УДК 004.56
ББК 32.973, 018.2
Д44

Диогенес Ю., Озкайя Э.
Д44 Кибербезопасность: стратегии атак и обороны / пер. с анг. Д. А. Беликова. – М.: ДМК Пресс, 2020. – 326 с.: ил.

ISBN 978-5-97060-709-1

Книга посвящена многим аспектам компьютерной безопасности - начиная от стратегии защиты до управления уязвимостями. В ней рассматриваются различные отраслевые стандарты и передовые методы реагирования, процессы взлома данных и политики безопасности, базовые средства контроля безопасности.

Предполагается, что читатели этой книги знакомы с основными понятиями информационной безопасности и операционными системами Windows и Linux.

Издание будет полезно специалистам по информационной безопасности и всем IT-специалистам, которые хотят узнать больше о кибербезопасности.

УДК 004.56
ББК 32.973, 018.2

ISBN 978-1-78847-529-7 (анг.)
ISBN 978-5-97060-709-1 (рус.)

Содержание

Об авторах 11

О рецензентах 12

Предисловие 13

Глава 1. Стратегия безопасности 17

Текущий ландшафт киберугроз 17
Учетные данные – аутентификация и авторизация 20
Приложения 21
Данные 23
Проблемы кибербезопасности 24
Старые методы и более широкие результаты 24
Изменение ландшафта угроз 25
Улучшение стратегии безопасности 26
Красная и Синяя команды 27
Подразумеваем взлом 30
Справочные материалы 31
Резюме 33

Глава 2. Процесс реагирования на компьютерные инциденты 34

Процесс реагирования на компьютерные инциденты 34
Причины иметь в своем распоряжении процесс реагирования на компьютерные инциденты 35
Создание процесса реагирования на компьютерные инциденты 37
Команда реагирования на компьютерные инциденты 39
Жизненный цикл компьютерного инцидента 40
Обработка инцидента 40
Передовые методы оптимизации обработки компьютерных инцидентов 43
Деятельность после инцидента 44
Реальный сценарий 44
Выводы 45
Реагирование на компьютерные инциденты в облаке 46
Обновление процесса реагирования, чтобы включить облако 47
Справочные материалы 48
Резюме 48

Глава 3. Жизненный цикл атаки 50
Внешняя разведка 50
Сканирование 51
Доступ и повышение привилегий 61
Вертикальное повышение привилегий 62
Горизонтальное повышение привилегий 63
Проникновение и утечки 63
Тыловое обеспечение 64
Штурм 65
Обфускация 66
Управление жизненным циклом угроз 67
Справочные материалы 70
Резюме 72

Глава 4. Разведка и сбор данных 73
Внешняя разведка 73
Копание в мусоре 73
Социальные сети 74
Социальная инженерия 75
Внутренняя разведка 82
Анализ трафика и сканирование 83
Вардрайвинг 89
Завершая эту главу 91
Справочные материалы 92
Резюме 93

Глава 5. Компрометация системы 94
Анализ современных тенденций 94
Вымогательство 95
Манипулирование данными 96
Атаки на IoT-устройства 97
Бэкдоры 98
Атаки на мобильные устройства 99
Взлом повседневных устройств 99
Взлом облака 100
Фишинг 102
Эксплуатация уязвимостей 104
Уязвимость нулевого дня 104
Фаззинг 105
Анализ исходного кода 105
Типы эксплойтов нулевого дня 106
Перезапись структурированного обработчика исключений 107

Выполнение шагов, направленных на компрометацию системы 107
Развертывание полезных нагрузок 108
Компрометация операционных систем 111
Компрометация удаленной системы 114
Компрометация веб-приложений 116
Справочные материалы 118
Резюме 120

Глава 6. Охота на пользовательские реквизиты 121

Реквизиты доступа – новый периметр 121
Стратегии компрометации реквизитов доступа пользователя 124
Получение доступа к сети 125
Сбор учетных данных 126
Взлом реквизитов доступа пользователя 128
Полный перебор 128
Социальная инженерия 130
Атака Pass-the-hash 136
Другие способы взлома реквизитов доступа 139
Справочные материалы 139
Резюме 139

