

Оглавление

Об авторах	14
О научном редакторе	16
Предисловие	17
Благодарности	19
Введение	21
Для кого эта книга	21
Чего в этой книге нет	22
Почему Go	23
Чем может не понравиться Go	24
Краткий обзор	24
От издательства	28
Глава 1. Go. Основы	29
Настройка среды	29
Скачивание и установка Go	29
Настройка GOROOT для определения расположения двоичного файла	30
Настройка GOPATH для определения местоположения рабочего пространства	30
Выбор интегрированной среды разработки	31
Использование стандартных команд Go tool	34
Синтаксис Go	39
Типы данных	39
Управляющие конструкции	43
Многопоточность	45

Обработка ошибок	47
Обработка структурированных данных	48
Резюме	50
Глава 2. TCP, сканеры и прокси	51
TCP Handshaking	52
Обход брандмауэра с помощью переадресации портов	53
Написание TCP-сканера	54
Тестирование портов на доступность	54
Выполнение однопоточного сканирования	55
Параллельное сканирование	56
Создание TCP-прокси	63
Использование io.Reader и io.Writer	63
Создание эхо-сервера	66
Создание буферизованного слушателя для улучшения кода	69
Проксирование TCP-клиента	70
Воспроизведение функции Netcat для выполнения команд	72
Резюме	76
Глава 3. HTTP-клиенты и инструменты удаленного доступа	77
Основы HTTP с Go	77
Вызов HTTP API	78
Создание запроса	80
Парсинг структурированного ответа	81
Создание HTTP-клиента для взаимодействия с Shodan	83
Шаги построения API клиента	84
Проектирование структуры	85
Приводим в порядок вызовы API	85
Запрос информации о подписке Shodan	86
Создание клиента	90
Взаимодействие с Metasploit	91
Настройка рабочей среды	92
Определение задачи	94
Извлечение действительного токена	95

Определение методов запроса и ответа	96
Создание структуры конфигурации и метода RPC	97
Выполнение удаленных вызовов	98
Создание работающей программы	100
Скрапинг Bing и парсинг метаданных документов	102
Настройка среды и планирование	102
Определение пакета метаданных	104
Отображение данных в структуры	106
Поиск и получение файлов через Bing	107
Резюме	111
Глава 4. HTTP-серверы, маршрутизация и промежуточное ПО	112
Основы HTTP-серверов	112
Создание простого сервера	113
Создание простого маршрутизатора	114
Создание простого промежуточного ПО	115
Маршрутизация с помощью пакета gorilla/mux	117
Создание промежуточного ПО с помощью Negroni	119
Добавление аутентификации с помощью Negroni	122
Создание HTML-ответов с помощью шаблонов	124
Сбор учетных данных	126
Кейлогинг с помощью WebSocket API	130
Мультиплексирование C2-соединений	136
Резюме	140
Глава 5. Эксплуатация DNS	141
Написание DNS-клиентов	141
Извлечение A-записей	142
Обработка ответов от структуры Msg	143
Перечисление поддоменов	145
Написание DNS-серверов	156
Настройка лаборатории и знакомство с сервером	156
Создание DNS-сервера и прокси	160
Резюме	170

Глава 6. Взаимодействие с SMB и NTLM	171
Пакет SMB	172
Что такое SMB	172
Токены безопасности SMB	173
Настройка сессии SMB	174
Смешанное кодирование полей структуры	175
Метаданные и ссылочные поля	179
Реализация SMB	179
Подбор паролей с помощью SMB	187
Повторное воспроизведение паролей с помощью техники pass-the-hash	188
Восстановление NTLM-паролей	191
Вычисление хеша	191
Восстановление хеша NTLM	192
Резюме	193
Глава 7. Взлом баз данных и файловых систем	194
Настройка баз данных с помощью Docker	195
Установка и заполнение MongoDB	195
Установка и заполнение баз данных PostgreSQL и MySQL	197
Установка и заполнение баз данных Microsoft SQL Server	198
Подключение к базам данных и запрос информации с помощью Go	199
Запрос данных из MongoDB	200
Обращение к базам данных SQL	201
Создание майнера данных	203
Реализация майнера данных из MongoDB	205
Реализация майнера для MySQL	208
Кража данных из файловых систем	211
Резюме	213
Глава 8. Обработка сырых пакетов	214
Настройка среды	214
Идентификация устройств с помощью субпакета rscap	215
Онлайн-перехват и фильтрация результатов	216

