

INDEX

Numbers and Symbols

- 3Com TFTP 2.0.1
 - downloading and installing, 42–43
 - public exploit for transport mode vulnerability, 427–429
- 3CTftpSvc* process, attaching, 424–425
- 3CTftpSvc.exe*, 295
- 7-Zip programs, 10
- & (ampersand), for running commands
 - in browser, 328
- \\ (double backslashes), for escape, 186
- > symbol, for redirecting input, 61
- >> operator, 61, 81
- #include command (C), 84
- | (pipe), 65
- / (slash), as delimiter character in sed, 65

A

- absolute path, 56
- Address Resolution Protocol (ARP)
 - basics, 161–163
- address space layout randomization (ASLR), 364, 440
- adduser command, 58–59, 309
- administrative privileges
 - gaining to control domain, 296
 - for Windows 7 applications, 285
- Administrator password, for
 - Windows, 33
- Adobe Acrobat Reader, 225–226
 - installing, 46
- Advanced Execution Standard (AES), 269
- Advanced Packaging Tool (apt), 66

- Aircrack-ng
 - cracking WEP keys with, 347–350
 - cracking WPA/WPA2 keys with, 353–356
- Aireplay-ng
 - to force client reconnection, 354
 - rebroadcasting ARP packets
 - with, 348
- airmon-ng check kill command, 342
- Airmon-ng* script, 341–342
- airodump-ng command, 342–343, 347
- all users, permissions for, 62
- ampersand (&), for running commands
 - in browser, 328
- Android, 456
 - emulators, 449
 - setting up, 22–27
 - starting, 26–27
 - relationship with security updates, 457
 - scripting languages vs. C code, 468
 - SDK manager, 23
 - software
 - building, 449–450
 - deploying, 450–451
 - installing, 24
 - Virtual Device Manager, 24–25
- Android Master Key vulnerability, 459, 462–463
- anonymous* user, on Windows XP target, 157
- antivirus application avoidance,
 - 257–275
 - hiding in plain sight, 274
 - Microsoft Security Essentials, 261–262

- antivirus application avoidance
 - (*continued*)
 - payload hiding, 263–274
 - Railgun, 283
 - trojans, 258–259
 - with Veil-Evasion, 270–274
 - VirusTotal, 262–263
- antivirus applications
 - how they work, 260–261
 - signatures for, 438
- antivirus definitions, 260
- Apache server
 - default “It Works” page, 169–170
 - installing, 44
- APK file, 461–464
- APKTool, installing, 462
- appending text to file, 61
- apt (Advanced Packaging Tool), 66
- argument string, Perl for creating, 376
- ARP (Address Resolution Protocol)
 - basics, 161–163
- ARP cache poisoning, 160–166
 - with Arpspoof, 164–165
 - as bottleneck, 166
 - impersonating default gateway
 - with, 165–166
- ARP request
 - generating, 349
 - relay attack, generating IVs with, 348–349
- Arpspoof, ARP cache poisoning with, 164–165
- ASLR (address space layout randomization), 364, 440
- assembly instructions, converting to shellcode, 398–399
- Atftpd TFTP server, 187
- attack string, finding in memory, 408–411
- Aurora exploit, 220–222
- authentication, fake, 347–348
- authorization, for penetration test, 3
- automatic security updates
 - opting out, in Windows 7, 50
 - turning off, 34
- AutoRunScript parameter, for Metasploit, 224–225
- auxiliary/server/capture/smb*
 - module, 302
- awk command (*sed*), 66

B

- backdoored code, 458–461
 - testing from, 193–194
- background command (Meterpreter), 311
- background job, killing in
 - Metasploit, 222
- BackTrack Linux, 55
- bar codes, QR (quick response)
 - codes, 447
- Bash command processor, 56
- Bash scripts, 75–81
 - else statement in, 78
 - for loop in, 78–79
 - if statement in, 77–78
 - pinging hosts on network with, 76
 - running, 77
 - streamlining results, 79–81
 - then statement in, 78
- .bash_history* file, 295–296
- BeEF (Browser Exploitation Framework), 331–335
- bind payload, 307
- bind shell payload, 102–103
- bind shells, 71, 98, 180
- bitwise XOR operation, 344
- Bkhive, 205
- Blackboard, Java for, 241
- BookApp custom web application
 - attacking, 313–337
 - installing, 53–54
- booting
 - Kali Linux, 11
 - virtual machine delay in, 207
- bootkey, 189, 205
- breakpoints in program, 368
 - running program to next, 370
 - setting, 393
- bridged network, for VMware
 - connection, 13, 14, 16, 31, 48
- Browser Exploitation Framework (BeEF), 331–335
- browser_autopwn* module, 235–237
- browsers
 - & for running commands in, 328
 - attack for opening link in mobile, 455
 - autopwning, 237
 - exploitation, 219–225
- brute forcing, 198
 - LM-hashed passwords, 208
 - MD5 hashes, 212

- NTLM-hashed passwords, 210–211
- use in Hyperion, 269
- WPS pin, 356–357
- buffer overflow
 - in Linux, 364–378
 - preventing exploits, 439–440
 - in third-party software, exploiting, 190–191
 - War-FTP crash due to, 384
 - in Windows, 379–400
- bugs, finding with code review, 422
- Bully, cracking WPS with, 357
- Burp Proxy, web application testing with, 314–319
- Burp Repeater, 314
- Burp Spider, 314

C

- C programs, 84–85
 - for Android devices, 468
 - causing crash, 366–367
 - memory use, 363–364
 - vulnerability to stack-based buffer overflow, 365–366
- CA (certificate authority), 171
- Cadaver, 150–151, 182
- Cain and Abel for Windows, 304
- Cain password tool, 303
- calling conventions, 390
- canaries, 440
- capturing traffic, 155–175. *See also* Wireshark
 - ARP cache poisoning, 160–166
 - DNS cache poisoning, 167–169
 - networking for, 156
 - on wireless network, 342–343
- cat command, 61
- cat /etc/shadow command, 194
- CCMP (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol), 351
- cd command, 56
- CERTCN option, 234
- certificate, for Java applet, 234
- certificate authority (CA), 171
- ceWL custom wordlist generator, 200–201
- check function, in Metasploit exploits, 147–148
- chmod command, 62
 - making script executable, 76
- clients
 - Aireplay-ng to force reconnection, 354
 - contact information for, 3
 - exploiting vulnerability in, 88
 - goals for pentest, 3
- client-side attacks
 - exploitation with, 218–239
 - mobile hacking, 454–457
- clipboard (Windows), stealing data from, 334
- closing
 - handler, 228
 - shell, 100
- code review, finding bugs with, 422
- command line arguments, in C, 84
- command shell
 - opening listener, 70–71
 - pushing back to listener, 71–72
- commands. *See also specific commands*
 - executing, 327–329
 - learning about, 57–58
- Common Vulnerabilities and Exposures (CVE) system, 142
- Common Vulnerability Scoring System (CVSS), 140
- compromised service, exploitation of, 193–194
- computer name, for Windows, 33
- Conficker worm, 90
- configuration file
 - cracking passwords, 212–213
 - downloading, 188–189
- connect function (Python), 83
- connect_ex function (Python), 83
- connect_udp function, 435
- contact information, for client, 3
- continue command (GDB), 370
- copying file, 60
- Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (CCMP), 351
- cp command, 60
- CPUs, registers in Intel-based, 362–363
- crashes, 151
 - attempting with fuzzing, 424–426
 - causing, 382–384
 - in GDB, 372–373
 - in War-FTP, 397–398, 403

