

Содержание

| | |
|--|----|
| Об авторе | 17 |
| Благодарности | 18 |
| Предисловие | 19 |
| Введение | 21 |
| 1. Что ты за хакер? | 23 |
| Большинство хакеров отнюдь не гении | 24 |
| Специалисты по ИБ — продвинутые хакеры | 26 |
| Хакеры особенны | 26 |
| Хакеры настойчивы | 27 |
| Шляпных дел мастера | 28 |
| 2. Как хакеры взламывают | 33 |
| Секрет взлома | 35 |
| Методология взлома | 35 |
| Сбор информации | 36 |
| Проникновение | 38 |
| Уязвимости нулевого дня | 39 |
| Непропатченное программное обеспечение | 40 |
| Вредоносные программы | 41 |
| Социальная инженерия | 42 |
| Подбор паролей | 42 |
| Перехват или атака посредника | 43 |
| Утечка данных | 43 |
| Неправильная конфигурация оборудования | 44 |
| Отказ в обслуживании | 44 |
| Участие инсайдеров, партнеров, консультантов, производителей и других третьих лиц | 45 |
| Пользовательский фактор | 45 |
| Физический доступ | 45 |
| Повышение привилегий | 46 |
| Упрощение доступа в будущем | 47 |
| Разведка системы | 47 |

| | |
|--|-----------|
| Перемещение | 47 |
| Выполнение запланированного действия | 48 |
| Заметание следов | 49 |
| Взлом скучно успешен | 50 |
| Автоматизированная вредоносная программа как инструмент взлома | 50 |
| Этика взлома | 51 |
| 3. Профиль: Брюс Шнайер | 53 |
| Информация о Брюсе Шнайере | 58 |
| 4. Социальная инженерия | 59 |
| Методы социальной инженерии | 59 |
| Фишинг | 59 |
| Троянский конь | 60 |
| По телефону | 61 |
| Мошенничество | 61 |
| Личное участие | 62 |
| Кнут или пряник | 63 |
| Защита от социальной инженерии | 63 |
| Обучение | 63 |
| Будьте осторожны при установке ПО со сторонних веб-сайтов | 64 |
| Цифровые сертификаты с расширенной проверкой | 65 |
| Избавьтесь от паролей | 65 |
| Технологии против социальной инженерии | 65 |
| 5. Профиль: Кевин Митник | 67 |
| Информация о Кевине Митнике | 73 |
| 6. Уязвимости программного обеспечения | 75 |
| Количество уязвимостей программного обеспечения | 76 |
| Почему уязвимости ПО — по-прежнему большая проблема? | 77 |
| Защита от уязвимостей программного обеспечения | 78 |
| Жизненный цикл безопасной разработки | 78 |
| Более безопасные языки программирования | 79 |
| Анализ кода и программы | 79 |
| Более безопасные операционные системы | 80 |
| Сторонние средства защиты и надстройки разработчиков | 80 |
| Идеальное программное обеспечение не решит все проблемы | 81 |
| 7. Профиль: Майкл Ховард | 82 |
| Информация о Майкле Ховарде | 88 |
| 8. Профиль: Гари Макгроу | 89 |
| Информация о Гари Макгроу | 93 |

