

《数据驱动的网络分析》

图书基本信息

书名：《数据驱动的网络分析》

13位ISBN编号：9787115376719

出版时间：2015-3

作者：Michael Collins

页数：264

译者：姚军

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.tushu111.com

《数据驱动的网络分析》

内容概要

传统的入侵检测和日志文件分析已经不再足以保护当今的复杂网络，本书讲解了多种网络流量数据集的采集和分析技术及工具，借助这些工具，可以迅速定位网络中的问题，并采取相应的行动，保障网络的运行安全。

《数据驱动的网络分析》分为3部分，共15章，内容包括数据采集的常规过程，用于采集网络流量的传感器，基于特定系统的传感器，数据存储和分析，使用互联网层次知识系统（SiLK）分析NetFlow数据，用于安全分析的R语言简介、入侵检测系统的工作机制以及实施，确定实施攻击的幕后真凶，探索性数据分析以及数据可视化，检查通信流量和行为，获取网络映射和库存盘点的详细过程等。

《数据驱动的网络分析》适合网络安全工程师和网络管理人员阅读。

《数据驱动的网络分析》

作者简介

Michael Collins，是RedJack有限责任公司的首席科学家，该公司是华盛顿首都特区的一家网络安全和数据分析公司。在任职于RedJack之前，Collins博士是卡内基·梅隆大学CERT/网络态势感知小组的成员。他的主要研究方向是网络测量和流量分析，特别是大流量数据集的分析。Collins博士于2008年毕业于卡内基·梅隆大学，获得电子工程博士学位。他的硕士和学士学位也来自于同一学校。

书籍目录

第1部分 数据

第1章 传感器和探测器简介3

1.1 观察点：传感器的位置对数据采集的影响4

1.2 领域：确定可以采集的数据7

1.3 操作：传感器对数据所做的处理10

1.4 小结12

第2章 网络传感器13

2.1 网络分层及其对测量的影响14

2.1.1 网络层次和观察点16

2.1.2 网络层次和编址19

2.2 封包数据20

2.2.1 封包和帧格式21

2.2.2 滚动缓存21

2.2.3 限制每个封包中捕捉的数据21

2.2.4 过滤特定类型封包21

2.2.5 如果不是以太网怎么办25

2.3 NetFlow26

2.3.1 NetFlow v5格式和字段26

2.3.2 NetFlow生成和采集28

第3章 主机和服务传感器：在源上的流量日志29

3.1 访问和操纵日志文件30

3.2 日志文件的内容32

3.2.1 优秀日志消息的特性32

3.2.2 现有日志文件以及处理方法34

3.3 有代表性的日志文件格式36

3.3.1 HTTP：CLF和ELF36

3.3.2 SMTP39

3.3.3 Microsoft Exchange：邮件跟踪日志41

3.4 日志文件传输：转移、Syslog和消息队列43

3.4.1 转移和日志文件留存43

3.4.2 syslog43

第4章 用于分析的数据存储：关系数据库、大数据和其他选项46

4.1 日志数据和CRUD范式47

4.2 NoSQL系统简介49

4.3 使用何种存储方法52

第2部分 工具

第5章 SiLK套件56

5.1 SiLK的概念和工作原理56

5.2 获取和安装SiLK57

5.3 选择和格式化输出字段操作：rwcut58

5.4 基本字段操纵：rfilter63

5.4.1 端口和协议63

5.4.2 大小65

5.4.3 IP地址65

5.4.4 时间66

5.4.5 TCP选项67

5.4.6 助手选项68

- 5.4.7 杂项过滤选项和一些技巧69
- 5.5 rfileinfo及出处69
- 5.6 合并信息流：rwcoun72
- 5.7 rwsset和IP集74
- 5.8 rwuniq77
- 5.9 rwbag79
- 5.10 SiLK高级机制79
- 5.11 采集SiLK数据81
 - 5.11.1 YAF81
 - 5.11.2 rwptoflow83
 - 5.11.3 rwtuc84
- 第6章 R安全分析简介86
 - 6.1 安装与设置86
 - 6.2 R语言基础知识87
 - 6.2.1 R提示符87
 - 6.2.2 R变量88
 - 6.2.3 编写函数93
 - 6.2.4 条件与循环95
 - 6.3 使用R工作区97
 - 6.4 数据帧98
 - 6.5 可视化101
 - 6.5.1 可视化命令101
 - 6.5.2 可视化参数101
 - 6.5.3 可视化注解103
 - 6.5.4 导出可视化104
 - 6.6 分析：统计假设检验104
 - 6.6.1 假设检验105
 - 6.6.2 检验数据107
- 第7章 分类和事件工具：IDS、AV和SEM110
 - 7.1 IDS的工作原理110
 - 7.1.1 基本词汇111
 - 7.1.2 分类器失效率：理解“基率谬误”114
 - 7.1.3 应用分类116
 - 7.2 提高IDS性能117
 - 7.2.1 改进IDS检测118
 - 7.2.2 改进IDS响应122
 - 7.2.3 预取数据122
- 第8章 参考和查找：了解“某人是谁”的工具124
 - 8.1 MAC和硬件地址124
 - 8.2 IP编址126
 - 8.2.1 IPv4地址、结构和重要地址126
 - 8.2.2 IPv6地址、结构和重要地址128
 - 8.2.3 检查连接性：使用ping连接到某个地址129
 - 8.2.4 路由跟踪131
 - 8.2.5 IP信息：地理位置和人口统计学特征132
 - 8.3 DNS133
 - 8.3.1 DNS名称结构133
 - 8.3.2 用dig转发DNS查询134
 - 8.3.3 DNS反向查找142