Сниффинг и отображение учетных данных пользователя в открытом виде	219
Сканирование портов через защиту от SYN-флуда	222
Проверка TCP-флагов	222
Создание фильтра BPF	223
Написание сканера портов	224
Резюме	227
Глава 9. Написание и портирование эксплойтов	228
Создание фаззера	228
Фаззинг для переполнения буфера	229
Фаззинг SQL-инъекций	233
Портирование эксплойтов в Go	238
Портирование эксплойта из Python	240
Портирование эксплойта из C	244
Создание шелл-кода в Go	256
Преобразование в C	256
Преобразование в Hex	257
Преобразование в Num	258
Преобразование в Raw	258
Кодировка Base64	259
Примечание по ассемблеру	260
Резюме	260
Глава 10. Плагины и расширяемые инструменты Go	261
Использование собственной системы плагинов Go	262
Создание основной программы	263
Создание плагина для подбора паролей	266
Запуск сканера	269
Создание плагинов в Lua	269
Создание HTTP-функции head()	271
Создание функции get()	272
Регистрация функций с помощью VM Lua	274
Написание функции main()	275

Создание скрипта плагина	276
Тестирование плагина Lua	277
Резюме	278
Глава 11. Реализация криптографии и криптографические атаки	279
Обзор базовых принципов криптографии	280
Криптография в стандартной библиотеке Go	281
Знакомство с хешированием	282
Взлом хеша MD5 или SHA-256	282
Реализация bcrypt	284
Аутентификация сообщений	286
Шифрование данных	289
Шифрование с симметричным ключом	289
Асимметричная криптография	293
Брутфорс RC2	301
Подготовка	301
Работа производителя	304
Выполнение работы и расшифровка данных	306
Написание функции Main	308
Выполнение программы	310
Резюме	311
Глава 12. Взаимодействие с системой Windows и ее анализ	312
Windows API-функция OpenProcess()	312
Типы unsafe.Pointer и uintptr	315
Внедрение в процесс с помощью пакета syscall	318
Определение Windows DLL и присваивание переменных	320
Получение токена процесса с помощью OpenProcess Windows API ...	321
Управление памятью с помощью VirtualAllocEx Windows API	324
Запись в память с помощью WriteProcessMemory Windows API	325
Поиск LoadLibraryA с помощью GetProcessAddress Windows API	326
Выполнение вредоносной DLL с помощью CreateRemoteThread Windows API	326
Проверка внедрения с помощью WaitForSingleObject Windows API	327

Очистка с помощью VirtualFreeEx Windows API	328
Дополнительные упражнения	329
Формат файлов Portable Executable	330
Особенности формата файлов PE	330
Написание PE-парсера	331
Дополнительные упражнения	342
Использование Си с Go	342
Установка набора инструментов С для Windows	343
Создание окна сообщений с помощью С и Windows API	343
Встраивание Go в С	344
Резюме	346
Глава 13. Скрытие данных с помощью стеганографии	348
Знакомство с форматом PNG	348
Заголовок	349
Последовательность блоков	350
Считывание байтов данных изображения	351
Считывание заголовка	351
Считывание последовательности блоков	352
Запись байтовых данных изображения для внедрения полезной нагрузки	355
Обнаружение смещения блока	355
Запись байтов с помощью метода ProcessImage()	356
Кодирование и декодирование байтов изображения с помощью XOR	361
Резюме	367
Дополнительные упражнения	367
Глава 14. Создание C2-трояна удаленного доступа	368
Подготовка	369
Установка Protocol Buffers для определения gRPC API	369
Определение и создание gRPC API	370
Создание сервера	372
Реализация интерфейса протокола	372
Написание функции main()	375

Создание клиентского импланта	377
Создание компонента Admin	379
Выполнение RAT	380
Доработка RAT	380
Зашифруйте коммункации	380
Обработка сетевых сбоев	381
Регистрация имплантов	381
Добавление базы данных	382
Поддержка нескольких имплантов	382
Расширение функциональности имплантов	382
Цепочка команд операционной системы	383
Повысьте доверие к импланту и примените нужный комплекс OPSEC ...	383
Добавление ASCII-графики	383
Резюме	384