

INDEX

A

- AArch64, 22
 - buffer initialization, 185
 - functions in, 146
 - instructions
 - adrp, 148
 - cbz/cbnz, 185
 - jump, 184
 - ldp, 148
 - ret, 147, 182
 - stp, 148, 186
 - pseudo-instructions, 184
 - registers, 65
 - x29 (frame pointer), 148
 - x30 (link register), 148, 183
 - x31 (zero register), 184
 - syscall convention, 65
- ABI (application binary interface),
 - 20, 111
 - parameters, 113
 - return values, 113
 - System V, 113
- accept function, 281
- adding two numbers
 - AArch64, 23
 - ARM, 22
 - C, 18
 - MIPS32, 24
 - MIPS64, 24
 - RISC-V, 25
 - SCTW-2000, 13
- addressing modes, 99
 - ARM
 - indirect PC-relative, 98
 - post-indexed, 180
 - post-indexed immediate offset, 266
 - pre-indexed, 186, 323
 - direct or register, 99
 - immediate, 99
 - indexed memory, 319
 - indirect, 99
 - PC region (pseudo-direct), 153, 326
 - PC relative, 99
- addressing space, 89
- address of operator (&), 131
- address pins, 81
- address space layout randomization (ASLR), 56, 140
- addition assignment operator (+=), 19
- Alpine Linux, 287
- application binary interface. *See* ABI
- application-level libraries, 4
- ar (GNU archiving tool), 163
- architecture, 8
- arithmetic logic unit (ALU), 8
- ARM, 21
 - AArch32 (ARM32), 21
 - AArch64 (ARMv8), 21
 - addressing modes
 - indirect PC-relative, 98
 - post-indexed, 180
 - post-indexed immediate offset, 266
 - pre-indexed, 186, 323
 - buffer initialization, 179
 - flags, 177
 - functions in, 143
 - instruction format, 177
 - CONDITION values, 178
 - db suffix, 181
 - ia suffix, 181
 - instructions
 - b, 176
 - bl, 143
 - bx lr, 144
 - bXX, 176
 - cmp, 177
 - eor, 179
 - jump, 176
 - ldr, 97, 99
 - lrb, 177

- ARM (*continued*)
 - instructions (*continued*)
 - mvn, 359
 - rev, 358
 - stmltia, 181
 - str, 179
 - strlt, 180
 - subs, 359
 - literal pool, 100
 - registers, 8, 64
 - r11/fp, 144
 - r13/sp, 144
 - r14/lr, 143–144, 176
 - r15/pc, 144, 176
 - syscall convention, 64
 - Thumb, 21, 144
 - Thumb2, 144
- arrays in C, 37, 159
- ASCII, 79
- ASLR (address space layout randomization), 56, 140
- assembler directives, 43, 88
- assembly, 29
- assignment operator (=), 212
- AT&T syntax, 43, 375
- attacks
 - BadUSB, 224
 - DDoS, 196
 - DoS, 340
- awk command, 40
- B**
- backdoor
 - ARM, 230
 - Base64 gzipped, 232
 - echo dumped, 232
 - C implementation, 210
 - MIPS, 233
 - Base64 gzipped, 235
 - echo dumped, 235
 - RISC-V, 236
 - Base64 gzipped, 238
 - echo dumped, 238
 - x86_64, 220
 - Base64 gzipped, 222
 - Base64 gzipped reduced, 229
 - echo dumped, 223
 - echo dumped reduced, 229
- bare metal, 4
- base 2 (binary), 76
- base 8 (octal), 76
- base 10 (decimal), 76
- base 16 (hexadecimal), 14, 74
- base64 command, 222
- Base64 encoding, 222
- bash
 - <> operator, 201
 - <& operator, 201
 - <<< operator, 242
 - >& operator, 201
 - /dev/tcp, 201
 - exec command, 201
 - for loop, 291
- big endianness, 86
- binary executables, 18
 - dynamic, 40
 - PIE vs. non-PIE, 56
 - static, 40
- binary numbers, 76
- bind function, 281
- binfmt_misc module, 387
- /bin/sh, 96
- bitmasks, 248, 362
- bits, 74
- bitwise negation operator (~), 346
- blocking vs. non-blocking I/O, 348
- botnets, 196, 276
 - bots/zombies, 196
- buffer overflow, 132, 141
- buffer overflow exploiting, 140–143
 - canary exfiltration, 140
 - crafting the exploit, 142
 - executable stack, 141
- buffers, 125, 159
- build systems, 245
- bus, 82
 - address, 75
 - control, 81
 - data, 75
- BusyBox, 287
- bytes, 74
- C**
- C2 (command and control) server, 158
- canaries, 140–143
 - __stack_check_guard function, 156

