Предметный указатель

A

ACL, 168
ActiveX, 200
API monitor, 143
ASP-страница, 151

B

BIOS, 357

C

CFI, 371
COM/DCOM, 200
CWD, 150

D

DDK, 327
DLL, 152
Dr.Watson log, 104

E

EEPROM, 357

F

FreeBSD, 270

H

HTML-код, 202
HTTPD, 263
HTTP-заголовок, 193

I

IDA, 94
IDC-сценарий, 112
IDS, 213
IDT, 383
IRQ, 381

J

Java, 259
Java 2, 153
JEDEC, 372
JVM, 37; 259

K

KLOC, 34

L

LKM, 385
LOC, 34

M

MBR, 373
MIME, 263
MIPS, 298

N

NVRAM, 255

P

PCL, 187
PHP, 173
PIC, 384
PID, 147

R

RISC, 298

S

SDK, 95
SourceScope, 66
SPARC, 301
SQL Server 7, 86
StackGuard , 66

T

TEB, 267

U

Unicode, 242
URI, 148
UTF-8, 243

W

Web-браузер, 200
Web-сервер, 150; 236
  Apache, 263

X

XOR, 296
XSS, 190

А

Адрес
  в векторе вторжения, 252
  внедрения, 254
  возврата, 252
  эффективный, 99
Анализатор, 228
Архитектура
  MIPS, 298
  RISC, 298
Атака, 63
  на Internet Explorer 5, 205
  на вызовы функций API, 169
  на неисполняемый стек, 321
  на переполнение буфера, 247
    в стеке, 249
    в ядре, 387
  подмены Web-узла, 205
  с помощью
    XSS, 191
    вредоносного содержимого, 204
    символических ссылок, 262
    файла данных, 261

Б

База данных
  Informix, 172
  Oracle, 167
Библиотека
  ActivePerl, 151
  DLL, 152
  irc.dll, 221
  mshtml.dll, 206
  NDIS, 374
  scrrun.dll, 196
  xt, 265
Библиотечные вызовы API
  отслеживание, 148
Брандмауэр, 72
Буфер
  клавиатуры, 188
Быстрый останов, 225

В

Вектор вторжения, 64; 250
Вентиль, 383
Ветвление процессов, 167
Взлом
  компилятора, 65
  с помощью
    драйвера устройства, 91
    совместно используемых буферов, 91
Вирус
  CIH, 364
Внесение ошибок, 125
Восстановление исходного кода, 78

Г

Гонка на выживание, 49

Д

Дамп памяти, 233
Декомпилятор, 83
Декомпиляция, 103
Дизассемблер, 83
  Dr. Watson, 130
  IDA, 94; 146; 279
  WDASM, 103
Диспетчер
  API, 143
Доверительные отношения, 149
Доступ
  к диску, 373
  к исполняемым файлам, 150
  к командному интерпретатору, 154
  с правами суперпользователя, 92
Драйвер, 327
  выгрузка, 330
  для перенаправления, 341
  регистрация, 332
  фильтрующий, 385

Ж

Журнал
  ошибок, 106

З

Заплата
  в ядро Windows NT, 348
  для образа ядра, 388
  установка, 125
Зона активизации, 64

И

Идентификатор
  сеанса, 175
    подбор, 176
Искажение данных
  в памяти, 249

К

Каталог
  cgi-bin, 149
  переход к другому, 170
  права доступа, 93
  просмотр содержимого, 111; 155
  сокрытие, 344
  текущий рабочий, 150
Код
  Java, 259
  возврата ошибки, 180
  двоичный
    исправление, 346
  командного интерпретатора, 60
    защита, 314
  опроса клавиатуры, 385
  переносимый, 37
  трассировка, 219
  управляющий, 182
    для терминала, 186
Кодирование
  символов
    альтернативное, 239
Кодировка
  Unicode, 242
  UTF-8, 243
Команда
  build, 328
  call, 293
  cd, 328
  dir, 111
  echo, 161
  getopt, 265
  in, 358
  jmp, 322; 348; 355
  jz, 354
  NOP, 298; 317
  out, 359
  passwd, 265
  push, 350
  retn, 350
  командного интерпретатора, 155
Командный интерпретатор, 154
  внедрение команд, 154
Компилятор
  для языка C++, 65
Контекст, 122
Контратака, 206
Контроллер
  клавиатуры, 386
Контрольная сумма, 297
Куча, 288

