

УДК 004.382
ББК 32.973-018
Э61

Энсон С.

Э61 Реагирование на компьютерные инциденты. Прикладной курс / пер. с англ. Д. А. Беликова. – М.: ДМК Пресс, 2021. – 436 с.: ил.

ISBN 978-5-97060-484-7

Эта книга написана практиками и для практиков, которым необходимо ежедневно выявлять действия злоумышленников в сетях и сдерживать кибератаки. Опираясь на свой опыт расследования вторжений, а также консультирования глобальных клиентов и разработки средств для цифровой криминалистики, автор предлагает наиболее эффективные методы борьбы с киберпреступниками.

Реагирование на инцидент информационной безопасности рассматривается в книге как непрерывный цикл, а не разовая процедура. Представлено несколько моделей реагирования на инциденты с учетом специфики современных киберугроз; обсуждаются меры по их предупреждению. В первой части речь идет о подготовке к реагированию на компьютерные атаки, затем подробно рассматриваются практические действия по обнаружению злоумышленника и устранению последствий взлома.

Подчеркивая, что хакерские тактики непрерывно обновляются, автор приводит ссылки на сторонние ресурсы, где можно найти самую свежую информацию по теме компьютерной безопасности.

УДК 004.382
ББК 32.973-018

This Translation publish under license with the original publisher John Wiley & Sons, Inc. Russian language edition copyright © 2021 by DMK Press. All rights reserved.

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 978-1-119-56026-5 (англ.)
ISBN 978-5-97060-484-7 (рус.)

© John Wiley & Sons, Inc., 2020
© Оформление, издание, перевод,
ДМК Пресс, 2021

Содержание

Предисловие	11
Об авторе	17
От издательства	19
Часть I. ПОДГОТОВКА	20
Глава 1. Картина угроз.....	21
Мотивы злоумышленника	21
Кража интеллектуальной собственности.....	22
Атака на цепочку поставок	22
Финансовые махинации	22
Вымогательство	23
Шпионаж	23
Власть	24
Хактивизм.....	24
Жажда мести.....	24
Методы атаки.....	25
DoS и DDoS	25
Черви	26
Программы-вымогатели	27
Фишинг.....	28
Целевой фишинг.....	28
Атака типа «водопой».....	29
Веб-атаки	29
Атаки на беспроводные сети	30
Анализ сетевого трафика и атака посредника	30
Криптомайнинг	30
Атаки с целью получения пароля	31
Анатомия атаки	32
Разведка и сбор данных	32
Эксплуатация	33
Расширение/внедрение	34
Утечка данных / ущерб	35
Удаление следов.....	35
Современный злоумышленник	36
Учетные данные – «ключи от королевства».....	37
Заключение	39

Глава 2. Готовность к инцидентам	41
Подготовка процесса	41
Подготовка персонала	47
Подготовка технологии	51
Обеспечение адекватной видимости	54
Вооружаем специалистов	58
Непрерывность бизнес-процессов и аварийное восстановление	59
Методы обмана	61
Заключение	65
Часть II. РЕАГИРОВАНИЕ НА КИБЕРИНЦИДЕНТЫ	66
Глава 3. Удаленная сортировка	67
В поисках зла	68
Нестандартные подключения	69
Необычные процессы	72
Необычные порты	75
Необычные службы	76
Подозрительные учетные записи	76
Необычные файлы	78
Места автозапуска	80
Охрана учетных данных	81
Разбираемся с интерактивными входами в систему	82
Меры предосторожности при работе с инцидентом ИБ	84
Режим Restricted Admin для протокола удаленного рабочего стола и Remote Credential Guard	85
Заключение	87
Глава 4. Инструменты удаленной сортировки	88
Windows Management Instrumentation	88
Синтаксис WMI и WMIC	89
Правильные подходы с точки зрения компьютерной криминалистики	92
Элементы WMIC и WQL	93
Примеры команд WMIC	99
PowerShell	105
Основные командлеты PowerShell	108
PowerShell Remoting	112
Доступ к WMI/MI/CIM с помощью PowerShell	116
Фреймворки, используемые при реагировании на инциденты	119
Заключение	121
Глава 5. Создание дампа памяти	123
Порядок сбора улик	123
Сбор данных, хранящихся в памяти локальной системы	126