- __stack_chk_fail function, 140
 - x86_64 location, 140
- central processing unit. *See* CPUs
- C functions. *See names of individual functions*
- CHAR_BIT constant, 93
- C headers
 - arpa/inet.h*, 279
 - stdio.h*, 94, 278
 - stdlib.h*, 278
 - sys/mman.h*, 279
 - sys/socket.h*, 279
 - unistd.h*, 34, 278
- chip select (CS) pin, 81
- chipset, 4
- chronogram, 84
- C language
 - conditionals, 134, 161
 - if, 161
 - function prototype, 35
 - labels, 166
 - pointers, 88
 - casting to functions, 283
 - dereferencing, 131
 - string representation, 80
 - union, 342
- code instrumentation, 135
- compiling, 29
- complex instruction set computers (CISC), 22
- computer model, 11
- connect function, 213
- containers, 286
- control groups (cgroups), 286
- control pins, 81
- control units, 9–11, 15
- C operators. *See names of individual operators*
- CPUs (central processing units), 6–11
 - arithmetic logic units, 8
 - accumulator, 9
 - clock, 10, 84
 - control unit, 9–11, 15
 - cycles, 11
 - native word size, 74
 - pipeline, 9
 - registers, 7

- scalar vs. superscalar, 10
 - ticks, 11
- cross-compilation, 19, 20, 246
 - C preprocessor (cpp), 34
 - C runtime (CRT) files, 39, 61, 96

D

- data pins, 81
- .data section, 53, 165
- data types in C, 93
 - char, 93
 - sizes, 93
 - void *, 94
- debuggers, 91
- decimal representation, 13
- delay slots, 331, 376
- dereference operator (*), 131
- /dev/null*, 228
- /dev/shm*, 249
- /dev/tcp*, 201
- /dev/zero*, 228
- direct addressing mode, 99
- disassembly, 19
- Docker, 286
 - commit command, 305
 - container, 201, 286
 - Dockerfile, 286
 - exec command, 201
 - flags
 - ip (IP), 290
 - it (interactive terminal), 287
 - name, 288
 - rm, 291
 - net (network), 290
 - noexec, 249
 - v (volume), 288
 - images, 286, 289
 - images command, 289
 - network command, 289
 - ps command, 287
 - rm command, 287
 - run command, 287
 - stop command, 309
 - virtual networks, 286, 289
 - volumes, 287
- doublewords (dwords), 74

- droppers, 241
 - ARM, 260
 - Hajime, 269
 - MIPS, 258
 - RISC-V, 267
 - stealth droppers, 249
 - using existing tools, 242
 - x86_64, 255
- dynamic binaries, 40
- dynamic libraries, 41

E

- EBCDIC (Extended Binary Coded Decimal Interchange Code), 79
- echo command, 143
- End of File (EOF), 242
- errno command, 279
- errno variable, 279
- Ethernet, 343
- Executable and Linkable Format (ELF), 30
 - crafting
 - with gas, 391
 - with nasm, 388
 - headers, 49, 388
 - producing minimal ELFs, 388
 - program headers
 - DYNAMIC, 42
 - GNU_STACK, 47, 51
 - hand-crafted, 388, 391
 - INTERP, 42
 - LOAD, 49
 - NOTE, 51
 - program header table, 49, 388
 - sections, 53
 - manipulating with objcopy, 384
- execve function, 96
- EXIT_FAILURE macro, 279
- _exit function, 34
- exploits, 94
 - buffer overflow, 132, 141
 - command injection, 141
 - format strings, 135
 - return to libc, 140

