INDEX

A

absolute security descriptors, 149–151, 164
Abstract category attribute, 354
access checks, 25, 36, 222, 265
Active Directory, 366
automating, 275–277
discretionary, 228, 241–244, 249, 259
enterprise, 249–260
handle duplication, 269–272
kernel-mode, 222–225
mandatory (MACs), 228, 230–237, 242
object type, 249–255
in PowerShell, 227–244
remote access check protocol, 389–390
sandbox token checks, 244–249, 272–274
thread process, 271–272
token, 227–228, 230, 237–241
traversal checks, 266–269
user-mode, 225
worked examples, 261–263, 277–279
access control entries (ACEs), 145, 153–156. See also names of specific ACEs
access filter, 233
callback, 156
compound, 154–155, 213–214
discretionary access control lists, 145–146
finding resources with Audit ACEs, 294–295
flags, 156
flag strings mapped to, 167
mandatory label, 154, 167, 172, 201–203
normal, 154–155
object, 154–155
ordering, 158–159
security access control lists, 145–146
supported types, 153
type strings mapped to ACE types, 167
access control lists (ACLs), 151–156
ACEs, 153–156
DACLs, 145–146, 186, 215
flag strings mapped to control flags, 166
headers, 152–153
NULL ACLs, 146
SACLs, 144–146, 288–289, 292–293
AccessFilter ACEs, 154, 156, 167
access masks, 155
access strings mapped to, 168
closing handles, 40
converting, 38–39
displaying, 37–38
handle tables, 39–40
numeric value of, 39
generic mapping tables, 37
types of access, 36–37
access mode, 223–224
access strings
for file and registry types, 169
mandatory label access strings, 172
mapped to access masks, 168
AccessSystemSecurity access right, 37, 178
access tokens, 25
AccountNotDelegated flag, 490
ACE flag strings, 167
ACEs. See access control entries; names of specific ACEs
ACL flag strings, 166
ACLs. See access control lists
Active Directory, 341–396
  access checks, 366–382
  claims and central access policies, 382–384
  domain configuration, 342–349
  enterprise network domains, 301–302
  group policies, 349–353
  ObjectType GUIDs used in, 169
  property hierarchy, 250–251
  schema, 353–358
  security descriptors, 358–366
  worked examples, 387–395
Add- commands, 49–52, 59, 84, 157, 251, 309, 311, 324, 371, 389, 543, 415, 417–418
AddMember access right, 318
Add-Member function, 388
AD-Domain-Services feature, 541, 545
AdjustDefault access right, 100
AdjustGroups access right, 100
AdjustPrivileges access right, 100, 320
AdjustQuotas access right, 320
AdjustSessionId access right, 100
AdjustSystemAccess access right, 320
AdministerServer access right, 315
administrator users, 122–124
  LsaLogonUser API, 409–410
  removing privileges, 140–141
  SAM database, 326
  verifying tokens, 123–124
Advanced Encryption Standard (AES), 327–332
  AES keys, 470–471, 496
advanced local procedure call (ALPC) subsystem, 24, 55
AFD (Ancillary Function Driver), 47
Alarm ACEs, 154, 292
AlarmCallback ACEs, 154, 292
AlarmCallbackObject ACEs, 154, 292
AlarmObject ACEs, 154, 292
aliases, 12–13, 166, 318, 548
Allowed ACEs, 153–154, 158, 167
AllowedCallback ACEs, 154, 167
AllowedCallbackObject ACEs, 154, 167
AllowedCompound ACEs, 154–155
AllowedObject ACEs, 154, 167
ALPC (advanced local procedure call) subsystem, 24, 55
Ancillary Function Driver (AFD), 47
Anonymous flag, 518
Anonymous impersonation level, 104, 106, 136
anonymous sessions, 518–519
Anonymous type, 53
Anonymous user token, 214
ANSI strings, 79
APIs
  AcceptSecurityContext API, 426–427
  AcquireCredentialsHandle API, 424
  AuthzAccessCheck API, 156, 243
  AuthZ API, 387, 389–390
  Create APIs, 77–79, 87–90, 107, 117, 135, 208, 412–413
  Data Protection API (DPAPI), 322, 516
  DecryptMessage API, 440–441, 476
  EncryptMessage API, 440–442
  ExIsRestrictedCaller API, 272
  Generic Security Services API, 476
  Get APIs, 65–66, 78, 208–209, 212
  ImpersonateNamedPipe API, 104
  InitializeSecurityPipe API, 423–424
  LoadLibrary API, 65, 68
  LogonUser API, 102, 401
  LsaLogonUser API, 399–414
    accessing from PowerShell, 410–412
    creating user desktops, 398–399
    domain authentication, 403–404
    local authentication, 401–402
    logon and console sessions, 404–406
    logon types, 400
    protocol transition delegation, 489
    security packages, 400–401
    token creation, 407–410
  LsaManageSidNameMapping API, 323–324
LsaOpenPolicy API, 318–319
MakeSignature API, 441–443
NtAccessCheckByType API, 249
prefix-to-subsystem mapping, 24–25
Query APIs, 430, 442
RtlDosPathNameToNtPathName API, 83, 86
RtlIsSandboxToken API, 272, 274
Sam APIs, 313–316
SeAccessCheck API, 222–223
SeAccessCheckByType API, 249
SeAssignSecurityEx API, 180–182
SeCreateClientSecurity API, 484
SeImpersonateClient API, 484
SeSetSecurityDescriptorInfoEx API, 206–207
SetNamedSecurityInfo API,
208–210
SeTokenCanImpersonate API, 136
SetPrivateObjectSecurityEx API, 208
sets, 67–68
Shell, 89–91
VerifySignature API, 440–441
Win32 security APIs, 64–70, 77–80, 208–213
WinSock API, 47
AppContainer process, 120–122
Application Information service, 93
application package authority, 120
AP-REP message. See authentication
protocol reply message
AP-REQ (authentication protocol request) message, 494,
519–520
array type, 5
asInvoker UAC execution level, 126
AS-REP (authentication service reply)
message, 459
AS-REQ (authentication service request) message, 458
AssignPrimary access right, 100
Audit ACEs, 153, 167, 294–295
AuditCallback ACEs, 154, 167
AuditCallbackObject ACEs, 154
auditing. See security auditing
AuditLogAdmin access right, 319
AuditObject ACEs, 154, 167
audit policy security, 287–293
configuring global SACL, 292–293
configuring resource SACL,
288–291
authentication audit event log, 524–527
authentication protocol reply (AP-REP)
message
decryption, 476–477
delegation, 481
Kerberos authentication in
PowerShell, 468–469
Negotiate security package, 505
network service authentication,
463–464
authentication protocol request
(AP-REQ) message, 494, 519–520
cross-domain authentication, 478
decryption, 469–476
delegation, 481–483, 485–487
Kerberos authentication in PowerShell, 466–469
Negotiate security package, 505
network service authentication,
463–464
U2U authentication, 491–493
authentication protocol transitions,
486–487, 490
authentication service reply (AS-REP)
message, 459
authentication service request
(AP-REQ) message, 458
authentication tokens, 423, 500
Authencode mechanism, 54
AuthZAccessCheck function, 387
auto-inherit flags, 161, 181–182, 203,
209–210, 215
Auxiliary category attribute, 354
B
BackgroundColor parameter, 16
BaseNamedObjects (BNO) directory, 29
console sessions, 76–77
finding object manager resource
owners, 216–217
querying security descriptor and
owner for, 179
Win32 APIs vs. system calls, 78
bitwise operators, 6
BNO directory. See BaseNamedObjects directory
Boolean operators, 6
bool type, 5
brute-force attacks, 428–429, 465

