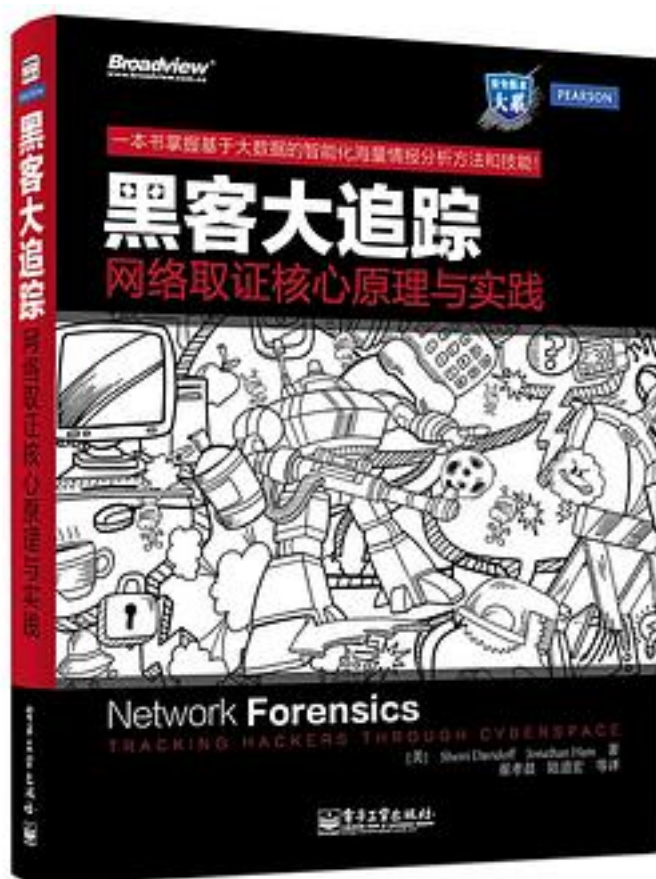


黑客大追踪



[黑客大追踪_下载链接1](#)

著者:[美] Sherri Davidoff

出版者:电子工业出版社

出版时间:2015-1

装帧:平装

isbn:9787121245541

网络取证是计算机取证技术的一个新的发展方向，是计算机网络技术与法学的交叉学科。《黑客大追踪：网络取证核心原理与实践》是网络取证方面的第一本专著，一经出版便好评如潮，在Amazon网站上的评分达4.5星。

《黑客大追踪：网络取证核心原理与实践》根据网络取证调查人员的实际需要，概述了网络取证的各个方面，不论是对各种网络协议的分析和对各种网络设备的处理方式，还是取证流程的设计都有独到之处。

《黑客大追踪：网络取证核心原理与实践》共分四大部分十二章，第1章“实用调查策略”，第2章“技术基础”和第3章“证据获取”属于第一部分，其中给出了一个取证的方法框架，并介绍了相关的基础知识；第4章“数据包分析”，第5章“流统计分析”、第6章“无线：无须网线的取证”和第7章“网络入侵的侦测及分析”属于第二部分，介绍了对网络流量进行分析的各种技术；第8章“事件日志的聚合、关联和分析”、第9章“交换机、路由器、防火墙”和第10章“Web代理”属于第三部分，详述了在各种网络设备和服务器中获取和分析证据的方法。第11章“网络隧道”和第12章“恶意软件取证”属于第四部分，针对网络隧道和恶意软件分析这两个网络取证中的难点和热点问题展开讨论。

《黑客大追踪：网络取证核心原理与实践》在学术理论上具有交叉性、前沿性和创新性，在实践应用中注重可操作性和实用性。可作为网络安全/计算机取证专业的教材，对于司法工作者、律师、司法鉴定人和IT从业人员，也具有良好的参考价值。

作者介绍:

目录: 第一部分 基础篇

第1章 实用调查策略 2

1.1 真实的案例 2

1.1.1 医院里被盗的笔记本电脑 3

1.1.2 发现公司的网络被用于传播盗版 5

1.1.3 被黑的政府服务器 6

1.2 足迹 7

1.3 电子证据的概念 8

1.3.1 实物证据 9

1.3.2 最佳证据 9

1.3.3 直接证据 10

1.3.4 情况证据 11

1.3.5 传闻证据 11

1.3.6 经营记录 12

1.3.7 电子证据 13

1.3.8 基于网络的电子证据 14

1.4 关于网络证据相关的挑战 14

1.5 网络取证调查方法（OSCAR） 15

1.5.1 获取信息 15

1.5.2 制订方案 16

1.5.3 收集证据 17

1.5.4 分析 18

1.5.5 出具报告 19

1.6 小结 19

第2章 技术基础 21

2.1 基于网络的证据来源 21

2.1.1 物理线缆 22

2.1.2 无线网络空口 22

2.1.3 交换机 23

2.1.4 路由器 23

2.1.5 DHCP服务器 24

2.1.6 域名服务器 24

2.1.7 登录认证服务器	25
2.1.8 网络入侵检测/防御系统	25
2.1.9 防火墙	25
2.1.10 Web代理	26
2.1.11 应用服务器	27
2.1.12 中央日志服务器	27
2.2 互联网的工作原理	27
2.2.1 协议	28
2.2.2 开放系统互连模型	29
2.2.3 例子：周游世界……然后再回来	30
2.3 互联网协议组	32
2.3.1 互联网协议组的早期历史和开发过程	33
2.3.2 网际协议	34
2.3.3 传输控制协议	38
2.3.4 用户数据报协议	40
2.4 小结	42
第3章 证据获取	43
3.1 物理侦听	43
3.1.1 线缆	44
3.1.2 无线电频率	48
3.1.3 Hub	49
3.1.4 交换机	50
3.2 流量抓取软件	52
3.2.1 libpcap和WinPcap	53
3.2.2 伯克利包过滤（Berkeley Packet Filter，BPF）语言	53
3.2.3 tcpdump	57
3.2.4 Wireshark	61
3.2.5 tshark	62
3.2.6 dumpcap	62
3.3 主动式获取	63
3.3.1 常用接口	63
3.3.2 没有权限时咋办	68
3.3.3 策略	68
3.4 小结	69
第二部分 数据流分析	
第4章 数据包分析	72
4.1 协议分析	73
4.1.1 哪里可以得到协议信息	73
4.1.2 协议分析工具	76
4.1.3 协议分析技巧	79
4.2 包分析	91
4.2.1 包分析工具	91
4.2.2 包分析技术	94
4.3 流分析	99
4.3.1 流分析工具	100
4.3.2 流分析技术	103
4.4 分析更高层的传输协议	113
4.4.1 一些常用的高层协议	114
4.4.2 高层协议分析工具	122
4.4.3 高层协议分析技术	124
4.5 结论	127
4.6 案例研究：Ann的约会	127
4.6.1 分析：协议概要	128
4.6.2 DHCP通信	128

4.6.3 关键词搜索	130
4.6.4 SMTP分析——Wireshark	133
4.6.5 SMTP分析——TCPFlow	136
4.6.6 SMTP 分析——附件提取	137
4.6.7 查看附件	139
4.6.8 找到Ann的简单方法	140
4.6.9 时间线	145
4.6.10 案件的理论推导	145
4.6.11 挑战赛问题的应答	146
4.6.12 下一步	148
第5章 流统计分析	149
5.1 处理过程概述	150
5.2 传感器	151
5.2.1 传感器类型	151
5.2.2 传感器软件	152
5.2.3 传感器位置	153
5.2.4 修改环境	154
5.3 流记录导出协议	155
5.3.1 NetFlow	155
5.3.2 IPFIX	156
5.3.3 sFlow	156
5.4 收集和汇总	157
5.4.1 收集器的位置和架构	157
5.4.2 数据收集系统	158
5.5 分析	160
5.5.1 流记录分析技术	160
5.5.2 流记录分析工具	164
5.6 结论	169
5.7 案例研究：奇怪的X先生	169
5.7.1 分析：第一步	170
5.7.2 外部攻击者和端口22的通信	171
5.7.3 DMZ中的受害者——10.30.30.20（也是172.30.1.231）	174
5.7.4 内部受害系统——192.30.1.101	178
5.7.5 时间线	179
5.7.6 案件分析	180
5.7.7 回应挑战赛问题	180
5.7.8 下一步	181
第6章 无线：无须网线的取证	183
6.1 IEEE 第二层协议系列	184
6.1.1 为什么那么多第二层协议	185
6.1.2 802.11 协议族	186
6.1.3 802.1X	195
6.2 无线接入点（WAP）	196
6.2.1 为什么要调查无线接入点	196
6.2.2 无线接入点的类型	196
6.2.3 WAP证据	200
6.3 无线数据捕获及分析	201
6.3.1 频谱分析	201
6.3.2 无线被动证据收集	202
6.3.3 有效地分析802.11	203
6.4 常见攻击类型	205
6.4.1 嗅探	205
6.4.2 未授权的无线接入点	205
6.4.3 邪恶双子	208