- CRC-32 (Cyclic Redundancy Check 32), 346
- CreateThread API, 271
- Credential Harvester Attack Method, 251–252
- credentials, 174
 - brute force to find, 198
 - for FTP server, 160
 - gathering, 292–294
 - in Nessus, 137
 - stealing stored, 294
- cron jobs
 - automating tasks with, 72–73
 - creating, 311
- crontab files, 72
- cross-site request forgery (CSRF), 335
- cross-site scripting (XSS), 329–335
 - checking for reflective vulnerability, 330
 - leveraging with BeEF, 331–335
- Crunch tool, 201
- CSRF (cross-site request forgery), 335
- Ctypes library (Python), 271
- custom cross compiling, 266–269
- cut command, 65, 80
- CVE (Common Vulnerabilities and Exposures) system, 142
- CVE-2008-2992, 225–228
- CVSS (Common Vulnerability Scoring System), 140
- Cyclic Redundancy Check 32 (CRC-32), 346
- cyclical pattern, generating to
 - determine offset, 385–388

D

- data execution prevention (DEP), 364, 441
- data manipulation, in Kali Linux, 64–66
- database
 - dumping with SQLMap, 322
 - exploiting access to, 188
 - finding name of first, 321
 - for SPF, 448–449
- debugger, installing, 46
- debugging information, for GDB, 366
- default gateway, 68
 - ARP cache poisoning for impersonating, 165–166
 - finding, 38
- default payload, for Metasploit, 97

- default port, for Simple Mail Transfer Protocol (SMTP), 124
- delegation token, 300–301
- deleting
 - files, 60
 - final character from each line, *see* command for, 81
- demilitarized zone, 304
- denial-of-service (DoS) condition, 163
- DEP (data execution prevention), 364, 441
- deploying Android application, 450–451
- Destination Host Unreachable message, 39
- /dev/warandom* file (Linux), 267
- DHCP (dynamic host configuration protocol), 68
- dictionary attack, against WPA/WPA2, 356
- dictionary words, in passwords, 198
- directories
 - changing, 56–57
 - creating, 60
 - displaying current, 56
- disass command (GDB), 370–371
- DNS. *See* Domain Name System (DNS)
- DNS cache poisoning, 167–169
- Dnsspoof, 169
- documentation, 57. *See also* man pages
- domain
 - adding administrator account, 309
 - getting administrative access to, 296
 - setup for simulating, 39–40
 - users, password hashes for, 302
- Domain Name System (DNS)
 - reconnaissance, 116–118
 - zone transfers, 117–118
- domain names, resolution, 167
- domain registrars, 115
- DoS (denial-of-service) condition, 163
- double backslashes (\\), for escape, 186
- downloading
 - 3Com TFTP 2.0.1, 42–43
 - Kali Linux, 10
 - payload by users, 105
 - sensitive files, 188–189
 - SLMail 5.5, 41–42
 - Smartphone Pentest Framework (SPF), 27–28
 - with TFTP, 187–188
 - War-FTP, 46
 - Windows SAM, 189
 - WinSCP, 46

dpkg command, 18
dual-homed systems, 304
dynamic analysis, 261
dynamic host configuration protocol
(DHCP), 68

E

EAX register, 362, 403
EBP register, 362, 363, 369, 390
EBX register, 362
echo command, 61, 76
ECX register, 363
EDI register, 362, 390
editing files, 62–64
EDX register, 363
EIP register, 362, 363
 controlling, 373–375
 locating, 384–388
 verifying offset, 388–389, 390
else statement, in Bash scripts, 78
email
 searching for addresses, 118–119
 social-engineering attacks
 with, 244
emulator, Android, 449
 setting up, 22–27
 starting, 26–27
encoders, 263–266
encryption key, for Syskey utility, 189
end, in Ruby, 434
endianness, 376–378, 394
enterprise connection process, in
 WPA/WPA2, 351
escape, double backslashes (\\)
 for, 186
ESI register, 362
ESP register, 362, 363, 390–391
 following on stack, 408–409
 /etc/crontab file, 72–73, 311
 /etc/john/john.conf file, 212
 /etc/network/interfaces file, 68–69
 /etc/proxychains.conf configuration
 file, 307
Ettercap
 installing, 22
 for man-in-the-middle attacks, 171
exceptions. *See* structured exception
 handler
executables
 embedded in PDF, 228–229
 Hyperion for encrypting, 269–270
 using return address from, 394

execute (x) permissions, 62
execution
 hijacking as goal, 373
 hijacking in Linux, 375–376
 hijacking in Windows, 390–395
executive summary of report, 5
exploit code, repositories of, 88
exploit command (Metasploit), 97
Exploit Database, 88, 427
exploit target, for Metasploit, 95
 exploit/multi/browser/java_signed_applet
 module, 233–234
exploitation, 179–196
 of buffer overflow in third-party
 software, 190–191
 with client-side attacks, 218–239
 of compromised service, 193–194
 with Java, 230–235
 mitigation techniques, 439–442
 of MS08-067 vulnerability,
 180–182
 of open NFS shares, 194–196
 phase of penetration testing, 2, 4
 of phpMyAdmin, 186–188
 running through pivot, 306–307
 of third-party web applications,
 191–193
 of WebDav default credentials,
 182–183
Exploit::Remote::UDP mixin, 435
exploits
 porting public, 427–432
 replacing shellcode, 430
 running, 100
 running through SPF agent, 468
 with SEH overwrites, 403–407
 writing, 361
 exploit/windows/fileformat/adobe_pdf_
 embedded_exe module, 228
 exploit/windows/fileformat/adobe_utilprintf
 module, 226
 exploit/windows/fileformat/winamp_maki_
 bof module, 238
 exploit/windows/local/ms11_080_
 afdjoinleaf module, 284
 exploit/windows/smb/psexec module, 296
 exploit/windows/tftp/tftpd32_long_
 filename.rb module, 435
external penetration test, 2
Ez7z program, 10

