．2 统计数据包的脚本 229
8．4．3 模拟ARP缓存表脚本 233
8．5 创建Wireshark解析器 236
8．5．1 解析器的类型 237
8．5．2 为什么需要解析器 237
8．5．3 动手实验 245
8．6 扩展Wireshark 247
8．6．1 数据包流向脚本 247
8．6．2 标记可疑的脚本 249
8．6．3 嗅探SMB文件传输 252
8．7 小结 255
・・・・・・(收起)

Wireshark与Metasploit实战指南_下载链接1_

## 标签

抓包

Wireshark

网络安全

web

架构

## 评论

很不错的一本书

---
这本书，，配套的环境国内估计拉不起来，不过自己可以改一下

---
Wireshark与Metasploit实战指南_下载链接1_

## 书评

---
Wireshark与Metasploit实战指南_下载链接1_