

INDEX

A

- active information gathering, 18–26
- ActiveX control, malicious, 184
- add_group_user command, 89, 279
- Add/Remove Windows Components, *Windows Components Wizard*, 269
- Address Resolution Protocol (ARP), 175–176
- add_user command, 89, 279
- Administrator user account, 83
- Adobe file format exploit, 141, 175
- Adobe Flash, zero-day vulnerability, 110, 146
- advanced service enumeration, 19
- airbase-ng component, 179
 - C 30 option, 179
 - v option, 179
- Aircrack-ng website, 179
- airmon-ng start wlan0 command, 179
- anonymous logins, *scanner/ftp/anonymous*, 29
- antivirus
 - avoiding detection from, 99–108
 - creating stand-alone binaries with *msfpayload*, 100–101
 - encoding with *msfencode*, 102–103
 - using custom executable templates, 105–107
 - using multi-encoding, 103–104
 - using packers, 107–108
 - processes, killing, 282
- APACHE_SERVER flag, 137
- API (application programming interface), for Meterpreter scripts, 241–244
- base API calls, 242
- Meterpreter mixins, 242–244
- printing output, 241–242

- Arduino interface, 159
- armitage*, 11–12
- ARP (Address Resolution Protocol), 175–176
- assembly languages, 216
- attack vectors, 17, 136
- Attempt SQL Ping and Auto Quick Brute Force option, Fast-Track, 169–171
- Aurora attack vector, 146
- Authentication Mode, SQL Server, 270
- autoexploit.rc* file, 73
- Automatic Targeting option, 62
- Automatic Updates option, Windows XP, 269
- Autopwn Automation menu, 164
- autopwn* exploits, 181
- Autopwn tool, using results in, 56
- autorun.inf* file, 157
- auxiliary class, 129
- auxiliary modules, 123–133
 - anatomy of, 128–133
 - defined, 8
 - in use, 126–128
- Auxiliary run method, 31
- Auxiliary::Scanner mixin, 31

B

- back command, 58
- backdoored executable, 106
- background command, 86, 279
- BackTrack
 - downloading, 267–268
 - updating, 272–274
- bad characters
 - avoiding, 13
 - and creating exploits, 210–213
- banner grabbing, 19, 36

- Base64, 102, 189, 193–194
 - binaries, creating with *msfpayload*, 100–101
 - Binary paste option, Immunity Debugger window, 113
 - binary-to-hex generator, Fast-Track tool, 174
 - Binary to Hex Payload Converter, Fast-Track, 174
 - bin/dict/wordlist.txt* file, Fast-Track, 169
 - bind shell, 8, 70
 - bind_tcp format, 113
 - bind_tcp payload, 281
 - blank password, 53, 84
 - Blowfish encryption algorithm, RATTE, 160
 - breakpoint, in Immunity Debugger window, 113
 - browser_autopwn server, 179
 - browser-based exploits, 110–112
 - browser exploit menu, *armitage*, 11–12
 - brute force attack, Apache Tomcat, 260–261
 - brute forcing ports, 71–72
 - buffer overflow exploits, porting to Metasploit, 216–226
 - adding randomization, 222–223
 - completed module, 224–226
 - configuring exploit definition, 219–220
 - implementing features of the Framework, 221–222
 - removing dummy shellcode, 223–224
 - removing NOP Slide, 223
 - stripping existing exploit, 218–219
 - testing base exploit, 220–221
 - Burp Suite, 253
- C**
- captive portal, Karmetasploit, 182
 - check command, 276
 - Check Names button, Login-New window, 272
 - CIDR (Classless Inter-Domain Routing) notation, 22, 44
 - clearev command, 279
 - client.framework.payloads.create(payload) function, 246
 - client-side attacks, 109–121
 - browser-based exploits, 110–112
 - file format exploits, 119–120
 - Internet Explorer Aurora exploit, 116–119
 - sending malicious file, 120–121
 - web exploits, 146–148
 - cmd_exec(cmd) function, 242
 - cmd variable, 188
 - cnt counter, 194
 - code reuse, and modules, 196
 - Collab.collectEmailInfo Adobe vulnerability, 139
 - commands
 - for Meterpreter, 80–82, 277–279
 - keystroke logging, 81–82
 - post exploitation, 282–283
 - screenshot command, 80–81
 - sysinfo command, 81
 - for *msfcli*, 281
 - for *msfconsole*, 275–277
 - for *msfencode*, 280
 - for *msfpayload*, 280
 - command shell, dropping into, 283
 - Common Vulnerabilities and Exposures (CVE) numbers, 42
 - community strings, 30
 - Conficker worm, 59
 - connect command, 9
 - Convert::ToByte, 193
 - copycat domain name, 142
 - covert penetration testing, 4, 5
 - credentialed scan, 43
 - Credential Harvester option, SET main menu, 149
 - credential harvesting, 149, 153–154, 181–182
 - cross-site scripting (XSS) vulnerability, 150
 - C-style output, 12
 - CTRL-C shortcut, 149
 - CTRL-W shortcut, in Nano, 188
 - CTRL-Z shortcut, 86, 97
 - custom scanners, for intelligence gathering, 31–33
 - CVE (Common Vulnerabilities and Exposures) numbers, 42
- D**
- Dai Zovi, Dino, 177
 - databases, working with in Metasploit, 20–25
 - Data Execution Prevention (DEP), 65
 - data/templates/template.exe* template, 105