| | |
|---|-----|
| 9. Вредоносные программы | 94 |
| Типы вредоносных программ | 95 |
| Количество вредоносных программ | 96 |
| Программы криминального назначения | 97 |
| Защита от вредоносных программ | 98 |
| Вовремя пропатченное программное обеспечение | 99 |
| Обучение | 99 |
| Антивирусные программы | 99 |
| Программы контроля запуска приложений | 100 |
| Инструменты пограничной защиты | 100 |
| Обнаружение вторжений | 101 |
| 10. Профиль: Сьюзен Брэдли | 102 |
| Информация о Сьюзен Брэдли | 106 |
| 11. Профиль: Марк Руссинович | 107 |
| Информация о Марке Руссиновиче | 112 |
| 12. Криптография | 114 |
| Что такое криптография? | 114 |
| Почему злоумышленники не могут просто подобрать все возможные ключи? | 115 |
| Симметричные и асимметричные ключи | 116 |
| О криптографии популярно | 116 |
| Хэши | 117 |
| Применение криптографии | 118 |
| Криптографические атаки | 119 |
| Математические атаки | 119 |
| Атака на основе доступной информации | 120 |
| Атаки по сторонним каналам | 120 |
| Небезопасные реализации | 120 |
| 13. Профиль: Мартин Хеллман | 122 |
| Информация о Мартине Хеллмане | 128 |
| 14. Обнаружение вторжений/угроз | 129 |
| Характеристики эффективного предупреждения об инциденте | 130 |
| Развитые устойчивые угрозы | 131 |
| Методы обнаружения вторжений | 132 |
| Обнаружение вторжений на основе поведения | 132 |
| Обнаружение вторжений на основе сигнатур | 133 |
| Инструменты и сервисы обнаружения вторжений | 133 |
| Системы обнаружения/предотвращения вторжений | 133 |
| Системы управления событиями | 134 |
| Обнаружение сложных постоянных угроз (APT) | 135 |

| | |
|---|-----|
| 15. Профиль: доктор Дороти Деннинг | 137 |
| Информация о докторе Дороти Деннинг | 142 |
| 16. Профиль: Михаил Дубинский | 143 |
| Информация о Михаиле Дубинском | 147 |
| 17. Брандмауэры | 148 |
| Что такое брандмауэр? | 148 |
| Происхождение брандмауэров | 149 |
| Правила брандмауэра | 151 |
| Размещение брандмауэров | 152 |
| На уровне сети | 152 |
| На узлах компьютеров | 152 |
| Повышенная безопасность | 153 |
| От чего защищают брандмауэры | 154 |
| 18. Профиль: Уильям Чесвик | 155 |
| Информация об Уильяме Чесвике | 160 |
| 19. Ханипоты | 161 |
| Что такое ханипот? | 161 |
| Взаимодействие | 162 |
| Зачем использовать ханипоты? | 163 |
| Как я ловил русского шпиона | 164 |
| Ресурсы для изучения ханипотов | 165 |
| 20. Профиль: Лэнс Спицнер | 167 |
| Информация о Лэнсе Спицнере | 171 |
| 21. Взлом паролей | 172 |
| Компоненты системы аутентификации | 172 |
| Пароли | 173 |
| Базы данных проверки подлинности | 173 |
| Хэши паролей | 173 |
| Вызов-ответ | 174 |
| Факторы аутентификации | 174 |
| Взлом паролей | 175 |
| Подбор пароля | 175 |
| Фишинг | 176 |
| Кейлоггинг (запись нажатия клавиш) | 176 |
| Взлом хэша пароля | 176 |
| Повторное использование учетных данных | 177 |
| Взлом сервиса восстановления пароля | 178 |
| Защита паролей | 178 |
| Сложность и длина | 178 |
| Частые изменения без повторного использования | 178 |

| | |
|---|------------|
| Разные пароли в разных системах | 179 |
| Блокировка аккаунта | 179 |
| Устойчивые хэш-функции | 180 |
| Не используйте пароли | 180 |
| Защита от кражи учетных данных | 181 |
| Защита сервисов восстановления пароля | 181 |
| 22. Профиль: доктор Кормак Херли | 182 |
| Информация о докторе Кормаке Херли | 186 |
| 23. Взлом беспроводной сети | 187 |
| Беспроводной мир | 187 |
| Типы взлома беспроводных сетей | 188 |
| Атака точки доступа | 188 |
| Отказ в обслуживании | 188 |
| Подбор пароля беспроводной сети | 189 |
| Перехват сессии | 189 |
| Кража информации | 189 |
| Обнаружение местонахождения пользователя | 190 |
| Некоторые инструменты для взлома беспроводных сетей | 190 |
| Aircrack-Ng | 190 |
| Kismet | 191 |
| Fern Wi-Fi Hacker | 191 |
| Firesheep | 191 |
| Защита беспроводных сетей от взлома | 191 |
| «Прыгающие частоты» | 191 |
| Предопределенная идентификация клиента | 192 |
| Устойчивые протоколы | 192 |
| Длинные пароли | 193 |
| Установка патчей точек доступа | 193 |
| Электромагнитное экранирование | 193 |
| 24. Профиль: Томас д'Отрепп де Буветт | 194 |
| Информация о Томасе д'Отреппе де Буветте | 197 |
| 25. Тестирование на проникновение | 198 |
| Самые запоминающиеся моменты в моей карьере пентестера | 198 |
| Взлом всех телевизионных приставок в стране | 198 |
| Одновременный взлом крупной телевизионной сети и кража порнографии | 199 |
| Взлом сайта крупной платежной системы | 200 |
| Создание «Камерного вируса» | 200 |

