

Раскрыты секреты элитного программирования

В своей новой книге Джеймс Фостер, автор ряда бестселлеров, впервые описывает методы, которыми пользуются хакеры для атак на операционные системы и прикладные программы. Он приводит примеры работающего кода на языках C/C++, Java, Perl и NASL, в которых иллюстрируются методы обнаружения и защиты от наиболее опасных атак. В книге подробно изложены вопросы, разбираясь в которых наспех неизвестно любому программисту, работающему в сфере информационной безопасности: программирование сокетов, shell-коды, переносимые приложения и принципы написания экспloitов.

«Прочтите эту книгу, поймите ее суть и используйте для своей пользы!» – Стюарт Макклор

Прочитав эту книгу, Вы научитесь:

- 1 Самостоятельно разрабатывать shell-код.
- 2 Переносить опубликованные экспloitы на другую платформу.
- 3 Модифицировать под свои нужды COM-объекты в Windows.
- 4 Усовершенствовать Web-сканер Nikto.
- 5 Разобраться в эксплойте «судного дня».
- 6 Писать сценарии на языке NASL.
- 7 Выявлять и атаковать уязвимости.
- 8 Программировать на уровне сокетов.

СОДЕРЖАНИЕ ДАННОЙ КНИГИ:

- Написание безопасных программ
- Язык сценариев NASL
- BSD-сокеты
- Сокеты на платформе Windows (Winsock)
- Советы по языку Java
- Написание переносимых программ
- Написание переносимых сетевых программ
- Написание shell-кода (I и II)
- Написание экспloitов (I, II и III)
- Написание компонентов для задач, связанных с безопасностью
- Создание инструмента для проверки уязвимости Web-приложения
- Глоссарий
- Полезные программы для обеспечения безопасности
- Архивы экспloitов
- Краткий справочник по системным вызовам
- Справочник по преобразованию данных

ЗАЩИТА ОТ ВЗЛОМА: СОКЕТЫ, ЭКСПЛОЙТЫ, SHELL-КОД

ЗАЩИТА ОТ ВЗЛОМА: Сокеты, Shell-код, Экспloitы

ВЫЯВЛЕНИЕ УЯЗВИМОСТЕЙ К АТАКАМ ХАКЕРОВ ОПЕРАЦИОННЫХ СИСТЕМ И ПРИКЛАДНЫХ ПРОГРАММ

Раскрытие секретов элитного программирования:

- самостоятельная разработка shell-кода на языках C++, Java, Perl и Nasl
- принципы написания и перенос экспloitов на платформы Windows, Linux, UNIX и MAC OS
- программирование на уровне сокетов

Джеймс С. Фостер
при участии Майка Прайса

ПРЕДИСЛОВИЕ
СТЮАРТА МАККЛЮРА
ВЕДУЩЕГО АВТОРА «HACKING EXPOSED»

Защита от взлома: сокеты, эксплойты, shell-код

ТРУДНОСТИ КОНСТРУИРОВАНИЯ ЭКСПЛОЙТОВ
И ИНСТРУМЕНТА КОДИРОВАНИЯ
ДЛЯ ПРОФЕССИОНАЛЬНОЙ ЗАЩИТЫ

Серия «Информационная безопасность»



ПРЕДИСЛОВИЕ
СТЮАРТА МАККЛЮРА
ВЕДУЩИЙ АВТОР «HACKING EXPLODED»

Джеймс С. Фостер
при участии Майка Прайса

УДК 004.2

ББК 32.973.26-018.2

Ф81

Ф81 Джеймс Фостер, при участии Майка Прайса

Защита от взлома: сокеты, эксплойты, shell-код: Пер. с англ. Слинкина А. А.
– М.: Издательский Дом ДМК-пресс. – 784 с.: ил.

ISBN 5-9706-0019-9

В своей новой книге Джеймс Фостер, автор ряда бестселлеров, впервые описывает методы, которыми пользуются хакеры для атак на операционные системы и прикладные программы. Он приводит примеры работающего кода на языках C/C++, Java, Perl и NASL, в которых иллюстрируются методы обнаружения и защиты от наиболее опасных атак. В книге подробно изложены вопросы, разбираясь в которых науочно необходимо любому программисту, работающему в сфере информационной безопасности: программирование сокетов, shell-коды, переносимые приложения и принципы написания эксплойтов

УДК 004.2

ББК 32.973.26-018.2

Original English language edition published by Syngress Publishing, Inc. Copyright © 2005 by Syngress Publishing, Inc. All rights reserved.

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.

Материал, изложенный в данной книге, многократно проверен. Но поскольку вероятность технических ошибок все равно существует, издательство не может гарантировать абсолютную точность и правильность приводимых сведений. В связи с этим издательство не несет ответственности за возможные ошибки, связанные с использованием книги.

ISBN 1-597490-05-9 (англ.) Copyright © by Syngress Publishing, Inc.