М

Маршрутизатор
  Cisco, 251; 257
Метасимвол, 228
  в архиве программы FML, 202
  в заголовке сообщения электронной почты, 202
  управляющий, 240
  эквивалентный, 240
Метод
  "белого ящика", 84
  "серого ящика", 85
  "черного ящика", 84
Микросхема
  8042, 386
  82559, 367
  8259, 384
  93C46, 367
  ASIC, 367

Н

Наблюдаемость, 47
Набор средств для взлома, 326
  ntroot, 374
  на уровне ядра, 326
Наследование
  дескрипторов, 167
  прав доступа, 168

О

Обработчик исключений, 267; 274
Окно регистров, 301

Опасность, 56
Операционная система
  FreeBSD, 270
  IOS, 257
  Windows NT
    установка заплат, 348
Операция
  XOR, 296
Определение
  операционной системы, 72
Отладчик, 82; 117
  GDB, 145
Отложенная передача управления, 298
Отслеживание маршрута, 73
Охват кода, 90
Ошибка, 49
  F00F, 358
  в сетевых адаптерах Ethernet, 92
  внесение, 125
  обработка, 180
  при выполнении арифметических операций, 275
  при классификации, 236
  строки форматирования, 260

П

Пакет
  IRP, 330
  UUCP, 142
Память
  EEPROM, 357
    параллельная, 370
    последовательная, 369
  искажение данных, 249
  управление, 275
  энергонезависимая
    операции чтения и записи, 358
Переменная
  глобальная, 173
    TERM, 265
  скрытой формы, 173
  среды, 172; 264
    $HOME, 265
    LD_LIBRARY_PATH, 173
    TARGETPATH, 328
  экземпляра, 291
Перенаправление атаки, 74
Переполнение буфера, 104
  в EFTP, 263
  в exim, 262
  в MidiPlug, 262
  в Netscape Communicator, 262
  в passwd, 265
  в rlogin, 265
  в sccw, 265
  в sendmail, 263
  в Web-сервере Apache, 263
  в Winamp, 261
  в стеке, 249; 268
  в ядре, 387
  на стороне клиента, 206
  с помощью переменных и тегов, 262
  с помощью переменных среды, 264
Перехват
  вызова, 335
  прерываний, 383
Переход
  внешний, 309
  локальный, 309
Платформа
  AIX/PowerPC, 313
  HP/UX PA-RISC, 305
  Solaris, 148
  SPARC, 301
Подключение
  к запущенному процессу, 146
Подмена
  Web-узла, 205
Полезная нагрузка, 250; 292
  для архитектуры MIPS, 298
  для архитектуры RISC, 298
  для нескольких платформ, 316
  для платформы PA-RISC, 305
  для платформы SPARC, 301
  кодирование, 296; 312
  размер, 294
Потайные ходы, 75
Предзагрузчик, 201
Преобразование символов, 229
Прерывание, 381
  клавиатуры, 386
  обработка, 119
  перехват, 383
Принцип наименьших привилегий, 141
Программа
  APISPY32, 93; 218
  Back Orifice 2000, 340
  Cold Fusion, 156
  Dbgvnt, 332
  Dependency Walker, 196
  Dr. Watson, 130
  dyninstAPI, 90
  elitewarp, 155
  exim, 262
  Fenris, 223
  File Monitor, 143
  FML, 202
  FST, 143
  GDB, 145; 232; 310
  GroupWise, 171
  Hailstrorm, 86
  Hotmail, 204

HSphere, 171
IDA, 94; 103
IDA-Pro, 105; 145
Internet Explorer, 201
Internet Explorer 5, 205
IPSwitch Imail, 176
ITS4, 66
jvmStart, 260
ltrace, 148
MailSweeper, 204
memcpy, 121
MidiPlug, 262
MS Excel, 195
MS Outlook XP, 202
mssql-ods, 258
netcat, 140; 152
Netscape Communicator, 262
Netterm, 187
nmap, 73
OllyDbg, 227
passwd, 265
Purify, 86
REC, 103
regmon, 143
rlogin, 265
sccw, 265
sendmail, 263
setlocate, 265
SoftIce, 227; 351; 374
SourceScope, 66
SQL Server, 258
SQL Server 7, 86
StackShield, 67
Taylor UUCP, 264
Telnet, 173
The PIT, 124
traceroute, 73
Trillian, 221
Tripwire, 340
Truss, 148
Webalizer, 193
Winamp, 261
xterm, 164
для внесения ошибок, 82
клиентская, 181
многопотоковая, 121
регистрации нажатий клавиш, 385
Просчет, 49
Протокол
BGP, 251
FTP, 163
OSPF, 251
TFTP, 165
T-SQL, 258
Процесс
ветвление, 167
идентификатор, 124
планирование запуска, 165
Процессор
Intel x86, 292