10 Как противостоять хакерским атакам

| | |
|--|------------|
| Как стать пентестером | 201 |
| Методология хакера | 201 |
| Получение официального разрешения | 202 |
| Оформление контракта | 202 |
| Отчеты | 203 |
| Сертификация | 203 |
| Институт SANS | 203 |
| Сертификат нравственности хакера (СЕН) | 205 |
| CompTIA Security+ | 205 |
| ISACA | 206 |
| Сертификаты производителей | 206 |
| Соблюдайте этику | 209 |
| Минимизация возможных сбоев в работе | 209 |
| 26. Профиль: Аарон Хигби | 210 |
| Информация об Аароне Хигби | 214 |
| 27. Профиль: Бенилд Джозеф | 215 |
| Информация о Бенилде Джозефе | 217 |
| 28. DDoS-атаки | 219 |
| Типы DDoS-атак | 219 |
| Отказ в обслуживании | 219 |
| Прямые атаки | 220 |
| Reflection-атаки | 220 |
| Усиление | 221 |
| Применение на каждом уровне модели OSI | 221 |
| Усиливающиеся атаки | 222 |
| Атаки на исходящий и входящий каналы | 222 |
| Инструменты и сервисы для совершения DDoS-атак | 223 |
| Инструменты | 223 |
| DDoS-сервисы | 223 |
| Защита от DDoS-атак | 224 |
| Обучение | 224 |
| Стресс-тестирование | 224 |
| Соответствующая настройка сети | 224 |
| Исследование потенциально слабых мест | 225 |
| Анти-DDoS сервисы | 225 |
| 29. Профиль: Брайан Кребс | 227 |
| Информация о Брайане Кребсе | 231 |

| | |
|--|-----|
| 30. Безопасность операционной системы | 232 |
| Как защитить операционную систему | 233 |
| Создание безопасной операционной системы | 233 |
| Общие критерии | 233 |
| Федеральные стандарты обработки информации | 235 |
| История о двух безопасных операционных системах | 235 |
| Рекомендации по обеспечению безопасности | 237 |
| Средства конфигурации параметров безопасности | 237 |
| Консорциумы по вопросам обеспечения безопасности | 238 |
| Trusted Computing Group | 238 |
| Альянс FIDO | 239 |
| 31. Профиль: Йоанна Рутковская | 240 |
| Информация о Йоанне Рутковской | 243 |
| 32. Профиль: Аарон Маргосис | 244 |
| Информация об Аароне Маргосисе | 249 |
| 33. Сетевые атаки | 251 |
| Типы сетевых атак | 251 |
| Прослушка | 252 |
| Атаки «через посредника» | 252 |
| DDoS-атаки | 253 |
| Защита от сетевых атак | 253 |
| Изоляция домена | 253 |
| Виртуальные частные сети | 254 |
| Использование защищенных протоколов и приложений | 254 |
| Системы обнаружения вторжений | 254 |
| Защита от DDoS-атак | 255 |
| Посещайте безопасные веб-сайты и используйте защищенные сервисы | 255 |
| 34. Профиль: Лаура Чаппелл | 257 |
| Информация о Лауре Чаппелл | 261 |
| 35. Взлом IoT | 262 |
| Как хакеры взламывают IoT? | 262 |
| Защита IoT-устройств | 264 |
| 36. Профиль: доктор Чарли Миллер | 266 |
| Информация о Чарли Миллере | 274 |
| 37. Политики и стратегия | 275 |
| Стандарты | 276 |
| Политики | 277 |