- db_autopwn command, 56, 277
- db_connect command, 42, 43, 48, 49, 56, 277
- db_create *name* command, 277
- db_destroy command, 43, 49, 277
- db_hosts command, 21–22, 27, 42, 44, 48, 51
- db_import command, 21, 42, 48, 56
- db_nmap command, 24, 277
- db_owner role membership, User Properties window, 272
- db_services command, 25
- db_status command, 20
- db_vulns command, 44, 49
- debug command, 192
- Defcon 18 Hacking Conference, 185
- def exploit line, 191
- def inject function, 238
- def powershell_upload_exec function, 192
- DEP (Data Execution Prevention), 65
- desktop screen captures, 80
- DHCP (Dynamic Host Configuration Protocol) server, 178
- dhcpd.conf* file, 178
- DistCC, 263
- DNS (Domain Name System), 17, 175
- domain administrator token, stealing, 282
- Domain Admins group, 282
- Domain Name System (DNS), 17, 175
- download *file* command, 279
- Drake, Joshua, 79
- drop_token command, 278
- dummy shellcode, 222, 230–231
- dumping password hashes, 83–84
- Dynamic Host Configuration Protocol (DHCP) server, 178
- dynamic memory allocation, 70
- dynamic ports, 168

E

- eb operation code, 209
- egg hunter, 204
- EHL0 command, 219
- EIP (extended instruction pointer) register, 216, 217, 219, 220
- Encase, 265
- EncodedCommand command, 193, 194
- encoders, 13
- endian-ness, 207, 221

- error message, SQL injection, 255
- ESP registers, 216
- ESSID, 179
- /etc/dhcp3/dhcpd.conf/ etc/dhcp3/dhcpd.conf.back* command, 178
- Ettercap, 175
- eventlog_clear(*evt* = "") function, 242
- eventlog_list() function, 242
- event_manager* tool, 265
- evil string, 207
- Excellent ranking
 - Autopwn tool, 56
 - encoders, 13
- exe command, 192
- execute -f *cmd.exe* command, 278
- execute_upload.rb* file, 244
- exploitation, 57–73
 - brute forcing ports, 71–72
 - client-side attacks, 109–121
 - browser-based exploits, 110–112
 - file format exploits, 119–120
 - Internet Explorer Aurora exploit, 116–119
 - sending a malicious file, 120–121
 - creating exploits, 197–213
 - and bad characters, 210–213
 - controlling SEH, 201–203
 - and fuzzing, 198–201
 - getting return address for, 206–210
 - and SEH restrictions, 204–206
 - defined, 8
 - phase of PTES, 3
 - resource files for, 72–73
 - simulated penetration test, 255, 257–260
 - for Ubuntu, 68–71
 - for Windows XP SP2, 64–68
- exploit command, 68, 70, 91, 97, 187, 276
- Exploit Database site, 198
- exploit-db*, to identify potential vulnerabilities, 260
- exploit module, 8
- exploit section, 206
- Exploits Database, 264
- Exploits menu, 164
- explorer.exe* process, 82
- extended instruction pointer (EIP) register, 216, 217, 219, 220
- extracting password hashes, 82–83

F

- false negatives, in vulnerability scans, 36
- false positives, in vulnerability scans, 36
- fasttrack-launching command, 163
- Fast-Track tool, 163–176
 - binary-to-hex generator, 174
 - defined, 79
 - main menu
 - BLIND SQL Injection attacks, 173
 - ERROR BASED SQL Injection attacks, 173
 - Mass Client-Side Attack option, 75
 - Metasploit Meterpreter Reflective Reverse TCP option, 173
 - mass client-side attack, 175–176
 - Microsoft SQL injection with, 164–174
 - manual injection, 167–168
 - MSSQL Bruter, 168–172
 - POST parameter attack, 166–167
 - query string attack, 165–166
 - SQLPwnage, 172–174
 - file exploits
 - file format exploits, 119–120
 - sending a malicious file, 120–121
 - file format vulnerability, 121
 - File Transfer Protocol (FTP)
 - scanning, 29
 - service, 269
 - Find SQL Ports option, Fast-Track, 169
 - fingerprinting targets, 5
 - Follow address in stack option, Immunity Debugger, 201
 - forensics analysis, 264
 - Foursquare credentials, 132
 - Foursquare service, 132
 - FTP (File Transfer Protocol)
 - scanning, 29
 - service, 269
 - FTP (File Transfer Protocol) Service
 - checkbox, 269
 - ftp_version* module, 29
 - Furr, Joey, 163
 - fuzzed variable, 199
 - fuzzers* directory, 124
 - fuzzing, 198–201
 - fuzz string, 199

G

- Gates, Chris, 129
- generate_seh_payload function, 230
- generic/debug_trap payload, 208, 220
- getgui* script, 257
- GET HTTP request, 36
- getprivs command, 279
- getsystem command, 86, 119, 249, 278, 282
- getuid command, 86
- Google, to identify potential vulnerabilities, 260

H

- h2b conversion method, 193
- Hadnagy, Chris, 135
- hashdump command, 83, 84, 93, 95, 279, 282
- hashdump* post exploitation module, 82
- haystack, 111
- heap, 111
- heap-based attack, 70
- heap spraying technique, 111
- help command, 9, 43, 80, 277
- hex-blob, 185
- host_process.memory.allocate function, 238
- host_process.memory.write function, 239
- host_process.thread.create function, 239
- HTTP (HyperText Transfer Protocol)
 - man-left-in-the-middle attack, 150
 - PUT command, 264
 - PUT method, 261
- HVE, Patrick, 97
- HyperText Transfer Protocol (HTTP).
See HTTP (Hyper Text Transfer Protocol)

I

- ICMP (Internet Control Message Protocol), 19
- IDS (intrusion detection systems), 13, 18, 229
- idx counter, 194
- iexplorer.exe*, 113, 117, 237
- iframe injection, 147
- iframe replacement, 151
- IIS (Internet Information Server), 269
- IMAP (Internet Message Access Protocol) fuzzer, 198