F

- Facebook, 172
- factory restore, 456
- fake authentication, 347–348
- file permissions, 61–62
- filename for exploit, random characters for, 438
- files
 - adding text, 61
 - copying, moving, and removing, 60
 - creating, 60
 - editing, 62–64
 - searching for text in, 65
 - sending script results to, 81
 - viewing list of, 18
- FileZilla server.xml* configuration file, 188–189
- FileZilla services, installing, 44
- filters, bypassing with Metasploit payloads, 216–218
- finding
 - attack string in memory, 408–411
 - compatible payloads, 96–97
 - return address, 429–430
 - valid usernames, 153
- firewalls, intrusion-detection and prevention systems on, 125
- folders, sharing via FTP, 45
- for loop, in Bash scripts, 78–79
- formats, for Nmap log, 125
- four-way handshake, 351, 352–353
 - capturing, 354
 - Wireshark for viewing, 355
- Framework Android App, 451
- FSTENV instruction, 398
- FTP account, default password for, 213
- FTP server
 - access to file on, 146–147
 - exploiting stack-based buffer overflow in, 379–380
 - logging in to, 157, 165
- FTP user, adding, 45
- futuresoft_transfermode.rb* module, 432–434
- fuzzing, 421–426
 - attempting crash, 424–426
 - finding bugs with code review, 422
 - for trivial FTP server, 422–423

G

- GCC (GNU Compiler Collection), 84, 289, 366
 - gcc command, 289
 - GDB (GNU debugger), 366
 - crashing program in, 372–373
 - running, 367–372
 - viewing source code, 368
 - getsystem command (Meterpreter), 283–286
 - getuid command (Meterpreter), 185, 279, 281
 - GNU Compiler Collection (GCC), 84, 289, 366
 - GNU debugger. *See* GDB (GNU debugger)
 - Google Play apps, signature for, 462
 - Google search, on vulnerability, 142
 - GoToMeeting, Java for, 241
 - grep command, 65
 - filtering script output, 80
 - greppable Nmap, 125
 - group, permissions for, 62
 - group transient key (GTK), 352
- ## H
- handler, closing, 228
 - Hardware dialog, 31
 - hashdump command (Meterpreter), 204, 205, 298
 - hashes
 - converting to plaintext, 203
 - for domain users, 302
 - dumping with physical access, 206–208
 - example, 211
 - LM vs. NTLM algorithms, 208
 - rainbow table for precompleted, 213
 - recovering from Windows SAM files, 204–206
 - reversing, 203, 298
 - heap in memory, 362
 - “Hello World” C program, 84
 - help
 - for Meterpreter commands, 278
 - for Msfcli, 101
 - for Msfconsole, 89–90
 - help upload command (Meterpreter), 279
 - hidden directories, ls command to show, 57–58

- hook.js* script (BeEF), 332–333
- host utility for DNS queries, 117
- host-only network, 13, 117
- HTML, for attack email, 254
- HTTP GET request, capture by Burp
 - Proxy, 316
- HTTP payload, 217–218
 - exploiting Java vulnerability with, 231–232
- HTTPS, 174
 - payloads, 217–218
- hub, and traffic capture, 156
- Hydra, guessing usernames and passwords with, 202–203
- Hyperion
 - encrypting executables with, 269–270
 - installing, 21, 270

I

- Iceweasel browser, proxy configuration, 315–316
- ICMP (Internet Control Message Protocol) message, 76
- if statement
 - Bash, 77–78
 - C, 84
 - Python, 83
- ifconfig command, 16, 67, 304–305
- IIS (Internet Information Services), user privileges, 329
- Immunity Debugger, 381–382
 - installing, 46–47
- #include command (C), 84
- Incognito tool, 301–302
- incoming connection, listening on port for, 70
- info command (Metasploit), 92–93
- information-gathering phase of penetration testing, 2, 4, 113–132
 - local, 291–296
 - on mobile device, 464–465
 - open source intelligence (OSINT), 114–123
- initialization vector (IV), 344
 - generating with ARP request relay attack, 348–349
- inline payloads, 181
- input, > symbol for redirecting, 61
- input function (Python), 82
- insert mode for vi, 64
- installed packages, managing, 66
- installing
 - 3Com TFTP 2.0.1, 42–43
 - Adobe Acrobat Reader, 46
 - Android emulators, 22–27
 - Apache, 44
 - APKTool, 462
 - debugger, 46
 - Ettercap, 22
 - FileZilla services, 44
 - Hyperion, 21, 270
 - Immunity Debugger, 46–47
 - Java 7 Update 6, 52
 - Microsoft Security Essentials, 52
 - Ming C Compiler, 20
 - Mona, 47
 - Mozilla Firefox, 52
 - MySQL, 44
 - Nessus, 17–20
 - Python, 46
 - SLMail 5.5, 41–42
 - Smartphone Pentest Framework (SPF), 27–28
 - Veil-Evasion, 21
 - VMware, 9–10
 - vulnerable software, 40–47
 - War-FTP, 46
 - Winamp version 5.55, 52
 - WinSCP, 46
 - XAMPP 1.7.2, 43–45
- Intel-based CPU registers, 362–363
- internal penetration test, 2
- Internet access, testing for Kali Linux, 17
- Internet Control Message Protocol (ICMP) message, 76
- Internet Explorer, vulnerability, 220–222
- Internet Information Services (IIS), user privileges, 329
- Internet Protocol (TCP/IP) Properties dialog, 39
- iOS, approach to preventing malicious code, 441
- IP address, 67–68
 - DNS mapping to, 167–168
 - mapping to MAC address, 161
 - setting static, 38–39
 - verifying, 16
- IP forwarding, 163–164
- ipconfig command, 38
 - output from, 328