| | |
|---|------------|
| Процедуры | 277 |
| Фреймворки | 277 |
| Нормативные законы | 278 |
| Глобальные проблемы | 278 |
| Поддержка систем | 279 |
| 38. Профиль: Цзин де Йонг-Чен | 280 |
| Информация о Цзин де Йонг-Чен | 286 |
| 39. Моделирование угроз | 288 |
| Зачем нужно моделирование угроз? | 288 |
| Виды моделирования угроз | 289 |
| Злоумышленники | 290 |
| Государства | 291 |
| Промышленный шпионаж | 291 |
| Финансовая преступность | 291 |
| Хактивисты (хакеры-активисты) | 292 |
| Геймеры | 292 |
| Инсайдеры | 292 |
| Обычные хакеры-одиночки или хакерские группы | 293 |
| 40. Профиль: Адам Шостаки | 294 |
| Информация об Адаме Шостаки | 299 |
| 41. Обучение информационной безопасности | 300 |
| Темы обучения в сфере ИБ | 301 |
| Осведомленность в вопросах безопасности конечных пользователей (Security Awareness) | 301 |
| Общие вопросы информационной безопасности | 302 |
| Реагирование на инциденты | 302 |
| Тренинги, специфичные для операционных систем и приложений | 302 |
| Технические навыки | 303 |
| Сертификация | 303 |
| Методы обучения | 304 |
| Онлайн-обучение | 304 |
| Взлом сайтов | 304 |
| Учебные заведения | 304 |
| Тренировочные лагеря | 305 |
| Корпоративное обучение | 305 |
| Книги | 305 |
| 42. Профиль: Стивен Норткат | 307 |
| Информация о Стивене Норткате | 311 |

| | |
|--|-----|
| 43. Конфиденциальность | 312 |
| Организации, курирующие вопросы конфиденциальности | 314 |
| Приложения с обеспечением конфиденциальности | 315 |
| 44. Профиль: Ева Гальперин | 317 |
| Информация о Еве Гальперин | 320 |
| 45. Установка патчей | 321 |
| Зачем устанавливать патчи | 322 |
| Большинство эксплойтов вызваны старыми уязвимостями, для которых выпущены патчи | 322 |
| Большинство эксплойтов вызваны всего несколькими непропатченными программами | 323 |
| Самая непропатченная программа не всегда самая опасная | 324 |
| Вам также нужно патчить аппаратное обеспечение | 324 |
| Основные проблемы, связанные с патчами | 325 |
| Не обнаруживаются отсутствующие патчи | 325 |
| Вы не всегда можете применить патчи | 325 |
| Некоторые патчи не устанавливаются | 326 |
| Патчи могут приводить к проблемам эксплуатации | 326 |
| Патч — оповещение об эксплойте на весь мир | 327 |
| 46. Профиль: Уиндоу Снайдер | 329 |
| Информация об Уиндоу Снайдер | 333 |
| 47. Карьера писателя | 334 |
| Куда можно писать об информационной безопасности | 335 |
| Блоги | 335 |
| Социальные сети | 336 |
| Статьи | 336 |
| Книги | 337 |
| Самиздат или издатель? | 338 |
| Техническая редакция | 340 |
| Новостные рассылки | 340 |
| Подробные отчеты | 341 |
| Технические обзоры | 341 |
| Конференции | 341 |
| Советы профессионального писателя | 342 |
| Самое сложное — начать | 342 |
| Читайте иначе | 343 |
| Начинайте безвозмездно | 343 |
| Будьте профи | 343 |
| Продвигайте себя | 344 |
| Лучше один раз увидеть, чем сто раз услышать | 344 |