- Immunity Debugger, 112–115, 200, 201, 208
 - F2 shortcut, 113, 114, 208
 - F5 shortcut, 114
 - F7 shortcut, 114, 208
- impersonate_token DOMAIN_NAME\ \ USERNAME command, 278
- INC ECX instructions, 209
- include Msf::Exploit::Remote:: BrowserAutopwn: directive, 179
- include statement, 188
- incognito command, 88, 282
- incremental IP IDs, 22
- indirect information gathering, 16
- Infectious Media Generator, 157
- info command, 63, 126, 130, 205, 275
- init.d* scripts, 20
- initialization constructor, 130
- 'INJECTHERE, SQL injection, 165
- insecure.org* site, 257
- INT3 instructions, 222, 223
- intelligence gathering, 15–33
 - active information gathering, port scanning, 18–26
 - custom scanners for, 31–33
 - passive information gathering, 16–18
 - using Netcraft, 17
 - using nslookup, 18
 - whois* lookups, 16–17
 - phase of PTES, 2
 - simulated penetration test, 252–253
 - targeted scanning, 26–31
 - FTP scanning, 29
 - for Microsoft SQL Servers, 27–28
 - SMB scanning, 26–27
 - SNMP sweeping, 30–31
 - SSH server scanning, 28
- Intel x86 architecture, *NOP*, 111, 112
- interactive Ruby shell, 241
- interfaces, for Metasploit, 8–12
 - armitage*, 11–12
 - msfcli*, 9–11
 - msfconsole*, 9
- Internet-based penetration tests, 19
- Internet Control Message Protocol (ICMP), 19
- Internet Explorer 7 Uninitialized Memory Corruption (MS09-002), 155
- Internet Explorer Aurora exploit, 116–119, 147
- Internet Information Server (IIS), 269

- Internet Message Access Protocol (IMAP) fuzzer, 198
- intrusion detection systems (IDS), 13, 18, 229
- intrusion prevention system (IPS), 18, 110, 252
- IP address, using Netcraft to find, 17
- ipidseq* scan, 22
- IPS (intrusion prevention system), 18, 110, 252
- irb command, 241, 242
- irb shell, 97
- is_admin?() function, 243
- is_uac_enabled?() function, 243
- ISO disc image, VMware Player, 268

J

- Java applet attack, 136, 142–146, 153–154, 156
- Java Applet Attack Method option, SET main menu, 144, 154
- Java Development Kit (JDK), Java applet attack, 136
- JavaScript output, 12
- JDK (Java Development Kit), Java applet attack, 136
- jduck, 79
- JMP ESP address, 221
- jmp esp command, 14
- JMP instruction set, 216

K

- KARMA, 177–178
 - karma.rc* file, 178, 182
- Karmetasploit, 177–184
 - configuring, 178–179
 - credential harvesting, 181–182
 - getting shell, 182–184
 - launching attack, 179–181
- Kelley, Josh, 185
- Kennedy, David, 79, 135, 163, 185, 248
- Kerberos token, 87, 89
- keylog_recorder* module, 82
- keystroke logging, for Meterpreter, 81–82
 - keyscan_dump command, 279
 - keyscan_start command, 279
 - keyscan_stop command, 279
- keystrokes, capturing, 282
- Killav, 93, 282

L

- LAN Manager (LM) hashes, 82, 84
- LHOST option, 62, 67, 86, 91, 96, 181, 246, 276
- lib/msf/core/exploit/http.rb* file, 130
- Linux system
 - dumping hashes on, 283
 - Metasploitable virtual machine, 251
 - as target machine, 268
- LIST command, 197, 199
- listener, 8
- listener handler, 86
- list_tokens -g command, 278
- list_tokens -u command, 88, 278
- little-endian format, 207, 221
- LM (LAN Manager) hashes, 82, 84
- load auto_add_route command, 91, 256, 258
- load nessus command, 49
- load nexpose command, 43
- load sounds command, 72
- Local System option, SQL Server Configuration Manager window, 271
- Log on as option, SQL Server Configuration Manager window, 271
- LPORT option, 62, 67, 72, 86, 96, 246
- lsass.exe* process, 117
- ls command, 277

M

- Macaulay, Shane, 177
- MailCarrier 2.51 SMTP commands, 216
- mailcarrier_book.rb* file, 220
- MailCarrier exploit, 218
- make_nops() function, 223
- malicious ActiveX control, 184
- malicious files, 119
- Management and Monitoring Tools
 - checkbox, *Windows Components Wizard*, 269
- man-left-in-the-middle attack, 150
- mass brute force attack,
 - SQLPwnage, 172
- mass client-side attack, 175–176
- mass emails, 142
- mass scan and dictionary brute option,
 - Fast-Track, 169
- McAfee antivirus software, 80
- MD5 checksum, 242
- Melvin, John, 163
- Memelli, Matteo, 197

- MessageBoxA function, 97
- messages* log file, 180
- Metasploitable, 251–252, 262
- Metasploit Browser Exploit Method
 - option, SET main menu, 147, 154
- Metasploit client-side exploit, 153–154
- Metasploit Express, vs. Pro, 14
- Metasploit Framework (MSF), 7–14
 - interfaces for, 8–12
 - armitage*, 11–12
 - msfcli*, 9–11
 - msfconsole*, 9
 - terminology in, 7–8
 - utilities for, 12–14
 - msfencode*, 13
 - msfpayload*, 12–13
 - nasm shell*, 13–14
 - working with databases in, 20–25
- Metasploit listener, 141, 256
- Metasploit Pro, vs. Express, 14
- Meterpreter, 75–97
 - commands for, 80–82, 277–279
 - keystroke logging, 81–82
 - post exploitation, 282–283
 - screenshot, 80–81
 - sysinfo, 81
 - compromising Windows XP virtual machine, 76–82
 - attacking MS SQL, 76–78
 - brute forcing MS SQL server, 78–79
 - scanning for ports with *nmap*, 76
 - xp_cmdshell*, 79–80
 - manipulating Windows APIs with
 - Railgun add-on, 97
 - and password hashes, 82–84
 - dumping, 83–84
 - extracting, 82–83
 - passing, 84–85
 - pivoting with, 89–91
 - post exploitation modules for, 95
 - privilege escalation with, 85–87
 - scripts for, 92–95
 - API for, 241–244
 - creating, 244–250
 - hashdump, 93
 - killav, 93
 - migrate, 92–93
 - overview, 235–241
 - packetrecorder, 93
 - persistence, 94–95