F

- fcntl function, 349
- fexecve function, 251

- fifo file, 142
- file command, 30
- file descriptors, 215
- File Transfer Protocol (FTP), 241
- file transfer server, 292
- filtered ports, 209
- firewalls, 209
- firmware, 4
- first in, first out (FIFO)
 - methodology, 108
- forensic analysis, 55, 248
- for loop, 160
- format strings, 94
- free function, 118
- functions, 111. *See also names of individual functions*
 - call convention, 114
 - epilogue, 115
 - leaf, 121
 - in ARM, 146
 - local variables, 120
 - parameters, 113, 128
 - pass by reference, 130
 - pass by value, 129
 - prologue, 115
 - stack frame, 116, 117
 - pointer, 117

G

- gas (GNU Assembler), 43
 - AT&T syntax, 43, 375
 - current address instruction (.), 176
 - directives
 - .asciz, 97
 - .balign, 330
 - .byte, 391
 - .data, 65
 - .equ, 165, 193
 - .fill, 175
 - .global/globl, 43
 - .intel_syntax noprefix, 375
 - .long, 391
 - nasm equivalence, 392
 - .quad, 330
 - .section, 48
 - .set reorder/noreorder, 376
 - .short, 391
 - .text, 59

- Intel syntax, 43, 376
- march flag (RISC-V), 366, 380
- tips and tricks, 375
- gcc command, 19
- && operator, 136, 167
- attribute naked, 52
- flags
 - c, 58
 - D*CONSTANT*, 68
 - e *FUNC*, 68, 382
 - fno-asynchronous-unwind
 - tables, 52
 - fno-pic, 91, 382
 - fno-pic (MIPS), 68
 - fnostack-protector, 382
 - fomit-frame-pointer, 19, 119
 - fpic, 382
 - fstack-protector, 121, 125, 382
 - g, 377, 382
 - I/*PATH*, 382
 - L*LIB*, 58, 382
 - L*PATH*, 382
 - L*path*, 58
 - march (RISC-V), 366, 380
 - mno-abi-calls (MIPS), 68
 - nodefaultlibs, 44, 381
 - no-pie, 91, 382
 - nostartfiles, 39, 381
 - nostdlib, 44, 381
 - o, 34
 - O0, 121, 377
 - pie, 382
 - static, 39, 382
 - TSEGMENT=*ADDR*_, 56
 - v/-verbose, 60, 381
 - Wl, option, 382
 - Wl, --build-id=*none*, 52
 - Wl, -e*FUNC*, 56, 382
 - Wl, -TSEGMENT=*ADDR*, 382
 - Wl, -verbose, 57, 382
 - x, 242
 - z execstack, 382
 - z noexecstack, 47, 382
 - z noseparate-code, 50, 382
- goto extension, 167
- gdb (GNU Debugger), 91
 - AT&T syntax, 378

- commands
 - detach inferior, 379
 - disassemble, 377
 - inferior, 379
 - info inferiors, 379
 - kill inferiors, 379
 - p (print), 378
 - set detach-on-fork, 379
 - set disassembly-flavor, 378
 - set follow-fork-mode, 379
 - target remote IP:port, 379
 - x (dump), 92, 378
- .gdbinit*, 377
- gdb-multiarch, 379
- gdbserver, 380
- Intel syntax, 378
- tips and tricks, 377
- gets function, 134
- glibc, 38, 288
- goto statement, 166
- grep command, 20
- guard conditions, 178

H

- hacker, xxi
- Harvard architecture, 8
- head command, 291
- heap, 283
- heavy wizardry, xxi
- “Hello, world!” program
 - ASM, 59
 - C, 90
 - x86_64 ASM, 87
- hexadecimal representation, 13, 74, 76

I

- immediate addressing mode, 99
- in_addr struct, 213
- #include directive, 35
- indexed memory addressing mode, 319
- indirect addressing mode, 99
 - ARM PC-relative, 98
- inet_ntoa function, 282
- infinite loop, 159
- Intel processor. *See* x86_64
- Intel syntax, 43, 376, 384
- Internet of Things (IoT), 23
- Internet Protocol (IP), 208

instruction set architecture (ISA), 12
I/O, blocking vs. non-blocking, 348

J

jargon file, xxi
Java, string representation in, 80
jump instructions
 AArch64, 184
 ARM, 174
 MIPS, 189
 RISC-V, 192
 x86_64, 166

