

УДК 004.056

ББК 16.8

076

Редактор:

Островская Светлана – ведущий специалист по реагированию на инциденты и компьютерной криминалистике в Group-IB.

Светлана Островская, Олег Скулкин

076 Криминалистика компьютерной памяти на практике: Как эффективно анализировать оперативную память / авторизован. пер. с англ. А. А. Слинкина. – М.: ДМК Пресс, 2023. – 256 с.: ил.

ISBN 978-5-93700-157-3

Книга знакомит читателя с современными концепциями активного поиска угроз и исследования передового вредоносного ПО с применением свободно распространяемых инструментов и фреймворков для анализа памяти. В издании принят практический подход, используются образы памяти из реальных инцидентов. Прочтя книгу, вы сможете самостоятельно создавать и анализировать дампы памяти, изучать действия пользователя, искать следы бесфайловых атак и реконструировать действия злоумышленников.

Издание адресовано специалистам по реагированию на инциденты, аналитикам кибербезопасности, системным администраторам, а также может быть полезно студентам вузов и инженерам из смежных областей.

УДК 004.056

ББК 16.8

First published in the English language under the title ‘Practical Memory Forensics – (9781801070331)’

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 (анг.) 978-1-80107-033-1

ISBN (рус.) 978-5-93700-157-3

Copyright ©Packt Publishing 2022

© Оформление, издание, перевод, ДМК Пресс, 2022

Оглавление

Предисловие от издательства	11
Отзывы и пожелания.....	11
Список опечаток.....	11
Нарушение авторских прав	11
Об авторах	12
О рецензентах	13
Предисловие.....	14
Целевая аудитория	14
Структура	14
Как извлечь максимум пользы из этой книги.....	15
Скачайте цветные изображения	16
Условные обозначения	16
Оставайтесь на связи.....	16
Поделитесь своими мыслями	17
ЧАСТЬ I. ОСНОВЫ КРИМИНАЛИСТИКИ ПАМЯТИ.....	19
Глава 1. Зачем нужна криминалистика памяти?	21
Основные преимущества криминалистики памяти	22
Без следов.....	22
Найди меня в памяти	22
Фреймворки	23
Living off the land	24
На страже конфиденциальности	24
Цели и методы исследования	25
Устройство потерпевшего.....	25
Устройство подозреваемого	26
Сложности исследования памяти.....	26
Инструменты	26

Критические системы	26
Нестабильность.....	27
Кратко.....	27
Глава 2. Создание дампов памяти	28
Введение в управление памятью	28
Адресное пространство.....	28
Виртуальная память	29
Разбиение на страницы	29
Разделяемая память	30
Стек и куча	31
Анализ живой памяти	32
Windows	32
Linux и macOS	34
Создание полного и частичного дампа памяти	34
Популярные инструменты и методы создания дампов	36
Виртуально или физически	36
Локально или удаленно.....	37
Как выбрать.....	38
О времени	38
Кратко.....	39
ЧАСТЬ II. КРИМИНАЛИСТИКА ПАМЯТИ В WINDOWS	41
Глава 3. Создание дампа памяти в Windows	43
Трудности создания дампов памяти в Windows.....	44
Подготовка к созданию дампа памяти в Windows.....	44
Создание дампа памяти с помощью FTK Imager.....	45
Создание дампа памяти с помощью WinPmem	48
Создание дампа памяти с помощью Belkasoft Live RAM Capturer	50
Создание дампа памяти с помощью Magnet RAM Capture	53
Кратко.....	54
Глава 4. Реконструкция пользовательской активности.....	55
Технические требования	56
Анализ запущенных приложений	56
Введение в Volatility	56
Идентификация профиля	57
Поиск активных процессов.....	58
Поиск завершившихся процессов	59
Поиск открытых документов.....	62
Документы в памяти процессов	62
Исследование истории браузера	64
Анализ Chrome с помощью плагина yarascan	65
Анализ Firefox с помощью Bulk Extractor	66
Анализ Tor с помощью Strings	69