- rules for, 244
- scraper, 93–94
- token impersonation with, 87–89
- upgrading command shell to, 95–97

Meterpreter shell, 68, 156

Microsoft IIS, vulnerability in WebDAV implementations, 127

Microsoft Security Bulletin
MS10-002, 116

Microsoft SQL Attack Tools menu,
MSSQL Bruter, 168

Microsoft SQL Server

- attacking, 76–78
- brute forcing, 78–79
- getting command execution on,
186–187
- injection with Fast-Track tool, 164–174
 - manual injection, 167–168
 - MSSQL Bruter, 168–172
 - POST parameter attack, 166–167
 - query string attack, 165–166
 - SQLPwnage, 172–174
- targeted scanning for, 27–28
- on Windows XP, 269–271

Microsoft SQL Tools option, 165, 172

Microsoft Windows–based payloads, 60

Microsoft Windows

- CreateSizedDIBSECTION
Stack Buffer Overflow, 119

migrate command, 82, 92–93

migrate -f command, 119

migrate PID command, 278

Mitnick, Kevin, 248

Mixed-mode authentication, MSSQL
Bruter, 168

mixins

- defined, 31
- for Meterpreter scripts, 242–244

modules, 185–196

- and code reuse, 196
- creating, 189–196
 - converting from hex to binary,
192–194
 - counters in, 194–195
 - running exploit, 195–196
 - running Shell exploit, 190–192
 - using PowerShell, 189–190
- defined, 8
- exploring, 187–188
- getting command execution on
Microsoft SQL, 186–187

modules directory, 191

MS08-067 exploit, 59, 60, 67, 96

ms08_067_netapi module, 10, 59

MS11-006 exploit, 119

MSF (Metasploit Framework). *See* Meta-
sploit Framework (MSF)

Msf::Auxiliary::Scanner mixin, 32

MSF binary payload, 185

msfbook database, 20, 24

msf exploit(ms08_067_netapi) prompt, 60

msfcli, 9–11, 86, 281

msfconsole, 9, 20, 32, 37, 42

- customizing *msfconsole*, 255–257
- commands for, 275–277
 - info, 63
 - save, 64
 - set and unset, 63
 - setg and unsetg, 64
 - show auxiliary, 58
 - show exploits, 58
 - show options, 58–60
 - show payloads, 60–62
 - show targ, 62–63
- customizing, 255–257
- running NeXpose within, 43–44
- running *nmap* from, 24–25
- testing exploits, 220

msfconsole -r karma.rc command, 180

msf.doc file, 120

msfencode, 13, 102–103, 280

msfencode -h command, 13, 102, 280

Msf::Exploit::Remote::Seh mixin, 228

Msf::Exploit::Remote::Tcp mixin, 32, 219

Msf::Exploit::Remote::Udp mixin, 228

msf MS08-067 prompt, 62

msfpayload, 12–13

- commands for, 280
- creating binaries with, 100–101

msfpayload command, 103, 112

msfpayload -h command, 13, 280

msfpescan command, 206

msf prompt, 59

msfupdate command, 274

::Msf::Util::EXE.to_win32pe
function, 246

Msf::Util::EXE.to_win32pe(framework,
payload.encoded) option, 192

msfvenom, 108, 281

MSSQL Bruter, Microsoft SQL injection,
168–172

MSSQL Bruter option, 169

mssql_commands.rb file, 188

mssql_exec auxiliary module, 187

- MSSQL Injector option, 165
- mssql_login* module, 78–79
- mssql_payload* exploit, and
 - PowerShell, 189
- mssql_payload* module, 79–80
- mssql_ping* module, 27, 77–78
- mssql_powershell* module, 185
- mssql_powershell.rb* file, 189, 191, 195
- mssql.rb* file, 188, 191, 192, 195
- Mudge, Raphael, 11
- multi-attack vector, 153–157
- Multi-Attack Web Method option, SET
 - main menu, 154
- multi-encoding, 103–104
- multi-handler, Meterpreter sessions, 239
- multi-handler listener, 120
- multi/handler* module, 100–101, 249
- multi/http/tomcat_mgr_deploy* exploit, 261
- multi_meter_inject* command, 235, 237
- Muts, 226

N

- Nano, CTRL-W shortcut, 188
- nasm_shell*, 13–14
- nasm_shell.rb* utility, 13
- NAT (Network Address Translation), 25
- Nessus, 44–51
 - Add button, 45, 47
 - Bridge plug-in, 49–50
 - Browse button, 47
 - configuring, 44–45
 - creating scan policy, 45–47
 - Discovered Assets section, 40
 - General settings, 46
 - Home Feed, 44
 - importing report from, 48–49
 - Launch Scan button, 47
 - nessus_connect* command, 50
 - .nessus* file format, 48
 - nessus_help* command, 49
 - nessus_report_get* command, 50
 - nessus_report_list* command, 50
 - nessus_scan_new* command, 50
 - nessus_scan_status* command, 50
 - Nessus window, 44–45
 - Plugins page, 46
 - Policies tab, 45
 - Preferences page, 47
 - reports in, 47–48
 - running scan, 47
 - scanning from within Metasploit, 49–51