K

K, KB, KiB (memory units), 7
kernel, 32
Knuth, Donald, xxv

L

labels, 88
last in, first out (LIFO)
 methodology, 108
ld (linker), 30
 flags
 -e *FUNC*, 58
 -I/*PATH*, 58
 -l*LIB*, 166
 -L*PATH*, 166
 -o, 30
 -z noexecstack, 47
 -z noseparate-code, 50
leaf functions, 121, 146
less command, 35
libc, 38
 glibc, 38, 288
 musl, 288
libraries
 dynamic, 41
 static, 163
 system, 4
linking, 29
listen function, 281
literal pool (ARM asm), 100
little endianness, 86
living off the land (LotL), 202, 276
 binaries, 277
local variable functions, 120
loop unfolding, 191

lsuf command, 219
lspci command, 343

M

MAC address, 343
MAC (medium access control)
 layer, 210
machine code, 13
macros, 279
main function, 36, 96
 argc, 36
 argv, 36
 envp, 96
make tool, 245
 makefile, 245
 variables, 245
malloc function, 118, 283, 294
malware
 botnets, 276
 viruses, 276
 worms, 276
 Hajime, 269, 297
 Linux.Wifatch, 297
 Mirai, 224, 297
 Morris worm, 276, 311, 340
memory, 6–7
 addresses, 7
 chip, pins on, 81
 contents, 7
 Flash, 8
 heap, 283
 locations, 7
 pages, 49
 RAM, 6
 reading, 82
 ROM, 6
 sections, 53, 165–166
 .data, 165
 .rodata, 166
 .text, 53, 165
 units, 7
memset function, 173
memory management unit
 (MMU), 45
microcode, 110
MIPS, 23
 32- vs. 64-bit, 24, 104
 buffer initialization, 191

- delay slots, 331
- functions in, 149
- instructions
 - bal, 149
 - beq, 189
 - bne, 189
 - j, 189
 - jal, 189
 - jr, 149, 187, 189
 - jump, 189
 - lb, 189
 - lui, 101
 - nop, 329, 376
 - ori, 101
 - slt, 190
 - sw, 191
- pseudo-instructions
 - beq, 189
 - bge, 190
 - bgt, 190
 - ble, 190
 - blt, 190
 - la, 101
 - li, 101
 - move, 188
- registers, 66
 - \$at, 190
 - \$gp, 151
 - \$ra, 149, 187, 189
 - \$s8/\$fp, 150
 - \$zero, 189
 - zeroing, 101
- __start function, 67
- syscall convention, 66
- MIPS64
 - instructions
 - daaddiu, 103
 - daddu, 104
 - dli, 102
 - dsll32, 103
 - lui, 103
 - mnemonics, 12, 13
 - pseudo-instructions, 102
 - registers, 68
 - syscall convention, 68
- mkfifo command, 142
- mmap function, 283
- MMU (memory management unit), 45

- mobile agent system
 - (MAS), 276
 - agency, 338
 - mount command, 249
- Motorola processor, 8
- mprotect function, 283
- musl, 288
- mystrip.sh*, 227

N

- namespaces, 286
- nasm assembler, 29
 - directives
 - \$, 318, 390
 - \$\$, 318, 390
 - db, 88, 97
 - dd, 389
 - dq, 221
 - dw, 389
 - EQU, 165
 - extern, 165
 - gas equivalence, 392
 - .org, 390
 - section, 95, 165
 - times, 165
 - flags
 - f bin, 390
 - f elf64, 30, 390
 - f FMT, 30
 - o, 30
 - octal values, 317
- native word size, 74
- netcat program, 211
 - flags
 - l (listen), 211
 - N, 242
 - p (port), 211
 - v (verbose), 211
 - w (wait), 242
 - serving files, 244
- NetKitty, 200
 - hub mode, 200
 - server mode, 211
- netmasks, 340
- netstat tool, 218
 - flags
 - a (all), 219
 - n (numeric), 219