- 8.3.4 使用whois查找所有者143
- 8.4 其他参考工具146
- 第9章 其他工具148
 - 9.1 可视化148
 - 9.2 通信和探查151
 - 9.2.1 netcat151
 - 9.2.2 nmap153
 - 9.2.3 Scapy154
 - 9.3 封包检查和参考157
 - 9.3.1 Wireshark157
 - 9.3.2 GeolIP157
 - 9.3.3 NVD、恶意软件网站和C*E158
 - 9.3.4 搜索引擎、邮件列表和人160
- 第3部分 分析
- 第10章 探索性数据分析和可视化162
 - 10.1 EDA的目标：应用分析163
 - 10.2 EDA工作流程165
 - 10.3 变量和可视化166
 - 10.4 单变量可视化：直方图、QQ图、箱线图和等级图167
 - 10.3.1 直方图167
 - 10.3.2 柱状图（不是饼图）169
 - 10.3.3 分位数—分位数（Quantile—Quantile，QQ）图170
 - 10.3.4 五数概括法和箱线图172
 - 10.3.5 生成箱线图173
 - 10.5 双变量描述175
 - 10.5.1 散点图175
 - 10.5.2 列联表177
 - 10.6 多变量可视化177
- 第11章 摸索185
 - 11.1 攻击模式185
 - 11.2 摸索：错误的配置、自动化和扫描187
 - 11.2.1 查找失败187
 - 11.2.2 自动化188
 - 11.2.3 扫描188
 - 11.3 识别摸索行为189
 - 11.3.1 TCP摸索：状态机189
 - 11.3.2 ICMP消息和摸索192
 - 11.3.3 识别UDP摸索193
 - 11.4 服务级摸索193
 - 11.4.1 HTTP摸索193
 - 11.4.2 SMTP摸索195
 - 11.5 摸索分析195
 - 11.5.1 构建摸索警报196
 - 11.5.2 摸索行为的取证分析196
 - 11.5.3 设计一个网络来利用摸索197
- 第12章 通信量和时间分析199
 - 12.1 工作日对网络通信量的影响199
 - 12.2 信标201
 - 12.3 文件传输 / 攫取204

- 12.4 局部性206
 - 12.4.1 DDoS、突发拥塞和资源耗尽209
 - 12.4.2 DDoS和路由基础架构210
- 12.5 应用通信量和局部性分析214
 - 12.5.1 数据选择214
 - 12.5.2 将通信量作为警报216
 - 12.5.3 将信标作为警报216
 - 12.5.4 将局部性作为警报217
 - 12.5.5 工程解决方案217
- 第13章 图解分析219
 - 13.1 图的属性：什么是图219
 - 13.2 标签、权重和路径222
 - 13.3 分量和连通性227
 - 13.4 聚类系数228
 - 13.5 图的分析229
 - 13.5.1 将分量分析作为警报229
 - 13.5.2 将集中度分析用于取证230
 - 13.5.3 广度优先搜索的取证使用231
 - 13.5.4 将集中度分析用于工程232
- 第14章 应用程序识别234
 - 14.1 应用程序识别机制234
 - 14.1.1 端口号234
 - 14.1.2 通过标志抓取识别应用程序238
 - 14.1.3 通过行为识别应用程序241
 - 14.1.4 通过附属网站识别应用程序244
 - 14.2 应用程序标志：识别和分类245
 - 14.2.1 非Web标志245
 - 14.2.2 Web客户端标志：User-Agent字符串246
- 第15章 网络映射249
 - 15.1 创建一个初始网络库存清单和映射249
 - 15.1.1 创建库存清单：数据、覆盖范围和文件250
 - 15.1.2 第1阶段：前3个问题251
 - 15.1.3 第2阶段：检查IP空间254
 - 15.1.4 第3阶段：识别盲目和难以理解的流量258
 - 15.1.5 第4阶段：识别客户端和服务端261
 - 15.2 更新库存清单：走向连续审计263

《数据驱动的网络分析》

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.tushu111.com