- Scans tab, 45, 47
- Submit button, 47, 48
- Users tab, 45
- netcat* listener, 32, 36
- Netcraft, passive information gathering
 - using, 17
- Netgear switch, 30
- net localgroup administrators metasploit*
 - /ADD command, 187
- netstat -an* command, 114
- net user* command, 85
- NetWin SurgeMail 3.8k44
 - vulnerability, 197
- Network Address Translation (NAT), 25
- Network Connections Control Panel,
 - Windows XP, 269
- Network Service account, 271
- New Database option, SQL Server Management Studio Express, 272
- New Login option, User Properties
 - window, 272
- New Table option, SQL Server Management Studio Express, 272
- NeXpose, 37–44
 - Administration tab, 37
 - Assets tab, 37
 - configuring, 37–42
 - Community edition, 37
 - Credentials tab, 38
 - Devices tab, 38
 - Home tab, 39
 - importing report from, 42–43
 - NeXpose Simple XML Export
 - option, 41
 - New Login button, 38
 - New Manual Scan button, 39
 - New Report button, 41
 - New Site button, 38
 - New Site wizard, 39
 - Report Configuration wizard, 42
 - Report format field, 41
 - running within *msfconsole*, 43–44
 - Scan Progress section, 40
 - Scan Setup tab, 38
 - Select Devices dialog, 42
 - Select Sites button, 41
 - Start New Scan dialog, 39
 - Start Now button, 39
 - Test Login button, 38
 - Vulnerabilities tab, 37
- nexpose_connect -h* command, 43
- nexpose_scan*, 43

- Next SEH (NSEH), 204, 208–209, 229
 - nmap*, 168, 257–259
 - idle scan, 22, 23
 - importing results into Metasploit, 21–22
 - Pn flag, *nmap*, 19
 - port scanning with, 18–20, 76
 - running from *msfconsole*, 24–25
 - scan, 252
 - script options, 64–65
 - TCP idle scan, 22–23
- No Execute (NX), 67
- noncredentialed scan, 43
- NOP (no-operation instruction), 111, 204, 209, 216, 219
- Notepad, 239–240
 - notepad.exe*, 156
- NSEH (Next SEH), 204, 208–209, 229
- nslookup, passive information gathering using, 18
- NT AUTHORITYSYSTEM server user-name, 86
- NTLM (NT LAN Manager), 82, 83
- NTLMv2 (NT LAN Manager v2), 82
- NX (No Execute), 67

O

- offset value, 223
- oledlg.dll* file, 230
- opcodes, 13
- Open option, Immunity Debugger, 113
- open source intelligence (OSINT), 16
- OpenSSH, 28, 259
- Open Table option, SQL Server Management Studio Express, 272
- open_x11* scanner, 54–55
- opt/framework3/msf3/lib/rex/post/meterpreter/ui/console/command_dispatcher/* directory, 242
- OSINT (open source intelligence), 16
- OS X system
 - dumping hashes on, 283
 - VMware Player, 268
- overt penetration testing, 4, 5
- overwrite exploits, for SEH, 226–232

P

- packers, 107–108
- packetrecorder command, 93
- passing password hashes, 84–85

- passive information gathering, 16–18
 - using Netcraft, 17
 - using nslookup, 18
 - whois* lookups, 16–17
- pass-the-hash technique, 84
- passwords
 - harvesting, 148–150
 - hashes for, 82–84
 - dumping, 83–84
 - extracting, 82–83
 - passing, 84–85
- pattern_offset.rb* file, 203
- `pay = client.framework.payloads.create(payload)` function, 239
- payload, 8, 75
- `payload.encoded` function, 224
- payload.exe* file, 85, 86
- .pcap* file format, 93
- .pde* file, 159
- PDF file format bug, spear-phishing attack vector, 137
- PE (Portable Executable) format, 100
- penetration testing, 4–5. *See also* simulated penetration test
- Penetration Testing Execution Standard (PTES), phases of, 2–4
 - exploitation, 3
 - intelligence gathering, 2
 - post exploitation, 3–4
 - pre-engagement interactions, 2
 - reporting, 4
 - threat modeling, 2–3
 - vulnerability analysis, 3
- pentest/exploits/fastrack/* directory, 274
- pentest/exploits/set/* directory, 136, 274
- Perez, Carlos, 235
- Perform a Mass Email Attack option, SET main menu, 139
- persistence command, 94–95
- PID (process ID), 236
- PID variable, 238
- ping command, 19
- pivoting
 - with Meterpreter, 89–91
 - process of, 25
- polymorphic encoding, 103
- PolyPack project, 108
- POP3 service, 181
- POP-POP-RETN* sequence of instructions, 204, 206, 208, 226, 229, 230
- Portable Executable (PE) format, 100

- porting exploits to Metasploit, 215–233
 - assembly languages, 216
 - buffer overflow exploits, 216–226
 - adding randomization, 222–223
 - completed module, 224–226
 - configuring exploit definition, 219–220
 - implementing features of the Framework, 221–222
 - removing dummy shellcode, 223–224
 - removing NOP Slide, 223
 - stripping existing exploit, 218–219
 - testing base exploit, 220–221
 - SEH overwrite exploit, 226–232
- port scanning with *nmap*, 18–20, 76
- portscan syn* module, 26
- post exploitation
 - modules for Meterpreter, 95
 - phase of PTES, 3–4
- Postfix mail server, 260
- PostgreSQL database, 20
- postgres* username, in PostgreSQL database, 20
- POST parameter attack, Microsoft SQL injection, 166–167
- POST parameters, 148
- PowerShell, 185, 189–190, 192–194
- powershell_upload_exec* function, 191
- pre-engagement interactions, 2
- print_error()* function, 242
- printing output, for Meterpreter scripts, 241–242
- print_line()* function, 241
- print_status()* function, 241
- priv* extensions, 86
- privilege escalation, 85–87, 119
- privilege-escalation attack, 110
- PRNG exploit, 262
- Process Explorer, Windows, 105
- process ID (PID), 236
- ProFTPD 1.3.1, 259
- protection mechanisms, 283
- Protocols for SQLEXPRESS option, SQL Server Configuration Manager window, 270
- Protocol tab, SQL Server Configuration Manager window, 270
- ps* command, 81–82, 87–89, 180, 278
- PTES (Penetration Testing Execution Standard). *See* Penetration Testing Execution Standard (PTES)