| | |
|---|-----|
| 48. Профиль: Фахмида Я. Рашид | 346 |
| Информация о Фахмиде Я. Рашиде | 351 |
| 49. Руководство для родителей юных хакеров | 352 |
| Как определить, что ваш ребенок — хакер | 353 |
| Он рассказывает о том, что ломает | 354 |
| Чрезмерная секретность в Интернете | 354 |
| Тайные аккаунты в соцсетях или адреса электронной почты | 354 |
| Вы нашли хакерские инструменты на его компьютере | 355 |
| Люди жалуются на взломы | 355 |
| Ребенок выключает экран, когда вы входите в комнату | 355 |
| Эти признаки могут быть нормальными | 355 |
| Не все взломы плохие | 356 |
| Как наставить злонамеренного хакера на праведный путь | 356 |
| Переместите компьютер ребенка под ваш контроль | 357 |
| Научите этике | 357 |
| Обговорите юридические моменты хакинга | 358 |
| Веб-сайты для хакинга | 358 |
| Программы Bug Bounty | 358 |
| Взлом оборудования | 359 |
| Клубы робототехники | 359 |
| Конкурсы Capture the Flag | 360 |
| Обучение и сертификация | 360 |
| Поиск хорошего наставника | 361 |
| 50. Кодекс чести хакера | 362 |
| Кодекс чести хакера | 364 |
| Будьте этичным, прозрачным и честным | 364 |
| Не нарушайте закон | 364 |
| Получите разрешение | 365 |
| Будьте конфиденциальны с защищенной информацией | 365 |
| Не причиняйте вреда | 365 |
| Ведите себя профессионально | 366 |
| Станьте примером для других | 366 |

Введение

Цель этой книги — раскрыть мир специалистов по информационной безопасности (ИБ), некоторых из лучших хакеров, защитников конфиденциальных данных, преподавателей и писателей. Я надеюсь, что вы прочитаете ее с большим удовольствием от осознания усилий, которые потребовались, чтобы реализовать фантастический мир компьютеров, в котором мы живем сегодня. Без добрых людей на светлой стороне, воюющих против злоумышленников, компьютеры, Интернет и все, что с ними связано, были бы невозможны. Эта книга — ода специалистам по ИБ.

Я хочу призвать всех, кто собирается сделать карьеру в области информационных технологий, подумать о карьере в сфере информационной безопасности. Я также хочу призвать всех начинающих хакеров, особенно тех, кто переживает насчет этичности применения своих знаний, сделать карьеру в этой области. Я противостоял вредоносным хакерам и их творениям. Я смог исследовать каждый интерес в области хакинга, который у меня был, этичным и законопослушным способом. И десятки тысяч других. Информационная безопасность — одна из самых востребованных и высокооплачиваемых отраслей в любой стране. Это стало моим призванием и может стать вашим.

Книга разделена на главы, в которых кратко описывается реализация определенного способа атаки, а затем приводится один или два профиля специалистов по ИБ, преуспевших в этой области. Я попытался выбрать лучших из множества легенд, светил и даже некоторых относительно скромных специалистов, которые достигли блестящих успехов, даже

если они не очень известны обывателям. Я попытался сформировать сочетание опыта ученых, разработчиков, преподавателей, лидеров, писателей и частных практиков, живущих в Соединенных Штатах и во всем мире. Я надеюсь, что читатели, заинтересованные в карьере специалиста ИБ, смогут так же мотивировать себя, как и я, чтобы сделать сферу ИТ значительно безопаснее для всех нас.

Да пребудет с вами сила!

1

Что ты за хакер?

Много лет назад я переехал в дом с прекрасным гаражом. В нем было очень удобно парковаться и даже хранить лодку и небольшой фургон. Сооружение было построено из отличных прочных досок. Электрику провели профессионалы, а качественные окна выдерживали порывы ветра скоростью 70 метров в секунду. Большую часть интерьера создал профессиональный плотник из ароматного красного кедра. Я неспособен и гвоздь забить, не то что собрать мебель, но даже мне было понятно, что он знает свое дело, думает о качестве и уделяет внимание деталям.