- iPhone
 - default SSH login, 453–454
 - jailbreaking, 219, 441
 - running application on, 441
 - IV (initialization vector), 344
 - generating with ARP request relay attack, 348–349
 - iwconfig command, 340–341
 - iwlist wlan0 scan command, 341
- J**
- Java, signed Applet, 233–235
 - Java 7 Update 6, installing, 52
 - Java Applet Attack Method, 250
 - Java Runtime Environment (JRE), 230
 - java/meterpreter/reverse_http* payload, 231
 - JMP ESP instruction, 392
 - finding in *USER32.dll*, 429
 - reliance on location, 440
 - John the Ripper tool, 210–211, 303
 - wordlists, 200, 212
 - JRE (Java Runtime Environment), 230
- K**
- Kali Linux, 55–73
 - booting, 11
 - command line, 56
 - data manipulation in, 64–66
 - GUI, 13
 - opening virtual machine, 11
 - repository of exploit code, 288
 - running Android emulators, 27
 - setup, 10–28
 - starting Burp Suite in, 314
 - testing Internet access for, 17
 - user privileges, 58–61
 - kaliinstall* script, 28
 - keyscan_dump command
 - (Meterpreter), 292
 - keyscan_start command
 - (Meterpreter), 292
 - key-scheduling algorithm, in WEP, 345
 - keyspace brute-forcing, 201
 - kill command (Metasploit), 222
 - Kismet, 356
- L**
- LAN manager (LM) password
 - hashes, 208
 - insecurity of, 209
 - lateral movement, 296–304
 - Incognito tool, 301–302
 - PSEXec technique, 296–297
 - SMB capture, 302–304
 - SSH Exec, 299–300
 - token impersonation, 300–301
 - LHOST, 99–100
 - setting, 184
 - setting in Msfvenom, 104
 - license key, for Windows, 32
 - Linksys WRT54G2, web interface, 340
 - Linux. *See also* Kali Linux, Ubuntu 8.10
 - target machine
 - adding code to */tmp/run* file, 290–291
 - copying and compiling exploit, 289–290
 - cracking passwords, 212
 - filesystem, 56–57
 - finding an exploit, 288–289
 - finding a vulnerability, 287–288
 - learning kernel version, 287
 - stack-based buffer overflow in, 361–378
 - udev privilege escalation, 287–291
 - VMware Player for, 9–10
 - listener
 - pushing command shell back to, 71–72
 - setup on Kali Linux, 290
 - list_tokens command
 - (Meterpreter), 301
 - little-endian architecture, 377
 - LM (LAN manager) password
 - hashes, 208
 - insecurity of, 209
 - load command (Meterpreter), 301
 - local file inclusion, 324–327
 - local information gathering, 291–296
 - local privilege escalation, 283–291
 - for Windows, 284–285
 - Local Security Authority Subsystem Service (LSASS)
 - process, 214
 - local users, listing all, 294
 - login screen
 - for Kali Linux, 12
 - of web application, SQL injection issues in, 319–320
 - LPORT option, 216
 - ls command, 18, 56
 - man page for, 57

LSASS (Local Security Authority
Subsystem Service), 214
lsb_release command, 287

M

MAC (Media Access Control) address,
mapping IP address to, 161
MAC filtering, by access points, 350
Mac OS, and VMware Fusion, 10, 16,
31–32, 36
mail servers
for delivering attack email, 248–249
valid usernames for, 153
main function, 84
malicious code, asking users to
allow, 233
Maltego, 119–123
malware, techniques to avoid detection,
257–275
man-in-the-middle attacks, 160–161
Ettercap for, 22, 171
man ls command, 57
man pages, 57–58
mandatory code signing, 219, 441–442
manual port scanning, 124
mapping IP address, to MAC
address, 161
mass email attacks, 253–255
MD5 collision attack, 260
MD5 hash
brute forcing, 212
checking for trojans with, 260
md5sum program, 260
MDM (Mobile Device
Management), 466
Media Access Control (MAC) address,
mapping IP address to, 161
memory
content display options, 369
finding attack string in memory,
408–411
theory of, 362–364
memory address, byte order in, 376
message integrity code (MIC), 353
Metasm utility, 398–399
Metasploit
adding route in, 305–306
auxiliary module and exploit
database, 91
exploit check functions, 147–148
killing background job in, 222

modules, 89, 281–283. *See also*
specific modules
advanced parameters, 223–225
auxiliary, 107–108
database, 90–91
finding, 90–94
MS08-067, 90
post-exploitation, 281–283
scanner, 146–147
setting options, 94–96
verifying format
specifications, 438
writing, 432–439
Msfconsole for, 89
payloads, 96–98
bypassing filters with, 216–218
port scanners in, 306
search function, 91–94
starting, 88–90
support for encoders, 263
test run, 97–98
updating, 108
Metasploit Browser Exploit Method, 250
Meterpreter, 181–182
help for commands, 278
keylogger, 292
for post-exploitation, 278–280
scripts, 280–281
searching for files with, 291–292
session, 98
maintaining, 222
placing in background, 311
running scripts in, 223
shell command for dropping out
of, 287
upload command, 279
MIC (message integrity code), 353
Michael, MAC algorithm, 350
Microsoft Security Essentials, 261–262
installing, 52
non-detection of malware, 270
Microsoft Windows. *See* Windows
Ming C Compiler, installing, 20
Mingw32 cross compiler, 268
Mitnick, Kevin, 243
mkdir command, 60, 207
mobile browser, attack for opening link
in, 455
Mobile Device Management
(MDM), 466

- mobile hacking, 445–472
 - client-side attacks, 454–457
 - malicious apps, 458–463
 - near field communication (NFC), 446–447
 - pivoting through devices, 466–470
 - port scanning with Nmap, 467–468
 - privilege escalation, 471
 - remote attacks, 453–454
 - remote control, 465–466
 - with text messages, 446
 - Mobile Safari, 219
 - Mode field in TFTP, 423
 - modules. *See* Metasploit: modules
 - Mona
 - finding pattern offsets in, 387–388
 - generating cyclical pattern in, 385–388, 405
 - installing, 47
 - running SEH command in, 413
 - `!mona findmsp` command (Immunity Debugger), output, 390
 - `mona pattern_create` command (Immunity Debugger), 404–405
 - `mona.py` file, downloading, 46
 - moving files, 60
 - Mozilla Firefox, installing, 52
 - MS08-067 vulnerability, 180–182
 - Msfcli (command line interface), 89, 101–103
 - showing options, 101–102
 - SPF to interface with, 453
 - Msfconsole, 89
 - handler for catching payload, 185
 - `help` command for, 89–90
 - setting up handler, 469
 - Msf tidy tool, 438
 - `msfupdate` command, 108, 225, 438
 - Msfvenom, 258–259
 - creating standalone payloads with, 103–107
 - encoders, 264
 - generating shellcode, 273–274, 396, 428
 - multiencoding with, 265
 - output format for, 104–105
 - prebuilt templates for detection signatures, 266
 - serving payloads, 105, 183–185
 - `multi/handler` module, 105–107, 227, 469
 - `multi/ssh/sshexec` module, 299
 - multipronged attacks, 255
 - `mv` command, 60
 - MySQL
 - database, for SPF, 447
 - installing, 44
 - server, privileges, 186
- ## N
- nano (file editor), 62–63
 - NAT (network address translation), 13
 - National Institute of Standards and Technology (NIST), 141
 - near field communication (NFC), 446–447
 - negative feedback, 173–174
 - Nessus (Tenable Security), 134–142
 - credentials in, 137
 - detailed information on vulnerability, 140
 - exporting results, 141–142
 - installing, 17–20
 - login screen, 20–22, 135
 - Policies tab, 134–138
 - rankings, 140–141
 - scanning with, 138–140
 - starting, 18
 - `net` command (Windows), 294–295
 - `net localgroup` command (Windows), 295, 309
 - `net use` command (Windows), 303
 - `net user` command (Windows), 309
 - `net users` command (Windows), 294–295
 - Netcat tool
 - to check for listening port, 70
 - connecting to port with, 152
 - for file transfer, 72
 - for SMTP port connection, 124
 - for TCP/IP connections, 69–72
 - Netcraft, 114–115
 - `netstat` command, 69
 - network
 - for capturing traffic, 156
 - connecting virtual machine to, 16–17
 - managing, 67–69
 - viewing connections, 69
 - network adapter
 - changing settings, 15
 - configuring for Windows XP, 31
 - network address translation (NAT), 13
 - Network File System (NFS), 144–145
 - exploitation of open shares, 194–196