- PureBasic language, 54
- PUT method, HTTP, 261, 264
- PuTTY Windows SSH client, 106

Q

- query string attack, Microsoft SQL injection, 165–166
- Query String Parameter Attack option, 165
- Quick TFTP Pro 2.1, 226

R

- Railgun add-on, manipulating Windows APIs with, 97
- rainbow table attack, 84
- random characters, 229, 230
- random dynamic port, TCP, 27
- random payload name, 193
- rand_text_alpha_upper* buffer, 223
- Rapid7, 37
- RATTE (Remote Administration Tool Tommy Edition), 160
- raw hexadecimal format, convert executable to, 192
- RDP (Remote Desktop Protocol), 257
- read-only (RO) community string, 30
- read/write (RW) community string, 30
- reboot command, 279
- reg_command* command, 278
- regedit*, 95
- registry keys, 95
- registry manipulation, 243
- Remote Administration Tool Tommy Edition (RATTE), 160
- Remote Desktop Protocol (RDP), 257
- remote GUI (VNC), getting, 283
- Remote Procedure Call (RPC) service, 59
- reporting phase of PTES, 4
- Reports tab
 - Nessus, 45, 48
 - NeXpose home page, 37, 40, 42
- Required column, 51
- resource command, 72
- resource files, for exploitation, 72–73
- resource karma.rc* command, 180
- resource.rc* file, 72
- restrictions for SEH, 204–206
- rev2self* command, 87, 278
- reverse Meterpreter payload, 145, 155

- reverse payload, 62
- reverse shell, 8
- reverse_tcp payload, 61, 67, 68
- Rex::Text.pattern_create, 202
- Rex::Text.rand_text_alpha function, 245
- RHOST option, 10, 276
- RHOSTS option, 22–23, 25, 67, 91, 125, 126
- RO (read-only) community string, 30
- robots.txt file, 127
- root/.msf3/config directory, 64
- root/.msf3/modules/exploits/windows/imap/ directory, 204
- root/.msf3/modules/auxiliary/fuzzers/ directory, 198
- route add command, 91
- route command, 90
- route print command, 90
- RPC (Remote Procedure Call) service, 59
- RPORT option, 10
- RSA company, 110
- RT73 chipset, 179
- Ruby programming language, 185
- Ruby shell, 97
- rules for Meterpreter scripts, 244
- run_batch(batch) method, 31
- run command, 130, 235, 249
- run get_local_subnets command, 89
- run hashdump command, 93
- run_host(ip) method, 31
- run migrate script, 117
- run_range(range) method, 31
- run screen_unlock command, 92
- run scriptname command, 92, 277
- run vnc command, 92
- RW (read/write) community string, 30

S

- sa (system administrator) account, 77, 79, 168, 186
- SAM (Security Account Manager) database, 83, 282
- Samba exploit, 69, 90
- save command, 64
- scanner/ftp/anonymous module, anonymous logins, 29
- scanner/http modules, 126
- scanner/ip/ipidseq module, 22
- scanner mixin, 31
- scanner/portscan/syn module, 257
- scanner/portscan/tcp module, 91, 257

- scanner/snmp/snmp_enum module, 30
- scanning
 - Metasploitable system, 258–259
 - a number of systems, 27
 - only one system, 27
- scan policies, list of available, 50
- scraper command, 93–94
- screenshot command, 80–81, 278
- scripts, for Meterpreter, 92–95, 235–250
 - API for, 241–244
 - creating, 244–250
 - hashdump, 93
 - killav, 93
 - migrate, 92–93
 - overview, 235–241
 - packetrecorder, 93
 - persistence, 94–95
 - rules for, 244
 - scraper, 93–94
 - script=smb-check-vulns plug-in, 65
 - scripts/meterpreter/ directory, 89, 235, 244
- Search button, Login-New window, 272
- search command, 58, 60
- search name command, 275
- search scanner/http command, 126
- Secure Shell (SSH), 28, 259
- Secure Sockets Layer (SSL), 31
- Security Account Manager (SAM) database, 83, 282
- SEH (Structured Exception Handler)
 - controlling, 201–203
 - overwrite exploits for, porting to Metasploit, 226–232
 - restrictions for, 204–206
 - three-byte overwrite of the, 207
- SEH chain option, Immunity Debugger, 201, 208
- send_request_cgi method, 130
- separate process, automigrating to, 282
- Server Message Block (SMB). *See* SMB (Server Message Block)
- service_(name) function, 243
- sessions -c cmd command, 277
- sessions -i 1 command, 68
- sessions -i sessionid, 86
- sessions -K command, 277
- sessions -l command, 68, 86, 276
- sessions -l -v command, 68, 277
- sessions -s script command, 277
- sessions -u 1 command, 96
- sessions -u command, 95
- sessions -u sessionID command, 277