ISBN 5-9706-0019-9 © Перевод на русский язык, оформление, издание,
Издательский Дом ДМК-пресс

Содержание

Благодарности	23
Об авторе	24
Об основном соавторе	25
Прочие соавторы, редакторы и авторы кода	26
Об авторе предисловия	28
Предисловие	29
Наступит ли «судный день»?	29
Глава 1. Написание безопасных программ	31
Введение	32
C/C++	33
Характеристики языка	34
Язык С	34
Язык C++	35
Безопасность	35
Пример «Здравствуй, мир!»	36
Типы данных	37
Поток управления	40
Функции	41
Классы (только C++)	42
Пример: ряды Фурье	44
Язык Java	48
Характеристики языка	49
Объектно-ориентированные возможности	49
Платформенная независимость	49
Многопоточность	49
Безопасность	50
Дополнительные возможности	50
Пример «Здравствуй, мир!»	50
Типы данных	51
Поток управления	52
Методы	54

6 Защита от взлома: сокеты, эксплойты и shell-код

Классы	54
Получение заголовков HTTP	57
Язык C#	59
Основания для перехода на C#	59
Характеристики языка	60
Объектно-ориентированные возможности	60
Прочие возможности	61
Безопасность	61
Пример «Здравствуй, мир!» на языке C#	62
Типы данных	62
Поток управления	64
Методы	66
Классы	66
Потоки в языке C#	69
Пример: разбор IP-адреса, заданного в командной строке	70
Язык Perl	79
Типы данных	80
Операторы	82
Пример Perl-сценария	84
Анализ	85
Специальные переменные	86
Сопоставление с образцом и подстановка	87
Модификаторы регулярных выражений	88
Канонические инструменты, написанные на Perl	88
Я умею писать на Perl!	89
Каноническая атака на Web-сервер	89
Анализ	90
Утилита модификации файла протокола	90
Результат выполнения	93
Анализ	94
Язык Python	96
Пакет InlineEgg	96
Анализ	98
Анализ	99
Резюме	101
Обзор изложенного материала	103
Ссылки на сайты	104
Часто задаваемые вопросы	105

Глава 2. Язык сценариев NASL	107
Введение	108
История	108
Назначение NASL	109
Простота и удобство	109
Модульность и эффективность	109
Безопасность	110
Ограничения NASL.....	110
Синтаксис языка NASL.....	110
Комментарии	110
Пример правильного комментария	110
Примеры неправильных комментариев	111
Переменные	111
Целые числа	111
Строки.....	111
Массивы	111
NULL	113
Булевские величины	113
Операторы	113
Операторы вне категории	113
Операторы сравнения	114
Арифметические операторы	114
Операторы работы со строками	115
Логические операторы	115
Побитовые операторы	116
Операторы составного присваивания в стиле С	116
Управляющие конструкции.....	117
Инструкции if	117
Циклы for	117
Циклы foreach	118
Циклы while	118
Циклы repeat-until	118
Инструкция break	118
Пользовательские функции	119
Встроенные функции.....	120
Инструкция return	120
Написание сценариев на языке NASL	120
Написание сценариев для личного пользования	121
Сетевые функции	121
Функции, связанные с протоколом HTTP	121

8 Защита от взлома: сокеты, эксплойты и shell-код

Функции манипулирования пакетами	121
Функции манипулирования строками	122
Криптографические функции	122
Интерпретатор команд NASL	122
Пример	122
Программирование в среде Nessus	124
Описательные функции	124
Функции, относящиеся к базе знаний	124
Функции извещения о результатах работы	125
Пример	125
Пример: канонический сценарий на языке NASL	127
Перенос на язык NASL и наоборот	131
Логический анализ	131
Логическая структура программы	131
Псевдокод	132
Перенос на NASL	133
Перенос на NASL с C/C++	134
Перенос с языка NASL	140
Резюме	142
Обзор изложенного материала	143
Ссылки на сайты	144
Часто задаваемые вопросы	145
Глава 3. BSD-сокеты	147
Введение	148
Введение в программирование BSD-сокетов	148
Клиенты и серверы для протокола TCP	149
Компиляция	151
Пример выполнения	151
Анализ	151
Компиляция	154
Пример выполнения	154
Анализ	154
Анализ	156
Клиенты и серверы для протокола UDP	156
Компиляция	158
Пример исполнения	158
Анализ	158

Компиляция	160
Пример исполнения	160
Анализ	161
Компиляция	163
Пример исполнения	163
Анализ	163
Компиляция	165
Пример исполнения	165
Анализ	165
Опции сокетов	166
Анализ	168
Сканирование сети с помощью UDP-сокетов	169
Компиляция	176
Пример исполнения	176
Анализ	177
Сканирование сети с помощью TCP-сокетов	178
Компиляция	188
Пример исполнения	188
Анализ	189
Многопоточность и параллелизм	191
Резюме	193
Обзор изложенного материала	193
Ссылки на сайты	195
Часто задаваемые вопросы	195
Глава 4. Сокеты на платформе Windows (Winsock)	197
Введение	198
Обзор Winsock	198
Winsock 2.0	200
Компоновка с использованием Visual Studio 6.0	201
Задание компоновки в исходном коде	201
Анализ	203
Пример: скачивание Web-страницы с помощью WinSock	206
Анализ	207
Программирование клиентских приложений	207
Анализ	210
Программирование серверных приложений	211

10 Защита от взлома: сокеты, эксплойты и shell-код

Анализ	214
Написание эксплойтов и программ для проверки наличия уязвимостей	215
Анализ.....	222
Анализ.....	223
Резюме	224
Обзор изложенного материала	224
Ссылки на сайты	225
Часто задаваемые вопросы	226
Глава 5. Сокеты в языке Java	233
Введение	234
Обзор протоколов TCP/IP	234
TCP-клиенты	235
Компиляция	237
Пример выполнения	238
Анализ	238
Разрешение IP-адресов и доменных имён	239
Пример выполнения	240
Анализ	240
Пример выполнения	241
Анализ	242
Ввод/вывод текста: класс LineNumberReader	242
Компиляция	245
Пример выполнения	245
Анализ	245
TCP-серверы	246
Компиляция	249
Пример выполнения	249
Анализ	249
Использование Web-браузера для соединения с сервером TCPServer1	250
Работа с несколькими соединениями	251
Компиляция	257
Пример выполнения	257
Анализ	258
Программа WormCatcher	260
Компиляция	264
Пример выполнения	264
Анализ	265