- network interface, 67
 - adding second, 52
- network mask, 68
- NFC (near field communication), 446–447
- NFS (Network File System), 144–145
 - exploitation of open shares, 194–196
- Nikto, 149
- NIST (National Institute of Standards and Technology), 141
- Nmap port scanning, 125–131
 - for mobile devices, 467–468
 - running through ProxyChains, 308
 - scanning a specific port, 130–131
 - SYN scan, 125–127
 - UDP scan, 128–130
 - version scan, 127–128
- Nmap Scripting Engine (NSE), 142–144
 - default scripts output, 143–144
 - running single script, 144–146
- nondisclosure agreement, 4
- NOP sled, 428–429
- NSE. *See* Nmap Scripting Engine (NSE)
- nslookup, 116–117, 167
- NT LAN Manager (NTLM) hash, for
 - password hash, 208
 - cracking with John the Ripper, 210–211

O

- offset
 - generating cyclical pattern to determine, 385–388
 - verifying, 388–389, 390
- Opcode field, in TFTP, 423
- open relay, 249
- open source intelligence (OSINT), 4
 - DNS reconnaissance, 116–118
 - Maltego, 119–123
 - Netcraft, 114–115
 - port scanning, 123–131
 - searching for email addresses, 118–119
 - whois lookups, 115–116
- Open Sourced Vulnerability Database (OSVDB), 149
- Open Web Application Security Project (OWASP), 335
- open wireless network, 343
- OSINT. *See* open source intelligence

- OSVDB (Open Sourced Vulnerability Database), 149
- output format, for Msfvenom, 104–105
 - overflowtest.c* file, functions in, 375
- OWASP (Open Web Application Security Project), 335
- owner, permissions for, 62

P

- pack method (Ruby), 435
- packages, managing installed, 66
- Packet Storm Security, 88
- pairwise master key (PMK), in WPA/WPA2, 352
- pairwise transient key (PTK), 352
- pass the hash technique, 298–299
- passphrase, for WPA or WPA2, 353
- password attacks, 197–214
 - offline, 203–213
 - online, 198–203
- password hashes
 - converting to plaintext, 203
 - for domain users, 302
 - dumping with physical access, 206–208
 - example, 211
 - LM vs. NTLM algorithms, 208
 - recovering from Windows SAM file, 204–206
 - reversing, 203, 298
- passwords
 - cracking with John the Ripper, 210
 - cracking Linux, 212
 - default root for SSH, 453
 - dumping plaintext with WCE, 213–214
 - guessing with Hydra, 202–203
 - lists of, 199–201
 - managing, 197–198
 - for Nessus, 20
 - online services for cracking, 213
 - recovering MD5 hashes, 188
 - saving, 293
 - setting in Windows 7 target machine, 49
 - setting in Windows XP, 37
 - strong, 198
 - system hashes, 194
 - use of same on multiple systems, 296
- PATH environmental variable, 77
- pattern matching, with awk, 66

- paused process, Immunity Debugger
 - and, 381–382
- payloads, 180–181
 - avoiding special characters, 396
 - creating standalone with Msfvenom, 103–107
 - handler for, 227
 - listing in Msfvenom, 104
 - in Msfcli, 102–103
 - servicing, 105
 - setting manually, 99–101
 - for structured exception handler overwrite, 418–419
- payment terms, 3
- PBKDF2 hashing algorithm, 352
- PDF (Portable Document Format)
 - software, exploitation with, 225–235
- penetration testing
 - basics, 1–2
 - data, tracking, 125–126
 - stages, 2–6
- Penetration Testing Execution Standard (PTES), 2
- Perl scripting language
 - for creating argument string, 376
 - string generation by, 372
- persistence, 309–311
 - persistence* script (Meterpreter), 310–311
- personal connection process, in WPA/WPA2, 351
- phishing attack, 244
 - via email, automating, 253
- phpMyAdmin, 149–150
 - exploitation, 186–188
- ping command, 17, 38
 - limiting number of times, 78
 - stopping, 39
- ping sweep, script for, 76
- pipe (|), 65
- pivoting, 304–308
 - through mobile devices, 466–470
 - Socks4a and ProxyChains, 307–308
- plaintext
 - converting hashes to, 203
 - for credentials, 174
 - dumping passwords with Windows Credential Editor, 213–214
- PMK (pairwise master key) in WPA/WPA2, 352
- POP instruction, 363, 411–412
 - reliance on location, 440
- port 4444, 98
- port scanning, 123–131
 - manual, 124
 - in Metasploit, 306
 - with Nmap, 125–131, 467–468
 - with Python script, 82
- Portable Document Format (PDF)
 - software, exploitation with, 225–235
- porting public exploits, 427–432
- ports, 69, 95
 - default, for Simple Mail Transfer Protocol (SMTP), 124
 - exploring, 151–152
 - Netcat for connecting to, 152
 - Nmap port scanning for specific, 130–131
- post-exploitation phase of penetration testing, 2, 4–5, 277–311
 - gathering credentials, 292–294
 - keylogging, 292
 - lateral movement, 296–304
 - local information gathering, 291–296
 - local privilege escalation, 283–291
 - Metasploit modules, 281–283
 - Meterpreter for, 278–280
 - mobile, 463–471
 - modules, 281–283
 - persistence in, 309–311
 - pivoting, 304–308
- PostgreSQL database, 88
- post/windows/gather/enum_logged_on_users*
 - module, 282
- post/windows/gather/hashdump*
 - module, 298
- Powershell, in Windows 7, 329
- pre-engagement phase of penetration testing, 2–4
- print command
 - Perl, 372
 - Python, 83
- printf function, 84
- private SSH keys, 194
- privilege escalation, in mobile devices, 470–471
- privileged commands, running, 59
- PRNG (pseudorandom number generator), 267, 345
- processes, 67
 - Immunity Debugger and paused, 381–382