- netstat tool (*continued*)
 - flags (*continued*)
 - p (process), 219
 - t (TCP), 219
- networks
 - address, 339, 340, 345
 - basic setup, 206
 - connection-oriented, 207
 - datagram-oriented, 207
 - interface/device naming, 342
 - IP, 208
 - MAC address, 343
 - MAC layer, 210
 - network layer, 208
 - OSI model, 209
 - protocol, 207
 - scanning, 337
 - subnetting, 339
 - TCP, 208
 - transport layer, 208
 - UDP, 208
- network scanner
 - acquiring current IP/netmask,
 - 340, 351
 - ARM, 358
 - C, 338
 - speeding up, 347
 - MIPS, 360
 - RISC-V, 361
 - scope of scan and subnetting,
 - 345–346, 353
 - x86_64, 351
- nibbles, 74
- non-blocking I/O, 348
 - EINPROGRESS, 357
- non-PIE binary, 56
- ntohl function, 345
- null byte, 95
- numeric format
 - binary, 76
 - hexadecimal, 76
 - octal, 76

O

- obfuscation, 128, 222
- objcopy, 54
 - automatically generated
 - symbols, 386

- flags
 - add-section, 385
 - add-symbol, 386
 - I, 386
 - O *FMT*, 385, 386
 - only-section=*sec*, 385, 393
 - redefine-sym, 385
 - remove-section=*sec*, 54, 384
 - rename-section, 385
 - set-section-flags, 385
 - strip-symbol=*sym*, 386
- tips and tricks, 384
- objdump program, 19
 - flags
 - d (disassemble), 19, 384
 - full-contents, 54
 - M intel, 19, 384
 - M no-aliases, 384, 395
 - section=*sec*, 54
 - Intel syntax, 384
 - tips and tricks, 384
- octal representation, 76
- one's complement, 78
- opcodes, 12
- operating systems, 4
- OSI model, 209
- output enable (OE) pin, 81

P

- packet storms, 311
- padding, 222
- parameter functions, 113, 128
- pass by reference functions, 130
- pass by value functions, 129
- PC region (pseudo-direct) addressing
 - mode, 153, 326
- PC relative addressing mode, 99
- Perl, 137
- perl -e command, 137
- permissions, 45
- perror function, 279
- PIC (position-independent code), 68
- Pico File Transfer Server
 - (PFTS), 292
- picoWorm, 297
 - ARM, 321
 - MIPS, 324
 - payload C function, 298

- RISC-V, 332
- x86_64, 316
- PIE (position-independent executable), 56, 68
- pLibC, 162
 - AArch64, 182
 - ARM, 174
 - MIPS, 187
 - RISC-V, 192
 - x86_64, 162
- pointer, stack frame, 117
- pointers, 88
 - casting to functions, 283
 - dereferencing, 131
- pop instruction, 109
- ports, 209
- post-decrement operator (x--), 161
- post-increment operator (x++), 161
- post-indexed addressing mode,
 - ARM, 180
 - immediate offset, 266
- #pragma directive, 383
- pre-decrement operator (--x), 161
- pre-increment operator (++x), 161
- pre-indexed addressing mode, ARM, 186, 323
- printf command, 230
- printf function, 94
- printing decimal numbers, 260, 261
- privilege escalation, 313
- /proc, 253
 - /proc/net/dev, 343
 - /proc/net/fib_trie, 340
 - /proc/<PID>/fd, 253
- processes, 31
 - memory sections, 53, 165–166
- processors. *See* CPUs
- processors pipelines. *See* CPUs
- prologue functions, 115
- protocols, 207
 - network, 208
 - transport, 208
- ps command, 253
- pseudocode, 261
- pseudo-instructions, 26
- push instruction, 109
- puts function, 134

Q

- qemu emulator, 379
 - binfmt_misc, 387
 - g port, 379
 - QEMU_STRACE, 380
- quadwords (qwords), 74

R

- radix-based positional numeral system, 76
- RAM disk, 249
- random-access memory (RAM), 6
- ranlib command, 164
- readelf tool, 41, 47, 226
 - flags
 - a (all), 285
 - d (dynamic), 42
 - h (header), 53, 57, 226
 - l (segments), 42, 53
 - n (notes), 51
 - p (string), 59
 - r (relocations), 394
 - S (sections), 53
 - s (symbols), 57
 - W (wide), 228
- readlink command, 42
- read-only memory (ROM), 6
- reduced instruction set computers (RISC), 22
- red zone (stack), 122
- register addressing mode, 99
- register keyword, 19
- registers
 - AArch64, 65
 - ARM, 64
 - instruction pointer, 8
 - MIPS, 66
 - MIPS64, 68
 - program counter, 8
 - RISC-V, 69
 - stack pointer, 108
 - x86_64, 62
- relational operators, 161
- remote code execution (RCE), 277, 338
- REPL, 157
 - AArch64, 182
 - ARM, 174