6.4.4 WEP破解	208
6.5 定位无线设备	209
6.5.1 获取设备描述	210
6.5.2 找出附近的无线接入点	210
6.5.3 信号强度	211
6.5.4 商业化企业级工具	213
6.5.5 Skyhook	214
6.6 总结	215
6.7 案例研究：HackMe公司	215
6.7.1 调查WAP	216
6.7.2 快速粗略的统计	221
6.7.3 对于管理帧的深层次观察	226
6.7.4 一个可能的“嫌疑犯”	228
6.7.5 时间线	229
6.7.6 案例总结	230
6.7.7 挑战问题的应答	231
6.7.8 下一步	233
第7章 网络入侵的侦测及分析	235
7.1 为什么要调查NIDS/NIPS	236
7.2 NIDS/NIPS的典型功能	236
7.2.1 嗅探	236
7.2.2 高层协议辨识	237
7.2.3 可疑字节的报警	238
7.3 检测的模式	239
7.3.1 基于特征的分析	239
7.3.2 协议辨识	239
7.3.3 行为分析	239
7.4 NIDS/NIPS的种类	239
7.4.1 商业化NIDS/NIPS	239
7.4.2 自我定制	241
7.5 NIDS/NIPS的电子证据采集	241
7.5.1 电子证据类型	241
7.5.2 NIDS/NIPS界面	243
7.6 综合性网络封包日志	244
7.7 Snort系统	245
7.7.1 基本结构	246
7.7.2 配置	246
7.7.3 Snort规则语言	247
7.7.4 例子	249
7.8 总结	251
7.9 教学案例：InterOptic拯救地球（第一部分）	252
7.9.1 分析：Snort 警报	253
7.9.2 初步数据包分析	254
7.9.3 Snort规则分析	255
7.9.4 从Snort抓包数据中提取可疑文件	257
7.9.5 “INFO Web Bug”警报	257
7.9.6 “Tcp Window Scale Option”警报	259
7.9.7 时间线	261
7.9.8 案情推测	261
7.9.9 下一步	262
第三部分 网络设备和服务器	
第8章 事件日志的聚合、关联和分析	266
8.1 日志来源	267
8.1.1 操作系统日志	267

8.1.2	应用日志	275
8.1.3	物理设备日志	277
8.1.4	网络设备日志	279
8.2	网络日志的体系结构	280
8.2.1	三种类型的日志记录架构	280
8.2.2	远程日志：常见问题及应对方法	282
8.2.3	日志聚合和分析工具	283
8.3	收集和分析证据	285
8.3.1	获取信息	285
8.3.2	策略制定	286
8.3.3	收集证据	287
8.3.4	分析	289
8.3.5	报告	290
8.4	总结	290
8.5	案例：L0ne Sh4rk的报复	290
8.5.1	初步分析	291
8.5.2	可视化失败的登录尝试	292
8.5.3	目标账户	294
8.5.4	成功登录	295
8.5.5	攻陷后的活动	296
8.5.6	防火墙日志	297
8.5.7	内部受害者——192.30.1.101	300
8.5.8	时间线	301
8.5.9	案件结论	303
8.5.10	对挑战问题的应答	303
8.5.11	下一步	304
第9章	交换机、路由器和防火墙	305
9.1	存储介质	305
9.2	交换机	306
9.2.1	为什么调查交换机	306
9.2.2	内容寻址内存表	307
9.2.3	地址解析协议	307
9.2.4	交换机类型	308
9.2.5	交换机证据	309
9.3	路由器	310
9.3.1	为什么调查路由器	310
9.3.2	路由器类型	310
9.3.3	路由器上的证据	312
9.4	防火墙	313
9.4.1	为什么调查防火墙	313
9.4.2	防火墙类型	313
9.4.3	防火墙证据	315
9.5	接口	317
9.5.1	Web接口	317
9.5.2	控制台命令行接口（CLI）	318
9.5.3	远程控制台	319
9.5.4	简单网络管理协议（SNMP）	319
9.5.5	私有接口	320
9.6	日志	320
9.6.1	本地日志	321
9.6.2	简单网络管理协议	322
9.6.3	syslog	322
9.6.4	身份验证、授权和账户日志	323
9.7	总结	323