- programming, 75–85. *See also* Bash scripts; Python
 - breakpoints in, 368
 - C programs, 84–85
 - Ruby, for Metasploit modules, 432
- proprietary data, loss of, 2
- protocol analyzer. *See also* Wireshark
- ProxyChains, 307–308
- ps aux command, 290
- ps command (Meterpreter), 67, 295
- PSEXEC technique, 296–297, 298
- pseudorandom number generator (PRNG), 267, 345
- PTES (Penetration Testing Execution Standard), 2
- PTK (pairwise transient key), 352
- public exploits
 - porting, 427–432
 - risks of working with, 142
- public SSH key, 194
- publisher, trusted vs. unknown, 235
- PUSH ESP instruction, 393
- PUSH instruction, 363, 411
- pwd command, 56
- Python, 81
 - connecting to a port, 83
 - Ctypes library, 271
 - if statements, 83
 - installing, 46
 - porting exploit, 436
 - variables in, 82
 - VirtualAlloc injection, 271
- Python-generated executables, creating
 - encrypted with Veil-Evasion, 270–274

Q

- QR (quick response) codes, 447
- query, Wireshark capture of, 166

R

- RADIUS (Remote Authentication Dial-In User Service)
 - server, 351
- Radmin Viewer program, trojan
 - and, 259
- radmin.exe* binary, embedding payload
 - inside, 259
- Railgun, 283
- rainbow tables, 213
- random variable, 267
- randomize_va_space, 364–365
- rand_text_english function (Metasploit), 435, 438
- Rapid7, 87
- raw_input function (Python), 82
- RC4 (Rivest Cipher 4) stream cipher, 343
- Rcrack tool, 213
- read (r) permissions, 62
- Ready to Create Virtual Machine
 - dialog, 30
- redirecting input, > symbol for, 61
- reflective DLL injection, 181
- reflective XSS attacks, 329
 - checking for vulnerability, 330
- registers
 - in Intel-based CPU, 362–363
 - jumping to, 392
- relative path, 56
- remote attacks, 453–454
- Remote Authentication Dial-In User Service (RADIUS)
 - server, 351
- remote control
 - of mobile devices, 465–466
 - USSD, 456–457
- remote file inclusion, for web
 - application testing, 327
- remote system
 - logging into, 298
 - pinging, 76
- removing files, 60
- reporting phase of penetration testing, 2, 5–6
- researching vulnerabilities, 142
- resource exhaustion attack, 471
- RET instruction, 411–412
 - reliance on location, 440
- return address, 363
 - finding, 429–430
 - using from executable module, 394
- return statement (C), 85
- return-oriented programming (ROP), 441
- rev2self command (Meterpreter), 284
- reverse shells, 71, 98–99, 180
- reverse_https_proxy* payload (Meterpreter), 218
- RHOST option, for Metasploit module, 94–95
- risk profile, 5
- risks of public exploit code, 88

- Rivest Cipher 4 (RC4) stream cipher, 343
- rm file command, 60
- rockyou.txt.gz file, 200
- root privileges, 56, 194, 287–291
- root@kali# prompt, 56
- ROP (return-oriented programming), 441
- route command (Metasploit), 68, 305–306
- router, for wireless traffic, 339
- RPORT option, for Metasploit module, 95
- RtlMovememory API, 271
- Ruby, for Metasploit modules, 432
- run migrate command (Meterpreter), 280
- running processes, viewing, 67

S

- SafeSEH, 412–416
- SAM (Security Accounts Manager) file
 - downloading, 189
 - recovering password hashes from, 204–206
- Samdump2, 205
- saving
 - passwords, 293
 - text to file, 61
- SCADA systems, 131
- scanner/portscan/tcp module, 306
- scanning
 - legality of, 124
 - with w3af, 335–337
 - web application, 148–151
- scope of pentest, 3
- scripts. *See also* Bash scripts; Python
 - running automatically, 72
 - running in Meterpreter, 223
 - running on target web server, 183
- search command (Meterpreter), 291–292
- searching
 - Metasploit auxiliary module and exploit database, 91
 - for text, 63
- searchsploit utility, 288
- Secure Socket Layer (SSL) attacks, 170–172
 - stripping attacks, 173–174
- Security Accounts Manager file. *See* SAM (Security Accounts Manager) file

- security updates, turning off
 - automatic, 34
- SecurityFocus.com, 88, 380, 427
- sed command, 65
 - to delete final character from each line, 81
- SEH chain, 401
 - viewing, 402
- SEH overwrites. *See* structured exception handler overwrites
- SEH registration record, 401
- Select Guest Operating system dialog, 29
- self-signed SSL certificates, social engineering tests with, 173
- sensitive files, downloading, 188–189
- service command, 67
- services, 67
- session, bringing to foreground, 283
- SET (Social-Engineer Toolkit), 235, 244–245
 - spear-phishing attacks, 245–250
- set payload command (Metasploit), 99
- setoolkit command, 245
- shell command, for dropping out of Meterpreter, 287
- shell scripts, 75
- shellcode
 - Msfvenom for generating, 273–274, 428
 - replacing, 430
- shellcode variable, in custom C code, 267
- shells, 395–400
 - closing, 100
 - types of, 98–99
- shikata_ga_nai encoder, 264
- short jump assembly instruction, 416–417
- show advanced command (Metasploit), 223
- show options command (Metasploit), 94, 96, 99
- show payloads command (Metasploit), 96–97, 180, 190–191, 216–218
- show targets command (Metasploit), 95–96, 234
- signatures
 - for antivirus applications, 438
 - for apps, 462
- signed Java Applet, 233–235