- SET (Social-Engineer Toolkit), 135–161
 - AUTO_DETECT setting
 - OFF option, 137
 - ON option, 136
 - config/set_config* file, 136
 - configuring, 136–137
 - Infectious Media Generator, 157
 - spear-phishing attack vector, 137–142
 - Teensy USB HID attack vector, 157–160
 - web attack vectors, 142
 - client-side web exploits, 146–148
 - Java applet attack, 142–146
 - man-left-in-the-middle attack, 150
 - multi-attack vector, 153–157
 - tabnabbing attack, 150
 - username and password harvesting, 148–150
 - web jacking attack, 151–152
- set autorunscript migrate -f
 - command, 276
- set command, 63
- set_config* file, 142
- setdesktop *number* command, 278
- set *function* command, 276
- setg command, 64, 96
- setg *function* command, 276
- SET Interactive Shell, 160
- set LHOST command, 67
- set payload *payload* command, 276
- set payload windows/shell/reverse_tcp
 - command, 61
- set target *num* command, 276
- SET Web-GUI, 160
- SHA1 checksum, 242
- SHA256 checksum, 242
- shell, upgrading to Meterpreter, 95–97
- SHELL32.DLL*, Windows XP SP2, 221
- shellcode, 8, 12–13
- shell command, 68, 278
- shell_reverse_tcp payload, 100
- SHIFT-F9 shortcut, in Immunity Debugger, 208
- shikata_ga_nai encoder, 103, 104, 281
- show command, 58–63, 65, 56, 67, 68, 118, 124, 191, 275, 276
- show_options command, 51
- sI flag, 23
- signatures, 99
- Simple Mail Transport Protocol (SMTP), 137, 260
- Simple Network Management Protocol (SNMP), 30–31, 269
 - simple_tcp.rb* script, 32
 - simulated penetration test, 251–266
 - attacking Apache Tomcat, 260–262
 - attacking obscure services, 262–264
 - covering tracks from, 264–266
 - customizing *msfconsole*, 255–257
 - exploitation, 255
 - intelligence gathering, 252–253
 - planning, 252
 - post exploitation, 257–260
 - identifying vulnerable services, 259–260
 - scanning Metasploitable system, 258–259
 - threat modeling, 253–255
- Single Target option, Fast-Track, 169
- Site Cloner option, SET main menu, 144, 147, 149, 151, 154
- SMB (Server Message Block)
 - scanning of, 26–27
 - vulnerability scanning for logins, 51–52
- smb_login* module, 51
- SMBPass variable, 85
- smb/psexec* module, 84–85
- smb_version* module, 26, 27
- SMPIPE option, 10
- SMTP (Simple Mail Transport Protocol), 137, 260
- sniffer_dump *interfaceID pcapname*
 - command, 279
- sniffer_interfaces command, 279
- sniffer_start *interfaceID packet-buffer*
 - command, 279
- sniffer_stats *interfaceID*
 - command, 279
- sniffer_stop *interfaceID* command, 279
- SNMP (Simple Network Management Protocol), 30–31, 269
- Social-Engineer.org site, 135
- Social-Engineer Toolkit (SET). *See* SET (Social-Engineer Toolkit)
- sock.put command, 219
- 'Space' declaration, 205
- spear-phishing attack vector, 110, 137–142, 145
- Spear-Phishing Attack Vectors option, SET main menu, 139
- SQL authentication, MSSQL Bruter, 168

- SQL injection
 - attempting to leverage, 254
 - error message, 255
- SQL Injector - Query String Parameter
 - Attack option, 166
- SQL Ping attempt, Fast-Track, 169
- SQL Server 2005 Services option, SQL
 - Server Configuration Manager window, 270
- SQL Server Authentication option, SQL
 - Server Management Studio Express, 272
- SQL Server Browser service, 270, 271
- SQL Server Configuration Manager window, 270–271
- SQL Server Management Studio Express
 - option, Windows XP, 272
- SQL Server (SQLEXPRESS) option,
 - SQL Server Configuration Manager window, 270
- SQLPwnage, Microsoft SQL injection, 172–174
- SRVHOST option, 117
- SRVPORT option, 117
- s flag, *nmap*, 19
- SSH (Secure Shell), 28, 259
 - ssh_version* module, 28
- SSL (Secure Sockets Layer), 31
 - sT flag, 65
- stand-alone exploits, 215
- Start Mode option, SQL Server Browser
 - service, 270
- Start MSF option, *armitage*, 11
- Start option, SQL Server Configuration
 - Manager window, 271
- Status Report email template, 140
- steal_token command, 88
- steal_token PID command, 278
- Stealth TCP connect, 65
- stealth TCP scan, 252
- stored procedure, in SQL Server 2005
 - and 2008, 186
- Structured Exception Handler (SEH).
 - See SEH (Structured Exception Handler)
- Subnet1.xml* file, 21
- sudo feature, 248
- surgemail.exe* file, 200, 204
- surgemail* service, 201–202
- SurgeMail vulnerability, 204
- SVN certificate, 274

- svn update command, 274
- SYN Port Scanner, 25
- sysadmin* role, 186
- sysinfo command, 81, 277
- SYSTEM-level permissions, 79

T

- t switch, in *db_autopwn* command, 56
- TAB key, 95, 235
- tabnabbing attack, 150
- targeted scanning, 26–31
 - FTP scanning, 29
 - for Microsoft SQL Servers, 27–28
 - SMB scanning, 26–27
 - SNMP sweeping, 30–31
 - SSH server scanning, 28
- target machines, 267–274
 - Linux, 268
 - setting up, 267–268
 - Windows XP, 269–274
 - configuring web server on, 269
 - creating vulnerable web application, 271–272
 - MS SQL server on, 269–271
 - updating BackTrack, 272–274
- [target['Ret']].pack('V'), 221
- target return address, 221
- 'Targets' section, 206, 207, 221, 222, 230
- Task Manager, Windows, 117
- TCP (Transmission Control Protocol)
 - Dynamic Ports option, TCP/IP
 - Properties dialog, 270
 - idle scan, 2223
 - port 80, 36
 - port 443, 70, 112, 114
 - port 1433, 27, 76–77, 168, 270
 - port 4444, 62
 - random dynamic port, 27
 - scanning with, 19
- TCP/IP option, 270
- TCP/IP Properties dialog, 270
- technical findings, 4
- Teensy USB HID attack vector, 157–160
- Temp* directory, 192
- template.pdf* file, 139
- Tenable Security, 44
- terminology, in Metasploit, 7–8
- text.rb* file, 223
- TFTP (Trivial File Transfer Protocol), 228–231