- REPL (*continued*)
 - MIPS, 187
 - RISC-V, 192
 - x86_64, 162
- return to libC exploit. *See* exploits
- reverse engineering, 108
- reverse shell, 206
 - detection, 218
 - file description dup, 215
 - launching a shell, 217
 - socket connection, 212
- RISC architectures, 23, 104
- RISC-V, 25
 - bswap32 implementation, 361
 - buffer initialization, 196
 - extensions, 365, 380
 - C, 365
 - Zbp, 361
 - functions in, 152
 - instructions
 - addi, 26
 - addu, 26
 - addw, 26
 - auipc, 105
 - beq, 195
 - bge, 195
 - bgtu, 195
 - bleu, 195
 - blt, 195
 - bne, 195
 - jal, 152
 - jalr, 152
 - jump, 194
 - rev8, 361
 - sd, 196
 - set.w, 26
 - slli, 362
 - srli, 362
 - sw, 196
 - pseudo-instructions
 - beqz, 195
 - bgez, 195
 - bgt, 195
 - bgtz, 195
 - ble, 195
 - blez, 195
 - bltz, 195
 - bnez, 195
 - 1a, 105
 - move, 194
 - ret, 152, 193
 - registers, 69
 - ra, 193
 - so/sp, 154
 - syscall convention, 69
 - .rodata section, 166
 - ROM (read-only memory), 6

S

 - scalar processor, 10
 - script kids, xxiii
 - SCTW-2000, 5
 - instruction set architecture, 12
 - opcodes, 12
 - specifications, 12
 - SEGFault exception, 45–46
 - setuid program, 313
 - shell
 - \$? variable, 29
 - call-home, 211
 - piping, 20
 - reverse, 206
 - shellcode, 73, 94, 278
 - AArch64, 100
 - ARM, 97
 - execution service, 278
 - MIPS32, 101
 - MIPS64, 102
 - RISC-V 64 bits, 104
 - writing, 94
 - x86_64, 95, 284
 - shm_open function, 250
 - shuf command, 291
 - sign extension, 78
 - simplest computer in the world.
 - See* SCTW-2000
 - simplified hardware memory model, 81
 - size command, 48
 - sizeof operator, 94
 - SNASE (SNASE’s Not a Shellcode
 - Executor), 278
 - sockaddr_in struct, 213, 279, 344
 - sockaddr struct, 213, 343
 - socket function, 212
 - AF_INET, 212
 - IPPROTO_TCP, 212

- IPPROTO_UDP, 212
- SOCK_STREAM, 212, 281
- sockets, 207
 - creating, 212
 - listening, 280
 - non-blocking, 348
 - reading from and writing to, 217, 244
- sprintf function, 254
- stack-based machines, 8
- stack frames, 116–117
- stacks, 45, 108
 - alignment on x86_64, 123
 - canary, 140
 - executable, 45
 - growth of, 109
 - pointer, 108
 - POP operation, 109
 - PUSH operation, 109
 - red zone, 122
 - smashing, 132
- standard input, 20, 158
- standard output, 87, 158
- __start function, 67
- _start symbol, 28, 39
- stat function, 294
- static binaries, 40
- static libraries, 163
- stderr descriptor, 199
- stdin descriptor, 158
- stdout descriptor, 87, 158
- strace command, 310, 328
- strchr function, 173
- strcmp function, 173
- strip command, 45
- stripping binaries, 45
 - mystrip.sh*, 227
- struct keyword, 213
- subnetting, 339
- superscalar processor, 10
- symbolic links, 42
- symbols, 28
 - global, 28
 - _start, 28, 55
 - symbol table, 57
- synthetic instructions, 26
- syscalls (system calls), 31–33
 - finding constant values for parameters, 328
 - i386, 32
 - SYS_accept, 280, 396
 - SYS_clone, 236, 237, 396
 - SYS_close, 396
 - SYS_connect, 213, 319, 396
 - SYS_dup2, 216, 236, 396
 - SYS_dup3, 236, 396
 - SYS_execve, 96, 217, 396
 - AArch64, 100
 - ARM, 97
 - MIPS32, 101
 - SYS_execveat, 255, 396
 - SYS_exit, 32, 396
 - AArch64, 66
 - ARM32, 64
 - MIPS32, 67
 - MIPS64, 69
 - RISC-V, 70
 - x86_64, 32
 - SYS_fcntl, 349, 396
 - SYS_fork, 218, 396
 - SYS_getpid, 254, 396
 - SYS_getsockopt, 396
 - SYS_ioctl, 340, 396
 - SIOCGIFADDR and SIOCGIFNETMASK constants, 341
 - SYS_listen, 280, 396
 - SYS_memfd_create, 250, 396
 - C wrapper, 251
 - SYS_mmap, 283, 396
 - SYS_mmap2, 396
 - SYS_mprotect, 283, 396
 - SYS_nanosleep, 357, 396
 - SYS_open, 247, 396
 - SYS_openat, 333, 396
 - SYS_ptrace, 92, 396
 - SYS_read, 396
 - SYS_recv, 244, 396
 - SYS_send, 396
 - SYS_setsockopt, 396
 - SYS_socket, 212, 396
 - AF_INET, 212
 - IPPROTO_TCP, 212
 - IPPROTO_UDP, 212
 - SOCK_STREAM, 212
 - SYS_socketcall, 396
 - SYS_stat, 294
 - SYS_unlink, 218, 396