Через несколько недель после новоселья пришел чиновник и сказал, что гараж, построенный много лет назад, не имеет нужных документов, и придется снести незаконную постройку, иначе мне грозят крупные штрафы за каждый день просрочки исполнения постановления. Я позвонил в ведомство, чтобы утрясти вопрос, ведь гараж возвели задолго до моего переезда, и продавался он как часть недвижимости. Безрезультатно. Его нужно было немедленно снести. Штрафные санкции за один день превышали сумму, которую я мог выручить за отделку, если бы аккуратно ее снял. Проще говоря, в целях экономии, чем быстрее я демонтирую гараж, тем лучше.

Я достал кувалду и за несколько часов превратил сооружение в груды деревянных обломков и прочего мусора. В процессе я думал о том, что строителю, вероятно,

потребовались недели, если не месяцы, чтобы возвести гараж, а я уничтожил его творение своими варварскими руками гораздо быстрее.

Вопреки распространенному мнению, злонамеренный взлом — это скорее кувалда стропальщика, чем тонкий инструмент ремесленника.

Если вы уверены, что сможете стать хакером, вам придется решить, будете вы стремиться к защите общего блага или довольствоваться низменными целями. Вы хотите быть скрывающимся, преступным хакером или праведным, опытным специалистом по ИБ? Эта книга — доказательство, что лучшие хакеры работают во благо. Они практикуются, развиваются интеллектуально, и им не нужно скрываться от правоохранительных органов. Они могут работать в центре сферы информационной безопасности, приводить в восхищение коллег и получать хорошие деньги. Эта книга о порой невоспетых героях, которые делают нашу невероятную цифровую жизнь возможной.

Примечание. Хотя термины «хакер» или «взлом» могут означать человека или деятельность как с хорошими, так и с плохими намерениями, в основном их используют в негативном ключе. Я понимаю, что хакеры могут быть разными, но во имя экономии бумаги впредь буду использовать эти слова без оговорок, подразумевая либо отрицательный, либо положительный их оттенок. Вникайте в смысл текста, чтобы понимать намерения, в связи с которыми упоминаются термины.

Большинство хакеров отнюдь не гении

К сожалению, почти каждый, кто пишет о «злых» хакерах, не имея реального опыта, романтизирует их как умные,

богоподобные, мифические фигуры. Они могут подобрать любой пароль менее чем за минуту (особенно под прицелом пистолета, если верить Голливуду), взломать любую систему и секретный шифр. Они работают в основном по ночам и пьют много энергетических напитков, а их рабочее место завалено упаковками от чипсов и фастфуда. Школьник крадет пароль учителя, чтобы изменить свои оценки, и СМИ подлизываются к нему, как к потенциальному Биллу Гейтсу или Марку Цукербергу.

Хакеры необязательно гениальны. Я — живое тому доказательство. Несмотря на то, что я вламывался в системы всех компаний, в которых меня когда-либо нанимали для проверки систем защиты, я никогда полностью не понимал квантовую физику или теорию относительности Эйнштейна. Я дважды провалил экзамен по родному языку в средней школе, никогда не получал оценки выше тройки с плюсом по математике, а мой средний балл в первом семестре колледжа составил 0,62. Я получил пять двоек и одну пятерку. Одинокая пятерка была по курсу безопасности на водах, потому что я на тот момент пять лет работал пляжным спасателем. Плохие оценки были не только следствием того, что я не учился. Я просто не был достаточно умен и не пытался с этим справиться. Позже я узнал, что учеба и усердная работа часто более ценны, чем врожденный высокий уровень интеллекта. Я окончил университет и преуспел в мире информационной безопасности.

Тем не менее, даже когда писатели не называют «злых» хакеров сверхумными, читатели частенько предполагают, что они именно таковы, потому что, похоже, практикуют какую-то передовую черную магию, о которой остальной мир не подозревает. Коллективный всемирный разум считает, что «злой хакер» и «суперинтеллект» должны идти рука об руку. Это неправда. Некоторые из них умные,