

УДК 004.058

ББК 32.973

К60

Майкл Коллинз

К60 Защита сетей. Подход на основе анализа данных / пер. с англ. А.В. Добровольская. – М.: ДМК Пресс, 2020. – 308 с.: ил.

ISBN 978-5-97060-649-0

Эта книга – подробное пошаговое руководство по эффективному использованию доступных инструментов обеспечения безопасности сетей. Её оценят как опытные специалисты по безопасности, так и новички.

Подробно рассматриваются процессы сбора и организации данных, инструменты для их анализа, а также различные аналитические сценарии и методики.

Издание идеально подходит для системных администраторов и специалистов по операционной безопасности, владеющих навыками написания скриптов.

УДК 004.458

ББК 32.973

All rights reserved. This work may not be translated or copied in whole or in part without the written permission of the author, except for brief excerpts in connection with reviews or scholarly analysis. Use in connection with any form of information storage and retrieval, electronic adaptation, or computer software is forbidden

Все права защищены. Любая часть этой книги не может быть воспроизведена в какой бы то ни было форме и какими бы то ни было средствами без письменного разрешения владельцев авторских прав.

ISBN 978-1-449-35790-0 (анг.)

ISBN 978-5-97060-649-0 (рус.)

© 2016 Michael Collins

© Оформление, издание, перевод, ДМК Пресс, 2020

Оглавление

Об авторе	5
Предисловие	11
Целевая аудитория	13
Содержание книги	14
Принятые обозначения	16
Использование примеров кода	17
Safari® Books Online (Сафари Букс Онлайн)	17
Контактная информация	18
Благодарственное слово	18
Предисловие от издательства	19
Отзывы и пожелания	19
Список опечаток	19
Нарушение авторских прав	19
ЧАСТЬ I. ДАННЫЕ	21
Глава 1. Сенсоры и детекторы: введение	23
Область обзора сенсора: зависимость сбора данных от расположения сенсора	24
Уровни расположения сенсоров: какие данные можно собрать	27
Действия сенсора: как сенсор обрабатывает данные	30
Заключение	32
Глава 2. Сетевые сенсоры	33
Влияние уровней сети на ее оснащение	34
Уровни сети и область обзора сенсоров	36
Уровни сети и адресация	40
Пакетные данные	41
Форматы пакетов и фреймов	42
Циклический (кольцевой) буфер	42
Лимитирование захваченных пакетных данных	42
Фильтрация специфических типов пакетов	43
Если вы не используете Ethernet	46
NetFlow	47
Форматы и поля NetFlow v5	47
«Поток и наполнение». NetFlow v9 и стандарт IPFIX	48
Генерация и сбор данных в NetFlow	49
Дополнительные материалы для чтения	50
Глава 3. Датчики хостов и сервисов: журналирование трафика в источнике данных	51
Доступ и управление файлами журнала	52
Содержание файлов журнала	54

Характеристики хорошего сообщения журнала	54
Существующие файлы журнала, и как ими управлять	57
Представительные форматы файла журнала	58
HTTP: CLF и ELF	58
SMTP	62
Microsoft Exchange: журналы, отслеживающие сообщения	64
Транспорт файла журнала: передачи, системы и очереди сообщений	65
Передача и ротация файла журнала	65
Системный журнал	66
Дополнительные материалы для чтения	67

Глава 4. Хранение данных для анализа: реляционные базы

данных, большие данные и другие опции	68
Данные журналов и парадигма CRUD	69
Создание хорошо организованной плоской файловой системы: уроки от SiLK	70
Краткое введение в системы NoSQL	72
Какой подход к хранению данных использовать	75
Иерархия устройств хранения данных, время выполнения запроса и старение	77

Часть II. Инструменты

Глава 5. Комплект SiLK

Что такое SiLK, и как он работает?	81
Получение и установка SiLK	82
Файлы данных	82
Выбор и форматирование выходного управления полем: rwcut	83
Основное управление полем: rwfilt	87
Порты и протоколы	88
Размер	89
IP-адреса	89
Время	91
Опции TCP	91
Вспомогательные опции	93
Разные опции фильтрации и некоторые взломы	94
rwfileinfo и источник	94
Объединение информационных потоков: rwcoun	96
rwset и IP Sets	98
rwuniq	101
rwbag	103
Усовершенствованные средства SiLK	103
pmaps	104
Сбор данных SiLK	105
YAF	106
rwptoflow	108
rwtuc	108
Дополнительные материалы для чтения	109

Глава 6. Введение в R для аналитиков

по вопросам безопасности	110
Установка и настройка	111
Основы языка	111

Подсказка R	111
R-переменные	113
Запись функций	118
Условные выражения и итерация	119
Использование рабочей области R	121
Фреймы данных	122
Визуализация	125
Команды визуализации	126
Параметры визуализации	126
Аннотация технологии визуализации	128
Экспорт визуализации	129
Анализ: проверка статистических гипотез	129
Проверка гипотез	130
Тестирование данных	132
Дополнительные материалы для чтения	134