9.8 案例研究：Ann的咖啡环	323
9.8.1 防火墙诊断命令	325
9.8.2 DHCP服务日志	326
9.8.3 防火墙访问控制列表	327
9.8.4 防火墙日志分析	327
9.8.5 时间线	331
9.8.6 案例分析	332
9.8.7 挑战问题的答复	333
9.8.8 下一步	334
第10章 Web代理	335
10.1 为什么要调查Web代理	335
10.2 Web代理的功能	337
10.2.1 缓存	337
10.2.2 URI过滤	339
10.2.3 内容过滤	339
10.2.4 分布式缓存	339
10.3 证据	341
10.3.1 证据的类型	341
10.3.2 获取证据	342
10.4 Squid	342
10.4.1 Squid的配置文件	343
10.4.2 Squid的Access日志文件	343
10.4.3 Squid缓存	344
10.5 Web代理分析	346
10.5.1 Web代理日志分析工具	347
10.5.2 例子：剖析一个Squid磁盘缓存	350
10.6 加密的Web流量	357
10.6.1 TLS（传输层安全）	358
10.6.2 访问加密的内容	360
10.6.3 商用的TLS/SSL拦截工具	364
10.7 小结	364
10.8 教学案例：InterOptic拯救地球（之二）	365
10.8.1 分析：pwny.jpg	366
10.8.2 Squid缓存的网页的提取	368
10.8.3 Squid的Access.log文件	371
10.8.4 进一步分析Squid缓存	373
10.8.5 时间线	377
10.8.6 案情推测	379
10.8.7 回答之前提出的问题	380
10.8.8 下一步	381
第四部分 高级议题	
第11章 网络隧道	384
11.1 功能型隧道	384
11.1.1 背景知识：VLAN链路聚集	385
11.1.2 交换机间链路（Inter-Switch Link, ISL）	385
11.1.3 通用路由封装（Generic Routing Encapsulation, GRE）	386
11.1.4 Teredo：IPv4网上的IPv6	386
11.1.5 对调查人员的意义	387
11.2 加密型隧道	387
11.2.1 IPsec	388
11.2.2 TLS和SSL	389
11.2.3 对取证人员的影响	390
11.3 隐蔽通信型隧道	391
11.3.1 策略	391

11.3.2 TCP序列号	391
11.3.3 DNS隧道	392
11.3.4 ICMP隧道	393
11.3.5 例子：分析ICMP隧道	395
11.3.6 对调查人员的影响	398
11.4 小结	399
11.5 案例教学：Ann的秘密隧道	400
11.5.1 分析：协议统计	401
11.5.2 DNS分析	402
11.5.3 追查隧道传输的IP包	405
11.5.4 对隧道传输的IP包的分析	409
11.5.5 对隧道传输的TCP报文段的分析	412
11.5.6 时间线	414
11.5.7 案情推测	414
11.5.8 回答之前提出的问题	415
11.5.9 下一步	416
第12章 恶意软件取证	418
12.1 恶意软件进化的趋势	419
12.1.1 僵尸网络	419
12.1.2 加密和混淆	420
12.1.3 分布式命令和控制系统	422
12.1.4 自动自我升级	426
12.1.5 变化形态的网络行为	428
12.1.6 混在网络活动中	434
12.1.7 Fast-Flux DNS	436
12.1.8 高级持续威胁（Advanced Persistent Threat, APT）	437
12.2 恶意软件的网络行为	440
12.2.1 传播	441
12.2.2 命令和控制通信	443
12.2.3 载荷的行为	446
12.3 未来的恶意软件和网络取证	446
12.4 教学案例：Ann的“极光行动”	447
12.4.1 分析：入侵检测	447
12.4.2 TCP会话：10.10.10.10:4444–10.10.10.70:1036	449
12.4.3 TCP会话：10.10.10.10:4445	455
12.4.4 TCP会话：10.10.10.10:8080–10.10.10.70:1035	461
12.4.5 时间线	466
12.4.6 案情推测	467
12.4.7 回答之前提出的问题	468
12.4.8 下一步	468
后记	470
• • • • •	(收起)

[黑客大追踪 下载链接1](#)

标签

安全

网络

取证

计算机

网络战

网络取证

黑客大追踪

美国

评论

2016-11: 1作为教材来用，对技术和操作层面介绍较多，但理论方面较少。实践方面，对新手的引导例子较少。许多分析的数据集若能提供作为训练会更好。

全是优点，但是很简洁了

毫无实用价值 专程来刷恶评的！~~

挺好的一本书。对网络取证的场景和维度覆盖的还算全，方法论和思路不错的。算是事件和理论并重。尤其是在有幸参加了Sherri的取证课程后，更是觉得不错

工作需要 找来翻了翻 书中用到wireshark等软件的地方好多……

讲的太皮毛了，本打算用来开拓思维的。

我能说这本书拉低了安全技术大系的水准么，翻译也是一般

[黑客大追踪 下载链接1](#)

书评

[黑客大追踪 下载链接1](#)