Исследование коммуникационных приложений.....	70
Почта, почта, почта	71
Мессенджеры	72
Восстановление паролей пользователя	74
Hashdump	74
Cachedump.....	74
Lsadump.....	75
Пароли в открытом виде.....	75
Обнаружение криптоконтейнеров	76
Следы пользовательской активности в реестре	80
Виртуальный реестр	80
Установка MemProcFS.....	81
Работа с реестром Windows	82
Кратко.....	87

Глава 5. Поиск следов вредоносных программ и их анализ 88

Поиск вредоносных процессов	88
Имена процессов	89
Обнаружение аномального поведения	90
Анализ аргументов командной строки.....	94
Аргументы командной строки процессов	95
История команд.....	96
Исследование сетевых соединений.....	99
Процесс-инициатор.....	100
IP-адреса и порты.....	102
Обнаружение внедрения кода в память процесса	104
Внедрение DLL.....	104
Удаленное внедрение DLL	104
Рефлексивное внедрение DLL.....	107
Внедрение переносимых исполняемых файлов	110
Внедрение в пустой процесс.....	113
Процесс-двойник.....	115
Поиск следов закрепления.....	118
Автозапуск при загрузке или входе в систему	118
Создание учетной записи	120
Создание или изменение системных процессов	122
Запланированная задача	124
Построение таймлайна	126
Таймлайн на основе файловой системы.....	126
Таймлайн на основе памяти.....	128
Кратко.....	129

Глава 6. Альтернативные источники

энергозависимых данных 130

Исследование файлов гибернации	130
Получение файла гибернации	131
Анализ файла hiberfil.sys.....	135

Изучение файлов подкачки	138
Получение файлов подкачки	138
Анализ pagefile.sys	140
Поиск по строкам	141
Карвинг файлов	145
Анализ аварийных дампов	149
Создание аварийного дампа	151
Имитация отказа системы	152
Создание дампа процесса	152
Анализ аварийных дампов	155
Аварийные дампы системы	156
Анализ дампа процесса	159
Кратко	162
ЧАСТЬ III. КРИМИНАЛИСТИКА ПАМЯТИ В LINUX.....	163
Глава 7. Создание дампа памяти в Linux.....	165
Трудности создания дампов памяти в Linux	166
Подготовка к созданию дампа памяти в Linux	166
Создание дампа памяти с помощью LiME	168
Создание дампа памяти с помощью AVML	170
Создание профиля Volatility	171
Кратко	174
Глава 8. Реконструкция действий пользователя	176
Технические требования	176
Исследование запущенных программ	177
Анализ истории Bash	180
Поиск открытых документов	181
Восстановление файловой системы	183
Проверка истории браузера	189
Изучение коммуникационных приложений	192
Поиск примонтированных устройств	194
Обнаружение криптоконтейнеров	197
Кратко	198
Глава 9. Обнаружение вредоносной активности	200
Исследование сетевой активности	201
Анализ вредоносной активности	206
Изучение объектов ядра	219
Кратко	222
ЧАСТЬ IV. КРИМИНАЛИСТИКА ПАМЯТИ В MACOS.....	223
Глава 8. Создание дампа памяти в macOS.....	225
Трудности создания дампов памяти в macOS	226
Подготовка к созданию дампа памяти в macOS	226

Создание дампа памяти с помощью osxrmem.....	228
Создание профиля Volatility	232
Кратко.....	235

Глава 11. Обнаружение и анализ вредоносной активности

в macOS..... 236

Особенности анализа macOS с помощью Volatility	237
Технические требования.....	237
Исследование сетевых соединений.....	237
Анализ процессов и их памяти.....	240
Восстановление файловой системы.....	242
Получение данных из пользовательских приложений.....	245
Поиск вредоносной активности	247
Кратко.....	250

Предметный указатель 252