Глава 7. Классификация и инструменты события:

IDS, AV и SEM	135
Как работает IDS	135
Базовый словарь	136
Частота отказов классификатора: понимание ошибки базовой ставки	140
Применение классификации	142
Улучшение производительности IDS	143
Улучшение обнаружения IDS	144
Улучшение ответа IDS	148
Упреждающая выборка данных	149
Дополнительные материалы для чтения	150

Глава 8. Ссылка и поиск: инструменты

для выяснения, кто есть кто	151
MAC и аппаратные адреса	151
IP-адресация	153
Адреса IPv4, их структура и важные адреса	154
Адреса IPv6, их структура и важные адреса	155
Проверка возможности соединения: используйте ping для соединения с адресом	157
Tracerouting	158
Интеллект IP: геолокация и демография	160
DNS	161
Структура имени DNS	161
Направление DNS-запроса с использованием dig	163
Обратный поиск DNS	169
Использование whois для нахождения владельца	171
Дополнительные ссылочные инструменты	173
DNSBLs	174

Глава 9. Больше инструментов

Визуализация	176
Graphviz	176
Связь и зондирование	179
netcat	179
nmap	181
Scapy	182

Проверка пакетов и ссылка.....	184
Wireshark.....	185
GeoIP	185
NVD, вредоносные сайты и C*Es	186
Поисковые системы, списки рассылки и люди	187
Дополнительные материалы для чтения.....	188

ЧАСТЬ III. АНАЛИТИКА.....189

Глава 10. Разведочный анализ данных и визуализация191

Цель разведочного анализа: проведение анализа	193
Порядок выполнения разведочного анализа	194
Переменные и визуализация.....	196
Визуализация одномерных данных:	
гистограммы, графики квантилей и коробчатые диаграммы.....	197
Гистограммы	197
Столбиковые диаграммы.....	199
Графики квантилей	200
Пятичисловая сводка и коробчатая диаграмма	202
Создание коробчатой диаграммы	203
Визуализация двумерных данных.....	206
Диаграммы рассеяния	206
Таблицы сопряженности	208
Визуализация многомерных данных.....	209
Оперативная визуализация.....	211
Дополнительные материалы для чтения.....	217

Глава 11. О «прощупывании»218

Модели нападения.....	218
Прощупывание: неверная конфигурация, автоматизация и сканирование	221
Ошибки в процессе поиска.....	221
Автоматизация.....	222
Сканирование.....	222
Определение попытокощупывания.....	223
Прощупывание TCP: диаграмма состояний.....	223
Сообщения ICMP иощупывание	226
Определениеощупывания в UDP	227
Прощупывание на уровне сервисов	228
Прощупывание HTTP.....	228
Прощупывание SMTP.....	230
Анализ попытокощупывания	230
Создание предупреждений оощупывании	230
Расследование попытокощупывания	231
Проектирование сети для извлечения пользы отощупывания	232
Дополнительные материалы для чтения.....	233

Глава 12. Анализ объема и времени.....234

Влияние рабочих часов на объем трафика	234
Тревожные сигналы.....	237
Рейдерство – несанкционированное копирование файлов	239
Локальность	243

Отказ в обслуживании, флешмобы и исчерпание ресурсов.....	245
DDoS и инфраструктура маршрутизации.....	246
Применение анализа объема и локальности.....	251
Сбор данных	252
Создание тревог на основе объема	254
Создание тревог из тревожных сигналов.....	254
Создание тревог по признакам локальности	255
Инженерные решения	256
Дополнительные материалы для чтения.....	256
Глава 13. Анализ графа	257
Атрибуты графа: что такое граф?	257
Метки, вес и пути.....	261
Компоненты и возможность соединения	266
Коэффициент кластеризации	267
Анализ графов.....	268
Создание тревог с использованием анализа компонентов	268
Использование оценок центральности при расследовании	270
Использование поиска в ширину при расследовании	270
Использование анализа центральности для проектирования	272
Дополнительные материалы для чтения.....	272
Глава 14. Идентификация приложения.....	273
Механизмы идентификации приложений	273
Номер порта	274
Идентификация приложений по баннерам	277
Идентификация приложений по поведению.....	280
Идентификация приложений по обращениям к сайтам	284
Баннеры приложений: идентификация и классификация.....	285
Баннеры, не принадлежащие браузерам.....	285
Баннеры веб-клиентов: заголовок User-Agent	286
Дополнительные материалы для чтения.....	287
Глава 15. Сетевое картирование.....	288
Создание начальной описи и карты сети	288
Создание описи: данные, охват и файлы	289
Этап I: три первых вопроса	290
Этап II: исследование пространства IP-адресов	293
Этап III: выявление слепого и странного трафика	297
Этап IV: идентификация клиентов и серверов.....	301
Идентификация инфраструктуры контроля и блокирования	303
Обновление описи: к непрерывному аудиту.....	303
Дополнительные материалы для чтения.....	304
Предметный указатель.....	305