Глава 7. Дальнейшее распространение по сети 141

Инфильтрация 142
Построение карты сети 142
Избежать оповещений 143
Дальнейшее распространение 144
Сканирование портов 144
Sysinternals 145
Общие файловые ресурсы 147
Удаленный доступ к рабочему столу 148
PowerShell 150
Инструментарий управления Windows 150
Запланированные задачи 151
Кража авторизационных токенов 153
Атака Pass-the-hash 153
Active Directory 154
Удаленный доступ к реестру 155
Анализ взломанных хостов 155
Консоли центрального администратора 156
Кража сообщений электронной почты 156
Справочные материалы 156
Резюме 157

Глава 8. Повышение привилегий 158
Инфильтрация 158
Горизонтальное повышение привилегий 159
Вертикальное повышение привилегий 159
Как избежать оповещений 160
Выполнение повышения привилегий 161
Эксплуатация неисправленных операционных систем 162
Манипулирование маркерами доступа 163
Эксплуатация специальных возможностей 164
Application Shimming 165
Обход контроля над учетной записью пользователя 169
Внедрение DLL-библиотек 170
Перехват порядка поиска DLL 172
Перехват поиска dylib 172
Исследование уязвимостей 173
Запускаемые демоны 174
Практический пример повышения привилегий в Windows 8 175
Выводы 176
Справочные материалы 177
Резюме 178

Глава 9. Политика безопасности 179
Проверка политики безопасности 179
Обучение конечного пользователя 181
Рекомендации по безопасности для пользователей социальных сетей 182
Тренинг по безопасности 183
Использование политики 183
Белый список приложений 185
Усиление защиты 187
Мониторинг на предмет соответствия 191
Справочные материалы 195
Резюме 195

Глава 10. Сегментация сети 197
Глубоко эшелонированная защита 197
Инфраструктура и службы 198
Документы в процессе передачи 199
Конечные точки 201
Сегментация физической сети 201
Открывая схему сети 203
Обеспечение удаленного доступа к сети 206
VPN типа «сеть–сеть» 207
Сегментация виртуальной сети 208

Безопасность гибридной облачной сети 210
Справочные материалы 212
Резюме 213

Глава 11. Активные сенсоры 214
Возможности обнаружения 214
  Индикаторы компрометации 216
Системы обнаружения вторжений 218
Система предотвращения вторжений 219
  Обнаружение на основе правил 220
  Обнаружение на основе аномалий 221
Поведенческая аналитика внутри организации 221
  Размещение устройств 226
Поведенческая аналитика в гибридном облаке 226
  Центр безопасности Azure 226
Справочные материалы 232
Резюме 232

Глава 12. Киберразведка 233
Введение в киберразведку 233
Инструментальные средства киберразведки с открытым исходным кодом 237
Средства киберразведки компании Microsoft 242
  Центр безопасности Azure 242
Использование киберразведки для расследования подозрительной деятельности 245
Справочные материалы 248
Резюме 248

Глава 13. Расследование инцидента 249
Масштаб проблемы 249
  Ключевые артефакты 250
Исследование скомпрометированной системы внутри организации 255
Исследование скомпрометированной системы в гибридном облаке 259
  Ищите и обрящете 266
Выводы 267
Справочные материалы 268
Резюме 268

Глава 14. Процесс восстановления 269
План послеаварийного восстановления 269
  Процесс планирования послеаварийного восстановления 270
  Вызовы 274

ŋqdqɏǝʎ pɆ dǝdɆbʎɜǝ d ɐɔɑбɔɏ Ɉqddʎqɏǝ̀

Восстановление без перерыва в обслуживании 274
Планирование на случай непредвиденных обстоятельств 276
Процесс планирования на случай непредвиденных обстоятельств в сфере IT 277
Передовые методы восстановления 282
Справочные материалы 283
Резюме 283

Глава 15. Управление уязвимостями 285

Создание стратегии управления уязвимостями 285
Инвентаризация ресурсов 286
Управление информацией 286
Оценка рисков 288
Оценка уязвимостей 290
Отчеты и отслеживание исправлений 291
Планирование реагирования 292
Инструменты управления уязвимостями 293
Реализация управления уязвимостями 300
Передовые методы управления уязвимостями 302
Реализация управления уязвимостями с помощью Nessus 304
Flexera (Secunia) Personal Software Inspecto 310
Заключение 312
Справочные материалы 313
Резюме 314

Глава 16. Анализ журналов 315

Сопоставление данных 315
Журналы операционной системы 316
Журналы Windows 317
Журналы Linux 320
Журналы брандмауэра 320
Журналы веб-сервера 322
Справочные материалы 323
Резюме 323

Предметный указатель 324