- Simple Mail Transfer Protocol (SMTP),
 - default port for, 124
- skins in Winamp, malicious code in, 239–240
- slash (/), as delimiter character in
 - sed, 65
- SLMail 5.5, downloading and installing, 41–42
- Smartphone Pentest Framework (SPF), 445, 447–452
 - Android emulators, 449
 - attaching app, 452
 - attaching to deployed agent, 460–461
 - attaching mobile modem, 449
 - backdooring APKs, 461–464
 - building Android app, 449–450
 - creating malicious agents, 458–463
 - downloading and installing, 27–28
 - running exploit through agent, 468
 - setting up, 447–449
 - starting, 448
- SMB capture, 302–304
- SMBPIPE option, for Metasploit
 - module, 95
- SMS, for spam and phishing attacks, 446
- SMTP (Simple Mail Transfer Protocol),
 - default port for, 124
- Social-Engineer Toolkit (SET), 235, 244–245
 - spear-phishing attacks, 245–250
- social engineering, 243–255
 - mass email attacks, 253–255
 - multipronged attacks, 255
 - tests, with self-signed SSL certificates, 173
 - web attacks, 250–252
- socket library, 82
- Socks4a, 307–308
- software
 - installing vulnerable, 40–47
 - investigating running, for vulnerabilities, 295
 - user account for, 58
 - versions in banners, 124
- source code, backdooring, 458–461
- spear-phishing attacks, 245–250
 - choosing a payload, 246–247
 - listener setup, 249–250
 - naming malicious file, 247
 - setting options, 247
 - setting target, 248–249
 - single vs. mass email, 247–248
 - template for, 248
- special characters, avoiding for
 - payload, 396
- Specify Disk Capacity dialog, 30
- SPF. *See* Smartphone Pentest Framework (SPF)
- SQL commands, executing, 186
- SQL injection, 319–322
- SQLMap, 321–322
- SRVHOST option, 220
- SSH, default root password, 453
 - .ssh directory, 194
 - vulnerability from access, 145–146
- SSH Exec, 299–300
- SSH key pair, generating, 195
- ssh-add command, 195
- ssh-keygen command, 195
- SSL (Secure Socket Layer) attacks, 170–172
 - stripping attacks, 173–174
- SSL certificate, warning of invalid, 19
- SSLstrip, 173–174
- stack, 362, 363
 - following ESP register on, 408–409
 - as last-in, first-out (LIFO) structure, 411
- stack-based buffer overflow in Linux, 361–378
 - C program vulnerable to, 365–366
 - causing crash, 366–367, 372–373
 - EIP register control, 373–375
 - hijacking execution, 375–376
- stack-based buffer overflow in
 - Windows, 379–400
 - causing crash, 382–384
 - getting shell, 395–400
 - hijacking execution, 390–395
 - locating EIP register, 384–388
 - searching for known vulnerability in War-FTP, 380–382
- stack buffer, 379
- stack cookies, 439–440
- staged payloads, 181
- static analysis, 260
- static IP address
 - setting, 38–39, 68–69
 - for Windows 7 target machine, 51
- stdio* library (C), 84
- stealing stored credentials, 294
- stopping keylogger, 292
- stored XSS attacks, 329

- strategic road map, 6
- strcpy function, 366–367, 422
- string, generating with Perl script, 372
- strong passwords, 198
- structured exception handler (SEH)
 - overwrites, 401–419
 - choosing payload, 418–419
 - exploits, 403–407
 - finding attack string in memory, 408–411
 - replacing with POP POP RET, 414, 415
 - SafeSEH, 412–416
 - short jump assembly instruction, 416–417
- structured exception handler, passing control to, 407–408
- su command, 59–60
- sudo command, 59
- sudoers file, 59
- superuser (root) prompt, 16
- switches, and traffic capture, 156
- SYN scan, 125–127
- Syskey utility, encryption key for, 189, 205
- system() command (PHP), 186
- system password hashes, 194
- system privileges, session running with, 297

T

- Tabnabbing Attack Method, 251
- target virtual machines, 28–29. *See also*
 - Windows 7 target machine,
 - Windows XP target machine,
 - Ubuntu 8.10 target machine
- TCP connection
 - creating socket, 82
 - Netcat tool for, 69–72
 - three-way handshake, 125
- TCP scan, 127
- TCP stream, Wireshark for
 - following, 159
- technical report, 6
- Temporal Key Integrity Protocol (TKIP), 350
- Tenable Security, Nessus, 17, 134–142
- testing window, 3
- text
 - adding to file, 61
 - searching for, 63, 65
- text messages, mobile hacking with, 446
- text segment of memory, 362

- TFTP (Trivial FTP) server
 - downloading file with, 187–188
 - fuzzing program, 424–426
 - packet, 435
 - packet format, 423
 - writing to file, 438
- Thawte (certificate authority), 171
- theHarvester (Python tool), 118–119
- then statement, in Bash scripts, 78
- third-party software, exploiting buffer overflow in, 190–191
- third-party web applications, exploitation, 191–193
- threat-modeling phase of penetration testing, 2, 4
- TikiWiki CMS software, 191–192
- TKIP (Temporal Key Integrity Protocol), 350
- TLS (Transport Layer Security) encryption, 181
- /tmp/run file (Linux), adding code to, 290–291
- token impersonation, 300–301
- touch command, 60
- tr utility (Linux), 267
- training employees, about social engineering, 244
- Transport Layer Security (TLS) encryption, 181
- Trivial FTP server. *See* TFTP (Trivial FTP) server
- trojans, 258–259
 - MD5 hash to check for, 260
- TrustedSec, Social-Engineer Toolkit, 244
- two-factor authentication, 198

U

- UAC (user account control), 285–287
- Ubuntu 8.10 target machine, 28. *See also* Linux
 - setup, 48
- udev (device manager for Linux), 288
- UDP scans, 128–130, 295
- UDP socket, setting up, 435
- uname command, 287
- unstructured supplementary service data (USSD), 456–457
- upload command (Meterpreter), 279
- uploading, Msfvenom payload, 183–185
- URIPATH option, 221

- user account control (UAC), 285–287
- user accounts
 - adding, 58–59
 - adding, persistence and, 309
 - adding to sudoers file, 59
 - creating in Windows, 35, 48–49
 - in Linux, 58
 - for logging in to FTP, 165
 - switching, 59–60
- user lists, 199
- user password. *See* passwords
- user privileges, 58–61
- USER32.dll*, 429–430
- usernames
 - finding, 118
 - finding valid, 153
 - guessing with Hydra, 202–203
- users. *See also* social engineering
 - downloading payload by, 105
 - enticing to download and install
 - Android agent, 460
 - listing all local, 294
 - logging keystrokes by, 292
 - sending messages to contacts, 465
 - /usr/share/exploitdb/platforms/linux/local/8572.c* exploit, 288–289
 - /usr/share/metasploit-framework/modules/post/windows/gather/credentials* module, 292
- USSD (unstructured supplementary service data), 456–457

V

- variables, in Python, 82
- Veil-Evasion, 270–274
 - available payloads, 272
 - installing, 21
 - Python VirtualAlloc in, 273
- VeriSign (certificate authority), 171
- version scan, 127–128
- Very Secure FTP (Vsftpd) 2.3.4, 133–134, 193–194, 258
- vi (file editor), 62
 - editing file, 63
- virtual lab setup, 9–54
 - installing VMware, 9–10
 - installing vulnerable software, 40–47
 - Kali Linux setup, 10–28
 - target virtual machines, 28–29
 - Ubuntu 8.10 target machine, 48