THREADS *number* option, 27
 THREADS option, 126
 THREADS value, 22–23, 25, 125
 threat modeling
 phase of PTES, 2–3
 simulated penetration test, 253–255
 three-byte overwrite, of SEH, 207
 time-based iframe replacement, 151
 timestomp command, 264, 279
 token impersonation, with Meterpreter,
 87–89
 toor password, in PostgreSQL
 database, 20
 Total size value, 205
 Transmission Control Protocol (TCP).
 See TCP (Transmission Control
 Protocol)
 Trivial File Transfer Protocol (TFTP),
 228–231
 Trojan backdoor, 125
 Turn off Automatic Updates option,
 Windows XP, 269
 Twitter, auxiliary module, 129
 types of penetration testing, 4–5

U

UAC (User Account Control), 243, 248
 Ubuntu, 68–71, 259–260, 267–268
 UDP (User Datagram Protocol)
 port 69, 228
 port 1434, 27, 77, 168
 uictrl enable keyboard/mouse
 command, 279
 unset command, 63
 unsetg command, 64
 upgrading command shell, to
 Meterpreter, 95–97
 upload *file* command, 279
 UPX packer, 107–108
 URIPATH option, 117
 usage function, 238
 use command, 51, 60, 125, 126, 132, 249
 use incognito command, 88, 278
 use multi/handler command, 94
 use *name* command, 276
 use priv command, 83, 86, 119, 278
 use scanner/http/webdav_scanner
 command, 125
 use scanner/mssql/mssql_ping
 command, 78
 use scanner/portscan/syn command, 25

use scanner/snmp/snmp_login module, 30
 use sniffer command, 279
 Use them all - A.K.A. 'Tactical Nuke'
 option, SET main menu, 154
 use windows/smb/ms08_067_netapi
 command, 59
 UsePowerShell method, 190, 191
 User Account Control (UAC), 243, 248
 User Datagram Protocol (UDP). *See*
 UDP (User Datagram Protocol)
 User Mapping option, User Properties
 window, 272
 User Properties window, 272
user32.dll, 97
 username harvesting, 148–150
 utilities, for Metasploit, 12–14
 msfencode, 13
 msfpayload, 12–13
 nasm shell, 13–14

V

variables, using uppercase characters, 63
 VBScript, 95
 VenueID, 132
 version command, 72
 virtual network computing (VNC)
 authentication, 52–54
 VMware Player, 268
.vmx file, 268
 VNC (remote GUI), getting, 283
 VNC (virtual network computing)
 authentication, 52–54
 vnc_none_auth command, 53
vncviewer, connecting to VNC with no
 authentication, 53
 VNC window, 92
 vulnerability scanning, 35–73
 defined, 5
 with Nessus, 44–51
 configuring, 44–45
 creating scan policy, 45–47
 importing report from, 48–49
 reports in, 47–48
 running scan, 47
 scanning from within Metasploit,
 49–51
 with NeXpose, 37–44
 configuring, 37–42
 importing report from, 42–43
 running within *msfconsole*, 43–44
 for open VNC authentication, 52–54

- for open X11 servers, 54–56
- overview, 36–37
- phase of PTES, 3
- using results in Autopwn tool, 56
- for valid SMB logins, 51–52
- vulnerable services, identifying, 259–260

W

- WEBATTACK_EMAIL flag
 - OFF option, 136
 - ON option, 136, 142
- web attack vectors, 142
 - client-side web exploits, 146–148
 - Java applet attack, 142–146
 - man-left-in-the-middle attack, 150
 - multi-attack vector, 153–157
 - tabnabbing attack, 150
 - username and password harvesting, 148–150
 - web jacking attack, 151–152, 153–154
- WebDAV, 127–128
 - webdav_scanner* module, 125
- web jacking attack, 151–152, 153–154
- Web Jacking Attack Method option, SET
 - main menu, 151, 154
- web server, configuring on
 - Windows XP, 269
- Website Attack Vectors option, SET
 - main menu, 144, 147, 149
- website clone, 148–149, 152
- Weidenhamer, Andrew, 163
- Werth, Thomas, 142
- White, Scott, 163
- white hat test, 4
- whois* lookups, 16–17
- WIDEOPENWEST service provider, 17
- Win2k8, 282
- Windows, Task Manager, 117
- Windows APIs, manipulating with
 - Railgun add-on, 97
- Windows authentication, MSSQL
 - Bruter, 168
- Windows Components Wizard, 269
- Windows debug 64KB restriction, 172
- Windows Firewall, Windows XP, 269
- Windows login credentials, 46
- Windows Management Interface (WMI), 269
- Windows UAC, 248, 249, 283

- Windows virtual machine, scanning, 21
- Windows XP, 76–82
 - attacking MS SQL, 76–78
 - brute forcing MS SQL server, 78–79
 - exploitation for, 64–68
 - nmap* scan against, 19
 - scanning for ports with *nmap*, 76
 - scanning only one system, 27
 - as target machine, 269–274
 - configuring web server on, 269
 - creating vulnerable web application, 271–272
 - MS SQL server on, 269–271
 - updating BackTrack, 272–274
 - xp_cmdshell*, 79–80
- windows/meterpreter/reverse_tcp* payload, 246
- windows/shell_reverse_tcp* payload, 100
- windows/smb/ms08_067_netapi* exploit, 59, 67
- windows/smb/psexec* module, 84–85
- wireless attack vector, 160–161
- wireless card, 179
- WMI (Windows Management Interface), 269
- WScript file, 157
- WSCRIPT HTTP GET MSF Payload option, SET main menu, 158

X

- X11 servers, vulnerability scanning for, 54–56
- x86/shikata_ga_nai* encoder, 13, 103
- x90, Intel x86 architecture, 112
- xCCs breakpoints, 208
- xp_cmdshell* stored procedure, 79–80, 166, 169, 172, 186, 187, 188, 255, 257
- xspy* tool, 55–56
- XSS (cross-site scripting)
 - vulnerability, 150
- xterm* window, 256

Z

- Zate, 49
- zero-day vulnerability, Adobe Flash, 110, 146