Подготовка носителя.....	127
Процесс сбора данных.....	129
Сбор данных, хранящихся в памяти удаленной системы	137
WMIC для сбора данных из удаленной системы	139
PowerShell Remoting для сбора данных, хранящихся в памяти удаленной системы	142
Агенты для удаленного сбора данных	145
Анализ памяти в реальном времени.....	149
Анализ памяти локальной системы в реальном времени.....	149
Анализ памяти удаленной системы в реальном времени	150
Заключение	151

Глава 6. Создание образа диска 152

Защита целостности улик	152
Создание образа по типу dead-box	156
Использование аппаратного блокиратора записи.....	158
Использование загрузочного дистрибутива Linux.....	162
Создание образа во время работы системы	168
Создание образа во время работы локальной системы.....	168
Создание образа во время работы системы удаленно.....	174
Создание образа виртуальной машины.....	176
Заключение	180

Глава 7. Мониторинг сетевой безопасности 181

Security Onion.....	181
Архитектура	182
Инструменты	185
Анализ текстового журнала	215
Заключение	218

Глава 8. Анализ журнала событий 220

Журналы событий.....	220
События, связанные с учетной записью	228
Доступ к объекту.....	238
Аудит изменений конфигурации системы	242
Аудит процессов	245
Аудит использования PowerShell.....	250
Использование PowerShell для запроса журналов событий	252
Заключение	254

Глава 9. Анализ памяти 256

Важность базовых показателей	257
Источники данных памяти	262
Использование Volatility и Rekall	264

Изучение процессов	269
Плагин pslist	269
Плагин pstree	271
Плагин dlllist	273
Плагин psxview	274
Плагин handles	274
Плагин malfind	275
Изучение служб Windows	276
Изучение сетевой активности	279
Обнаружение аномалий.....	281
Все дело в практике	289
Заключение	290
 Глава 10. Анализ вредоносных программ.....	291
Аналитические онлайн-сервисы	291
Статический анализ	294
Динамический анализ.....	301
Ручной динамический анализ	301
Автоматизированный анализ вредоносных программ.....	314
Уклоняемся от обнаружения.....	321
Реверс-инжиниринг	322
Заклучение	325
 Глава 11. Извлечение информации с образа жесткого диска	326
Инструменты компьютерной криминалистики.....	326
Анализ временных меток	329
Файлы ссылок и списки переходов	334
Папка Prefetch.....	336
Монитор использования системных ресурсов	337
Анализ реестра	339
Активность браузера	348
Журнал USN.....	351
Теневые копии томов	353
Автоматическая сортировка.....	355
Артефакты Linux/UNIX.....	356
Заклучение	360
 Глава 12. Анализ дальнейшего распространения по сети.....	361
Server Message Block	361
Атаки pass-the-hash.....	367
Атаки на Kerberos.....	369
Атаки pass-the-ticket и overpass-the-hash.....	370
Золотые и серебряные мандаты	377
Kerberoasting	380
PsExec	382

Запланированные задания	384
Команда sc.....	386
Протокол удаленного рабочего стола.....	387
Windows Management Instrumentation.....	389
Windows Remote Management	390
PowerShell Remoting	391
SSH-туннели и другие способы дальнейшего распространения по сети	393
Заключение	395
Часть III. УЛУЧШЕНИЕ	396
Глава 13. Непрерывное улучшение	397
Документировать и еще раз документировать	397
Утверждение мер по сглаживанию последствий	398
Опираемся на успехи и учимся на ошибках	400
Улучшение средств защиты	403
Привилегированные учетные записи	404
Контроль над выполнением	408
PowerShell.....	410
Сегментация и изоляция	412
Заключение	413
Глава 14. Активные действия	414
Поиск киберугроз	414
Эмуляция действий злоумышленника.....	423
Atomic Red Team.....	425
Caldera	430
Заключение	431
Предметный указатель	433