- Windows 7 target machine, 48–54
- Windows XP target machine, 29–40
- Virtual Machine Settings dialog, 15
- virtual machines
 - configuring network for, 13–17
 - connecting to network, 16–17
 - to delay booting, 207
 - target, 28–29
- virtual networks, and traffic
 - capture, 156
- VirtualAlloc injection method, 271
- VirusTotal, 262–263
 - results for encoded binary, 265
- VMware, installing, 9–10
- VMware Fusion (Mac OS), 10, 16, 31–32
 - installing VMware Tools for, 36
- VMware Player (Windows), 9–10, 14–15, 35–36
 - installing Windows XP on, 29–31
- VMware Tools
 - installing on Windows XP target machine, 35–36
 - installing on Windows 7 target machine, 48, 50
- VMware Workstation, 10
 - .vmx* configuration file, 207
- VRFY SMTP command, 153
- Vsftpd (Very Secure FTP) 2.3.4, 133–134, 193–194, 258
- vulnerabilities, 133–153
 - in Java, 230–233
 - manual analysis, 151–153
 - researching, 142
 - searching for known, in War-FTP, 380–382
 - web application scanning, 148–151
- vulnerability analysis phase of
 - penetration testing, 2, 4
- vulnerability repository, 149
- vulnerability scanners
 - Nessus Home, 17
 - reasons to use, 141
- vulnerable software, installing, 40–47

W

- w3af (Web Application Attack and Audit Framework), 335–337
- War-FTP
 - crashing, 397–398, 403
 - downloading and installing, 46
 - Python exploit to crash, 383

- War-FTP (*continued*)
 - searching for known vulnerability in, 380–382
 - USER buffer overflow, 439
- warning, for PDF embedded executable, 229
- Warning: system() [function.system]: Cannot execute a blank command in...* message, 187
- WCE (Windows Credential Editor), 213–214
- Web Application Attack and Audit Framework (w3af), 335–337
- web application testing, 313–337
 - with Burp Proxy, 314–319
 - command execution, 327–329
 - cross-site request forgery, 335
 - cross-site scripting (XSS), 329–335
 - local file inclusion, 324–327
 - remote file inclusion, 327
 - scanning with w3af, 335–337
 - signing up for account, 317–318
 - SQL injection, 319–322
 - XPath injection, 323–324
- web applications
 - access to server-side source code, 326
 - third-party, exploitation, 191–193
 - vulnerability scanning, 148–151
- web browsers. *See* browsers
- web server
 - copying app to, 451
 - running script on target, 183
- web server software, system privileges and, 185
- WebDAV (Web Distributed Authoring and Versioning)
 - software, 150
 - exploiting default credentials, 182–183
- WebEx, Java for, 241
- WebKit package, attacking, 454–456
- websites, for wordlists, 200
- WEP. *See* wired equivalent privacy (WEP)
- wget command, 289
- whoami command, 71, 291
- whois lookups, 115–116
- Wi-Fi protected access (WPA), 350
- Wi-Fi Protected Setup (WPS), 356–357
- Wifite tool, 350, 356
- Winamp
 - installing, 52
 - replacing configuration file for, 237–239
- Windows
 - APIs, Railgun for accessing, 283
 - clipboard, stealing data from, 334
 - firewall
 - and response to ping, 51
 - turning off, 37
 - Security Accounts Manager (SAM) file
 - downloading, 189
 - recovering password hashes from, 204–206
 - Service Control Manager, remote procedure call (RPC), 296
 - Syskey utility, 189
 - VMware Player, 9–10, 14–15
- Windows 7 target machine, 48–54
 - adding second network interface, 52
 - bypassing UAC on, 285–287
 - creating user account, 48–49
 - dumping hashes with physical attack, 206–207
 - installing additional software, 52–54
 - opting out of automatic updates, 50
 - Powershell in, 329
 - turning off real-time protection, 53
- Windows 2000, LM hashes storage, 211
- Windows Credential Editor (WCE), 213–214
- Windows XP target machine, 28
 - activating, 34
 - creating, 29–40
 - installing, 32–35
 - LM hashes storage, 211
 - local privilege escalation, 284–285
 - Nessus detection of vulnerabilities, 139
 - setup to behave as member of Windows domain, 39–40
 - windows/local/bypassuac* exploit, 286
 - windows/meterpreter/bind_tcp* payload, 307
 - windows/meterpreter/reverse_tcp* payload, 247, 265, 273–274
 - windows/smb/ms08_067_netapi* module, 306
- WinSCP, 292–294
 - downloading and installing, 46

- wired equivalent privacy (WEP), 343–350
 - challenges, 350
 - cracking keys with Aircrack-ng, 347–350
 - weaknesses, 346
- wireless attacks, 339–357
 - capturing packets, 342–343
 - scanning for access points, 341
 - setup, 339–341
 - viewing available interfaces, 340–341
 - Wi-Fi protected access, 350
 - Wi-Fi Protected Setup (WPS), 356–357
 - wired equivalent privacy (WEP), 343–350
 - WPA2, 351–356
- wireless network
 - monitor mode, 341–342
 - open, 343
- Wireshark, 156–160
 - capturing traffic, 156–158
 - dissecting packets, 160
 - filtering traffic, 158–159
 - following TCP stream, 159
 - for viewing WPA2 handshake, 355
- wordlists for passwords, 199–201
- Workgroup settings, for Windows XP, 33
- WPA (Wi-Fi protected access), 350
- WPA2, 351–356
 - cracking keys, 353–356
 - dictionary attack against, 356
 - enterprise connection process, 351
 - four-way handshake, 352–353
 - personal connection process, 351
- WPS (Wi-Fi Protected Setup), 356–357
- write (w) permissions, 62

X

- x/16xw \$esp command (GDB), 369
- XAMPP
 - Apache, default install location, 186
 - attacking, 149–150
 - default credentials, 150–151
 - default login credentials for WebDav, 182
 - installing, 43–45
 - starting control panel, 43
- XML
 - attacks on, 323–324
 - usernames and passwords in, 326
- Xpath, 320
 - injection, 323–324
- xp_cmdshell() function, 188
- xp_cmdshell stored procedure, 322
- xphashes.txt* file, 210
- XSS (cross-site scripting), 329–335
 - checking for reflective vulnerability, 330
 - leveraging with BeEF, 331–335

Z

- zero-day vulnerability, 220, 240
- Zervit server, 40–41
 - crashes from Nmap scan, 130, 131
- zone transfers, DNS, 117–118