P

Расширяемая система, 37
Регистр процессора, 254
EAX, 255
EBP, 271; 295
EBX, 297
ECX, 297
EDI, 293; 297
EIP, 293
ESP, 271
FS, 267
Режим недоверия, 88
Риск, 54

C

Сервер
Apache, 263
CesarFTP, 244
EFTP, 263
eXtremail, 288
FTP, 266
IceCast, 243
IIS, 143; 151; 242
I-Planet, 145; 232
SpoonFTP, 239
Titan, 243
Серверное приложение, 138
Сетевой адаптер
Ethernet, 92
ключ реестра, 377
неразборчивый режим, 376
Сигнальное значение, 318
Сигнатура
атаки, 215
Символ
ESC, 240
NULL, 170; 231; 249; 271
удаление, 315
альтернативная кодировка, 239
возврата каретки, 159
двойной кавычки, 157
косой черты, 240
обратной косой черты, 160
посторонний, 238
форматирования, 267
Синтаксический анализ, 228
Синхронизация, 366
Система обнаружения взлома
на основе аномальных событий, 213
на основе сигнатур, 213

Сканирование
  портов, 73
  сети, 71
Сокет, 166
Сокрытие
  каталога, 344
  процесса, 336
  файла, 344
Спецификатор формата
  %00u, 286
  %n, 285
Спецификация
  CFI, 371
Список
  запущенных потоков, 147
  контроля доступа, 168
Ссылка
  символическая, 262
Стек, 252
  неисполняемый, 321
Строка
  форматирования, 267; 283
СУБД, 258
  Progress, 260
  переполнение буфера, 258
Сценарий
  FTP, 163
  Perl, 151
  PHP, 164
  вложенный, 151
  переносимый, 190

T

Таблица
  vtable, 291
  дескрипторов прерываний, 383
  переходов
    динамическая, 293
  прерываний, 381
  соответствий, 295
Тег
  boron, 134; 380
  CFEXECUTE, 156
  EMBED, 206
Точка
  входа, 88
  останова, 118; 145
    для страниц памяти, 227
Трамплин, 309; 320
Трассировка, 145
  во время выполнения программы, 223
  кода, 219
  обратная, 220
  стека, 106

У

Уведомление
  об успехе, 64
  обратной связи, 65
Указатель, 230
Утилита
  at, 165
  cat, 155
  dumpbin, 111
  ping, 155
Уязвимое место, 49
  автоматизированное выявление, 110

Ф

Фазовое пространство, 176
Файл
  autorun.inf, 374
  cookie, 61; 263
  helpctr.exe, 104
  perl.exe, 149
  sfc.dll, 387
  SOURCES, 328
  драйвера, 328
  конфигурационный
    для расширения привилегий, 142
    поиск, 145
  с расширением
    lnk, 263
    MP3, 262
  сокрытие, 344
  сценария, 161
  шрифта, 152
Фильтр, 212
  для входных данных, 212
  для драйвера, 385
  для команд, 237
  с возможностью переполнения буфера, 264
Функция
  CreateFile(), 373
  DriverEntry(), 329
  fprintf(), 288
  GetObject(), 201
  glob(), 266
  HeapFree(), 290
  Host(), 195
  if(), 348
  lstrcpy, 93
  malloc(), 290
  OpenDataSource(), 258
  OpenThread, 122
  printf(), 260; 287
  QueryDirectoryFile(), 344
  recv(), 280
  scanf(), 268

SeAccessCheck(), 350
sprintf(), 113; 268
strcat(), 268
strcpy(), 93; 268
strlen(), 270; 275
strncat(), 271
strncpy(), 270
syslog(), 270; 288
SystemLoadAndCallImage, 333
VirtualQuery(), 225
VirtualQueryEx, 121
vsprintf(), 268
wcsncat, 106
while(), 348
WSARecvFrom(), 88
wsprintf(), 224
листовая, 308
файловой системы, 205

Х

Хакер, 45
Хранимая процедура, 258; 261

Ц

Цель атаки, 47

Ч

"Червь", 39
ADM w0rm, 40
Code Red, 40

Ш

Шаблон атаки, 64

Э

Электронный шпионаж, 28

Я

Ядро
"заражение" образа, 388
переполнение буфера, 387
установка заплаты, 348
Язык программирования
Java 2, 153
Perl, 88
PHP, 173
Visual Basic, 203