- syscalls (*continued*)
 - SYS_unlinkat, 236, 396
 - SYS_vfork, 236, 396
 - SYS_write, 396
- /sys/class/net, 343
- /system/bin/sh, 97
- system function, 141
- system libraries, 4
- system structs
 - ifreq, 341
 - in_addr, 213, 344
 - in_addr_t, 344
 - sockaddr, 213, 343
 - sockaddr_in, 213, 344
 - stat, 293
 - timespec, 357

T

- test environments, 286
 - extending for other platforms, 304
- TeXbook, The* (Knuth), xxv
- .text section, 53, 165
- time-of-check to time-of-use (TOCTOU) vulnerabilities, 313–314
- toolchain, 20
- trampoline function, 46
- Transmission Control Protocol (TCP), 208
 - connection packets, 350
 - handshake, 350
- two's complement, 78
- two-stage worm, 301

U

- undefined behavior, 128
- Unicode, 79
- User Datagram Protocol (UDP), 208
- UTF-8, 79
- UTF-16, 80

V

- variables
 - declaration, 126
 - global, 120
 - initialization, 126
 - local, 120
- viruses, 276
- von Neumann architecture, 8

- vulnerabilities
 - buffer overflow, 107, 132
 - race condition, 312
 - remote code execution, 338
 - time-of-check to time-of-use, 313–314

W

- wannabes, xxiii
- while loop, 159
- words, 74
- worms, 276
 - file transfer, 292
 - going wrong, 311
 - infection (RCE), 277
 - payload, 297
 - single-stage, 316
 - target selection/network scanning, 298, 338
 - two-stage, 301
- write/read (WR/RD) pin, 81

X

- x86_64, 18
 - addressing modes
 - PC relative, 221
 - RIP relative, 221
 - buffer initialization, 169–174
 - flags, 168
 - instructions
 - bswap, 354
 - call, 112, 166
 - cmp, 167, 170
 - cmp vs. test, 317
 - dec, 170
 - enter, 123
 - inc, 170
 - jmp, 166
 - jne, 170
 - jnz, 170
 - jrcxz, 185
 - jump, 166
 - jx (conditional jumps), 169
 - lea, 131, 221, 376
 - leave, 123
 - loop, 171
 - movabs, 376
 - ret, 112
 - test, 317

- registers, 8, 62
- string instructions, 172
 - cld, 174
 - cmps, 173
 - lods, 173
 - movs, 173
 - repe/repz prefix, 173
 - rep stosq, 172
 - scans, 173
 - std, 174
 - stos, 173
- syscall convention, 32, 62

- xxd tool, 103, 225
 - flags
 - e (endian), 266
 - g (group), 266
 - i (include), 301
 - p (plain), 228

Z

- Z-80 processor, 8
- zero copy operations, 244
- 0x00sec.org*, xxii