НИКИТА СКАБЦОВ

KALI LINUX

В ДЕЙСТВИИ

АУДИТ БЕЗОПАСНОСТИ
ИНФОРМАЦИОННЫХ СИСТЕМ

2
ИЗДАНИЕ

ПИТЕР®
Санкт-Петербург • Москва • Мі
2025

Оглавление

Что нового во втором издании 6
Благодарности 6
Отзывы и предложения 7
От издательства 7
Список использованных сокращений 7

Глава 01. Общие сведения об аудите информационных систем 9
Вопросы этики 10
Разрешение на взлом 13

Глава 02. Методология 18
Стандарт оценки безопасности информационной системы 18
Руководство по методике тестирования безопасности с открытым исходным кодом 23
Другие методики 27

Глава 03. Сбор открытой информации о цели 28
Что искать? 29
OSINT 30
Пассивный сбор данных 32
Скрытый интернет 98

Глава 04. Активный сбор данных 110
Определение активных хостов 110
Сканирование портов 113
Получение информации от DNS-серверов 128
Получение данных с использованием SMB 138
Поиск NFS 144
Работа с электронной почтой 147
Получение информации от NTP-сервера 149
Получение информации с использованием SNMP 150

Глава 05. Отчеты 154
Проблема перегруженности информацией 155
Работа с данными, визуализация 156
Написание отчета 172

Глава 06. Поиск уязвимостей ... 184
Принцип работы сканеров уязвимостей ... 184
Автоматическое и ручное сканирование ... 185
Сканирование из внутренней и внешней сети ... 186
Аутентифинициированное и неаутентифицированное сканирование ... 187
OpenVAS ... 187
Nessus ... 197

Глава 07. Атаки на веб-приложения ... 206
Знакомство с cookie ... 207
REST API ... 208
HTTP-методы ... 208
OWASP ... 209
Инструменты OWASP ... 209
Нарушение контроля доступа ... 212
Дефекты в криптографии ... 216
Инъекции ... 219
Небезопасный дизайн ... 227
Небезопасная конфигурация ... 228
Уязвимые и устаревшие компоненты ... 229
Сбой идентификации и аутентификации ... 230
Ошибки проверки целостности ПО и данных ... 237
Ошибки мониторинга и ведения журналов безопасности ... 239
Подделка запросов на стороне сервера ... 240

Глава 08. Социальная инженерия ... 241
Этические аспекты социальной инженерии ... 241
Психологические концепции в социальной инженерии ... 243
На кого обратить внимание? ... 244
Типы атак ... 245
Фазы атаки ... 249
Social-Engineer Toolkit ... 250

Глава 09. Взлом паролей ... 257
Основные методы ... 257
Работа со списками паролей ... 258
Атаки на сервисы ... 261
Офлайн-атаки ... 265

Глава 10. Перехват информации ... 271
Пассивный перехват трафика ... 272
Активный перехват трафика ... 281

Глава 11. Передача файлов ... 286
TFTP ... 286
FTP ... 287
Передача файлов в Windows ... 290

Глава 12. Закрепление в системе ... 292
Netcat ... 292
NC и обратный шелл ... 293
Перенаправление портов и туннелирование ... 294
Перенаправление портов ... 294
SSH-туннелирование ... 296
Plink ... 299

Глава 13. Сокрытие следов ... 301
Манипуляция лог-файлами ... 301
Сокрытие файлов ... 304

Глава 14. Metasploit Fremework ... 307
Основные компоненты ... 307
Основные команды ... 323
Практические примеры ... 325

Глава 15. Переполнение буфера ... 331
Что такое переполнение буфера? ... 332
Программы, библиотеки и бинарные файлы ... 333
Угрозы ... 334
Основы компьютерной архитектуры ... 335
Организация памяти ... 335
Разбиение стека (Smashing the stack) ... 337
Перезапись указателя фрейма ... 344
Атака возврата в библиотеку ... 346
Переполнение динамической области памяти ... 347
Пример нахождения и эксплуатации уязвимости переполнения буфера ... 348

Глава 16. Сохранение анонимности ... 360
Анонимность при проведении тестов ... 360
Анономность в Глобальной сети ... 361
Как сохранить анонимность? ... 362

Глава 17. Тесты на проникновение: обобщение ... 374
Стандарт выполнения тестов на проникновение ... 375
Зачистка ... 382

В заключение. Обращение к читателю ... 383