C
canonicalization, 84–85, 362
CBC (cipher block chaining), 330
central access policies, 255–260
    access checks, 258–259
    Active Directory, 382–384
    claims, 255–256, 382–384
displaying, 257
enabling, 259–260
information contained in, 257
simple configuration vs., 256
ChangePassword access right, 316, 377
channel binding, 444–445
ChannelBindings buffer flag, 500
Chrome web browser, 117
cipher block chaining (CBC), 330
ciphertext-stealing mode (CTS), 466
Citrix, 77
claims
    Active Directory, 382–384
device, 255–256
user, 255–256
Class88 category attribute, 354
Client Server Runtime Subsystem (CSRSS), 71
CLI XML format, 20–21
CloudAP security package, 403
code integrity, 54–55
    Authenticode mechanism, 54
    kernel, 24
    prefix, 25
    purpose of, 54
COM (Component Object Model)
    server processes, 93
command line parsing, 88–89
commands. See also names of specific commands
    accepting parameters, 9
    accessing properties and methods, 9
    aliases, 12–13
    discovering, 10
    executing, 9–10
    line breaks, 9–10
    naming conventions, 9
    passing output of one to another, 9
    usage examples of, 11–12
Commit state value, 50
Compare- commands, 42, 231, 233
Component Object Model (COM)
    server processes, 93
conditional expressions, 155, 169–171
    access filter ACEs, 233–235
    central access policy, 255, 257–259
    infix operators for, 171
    type values, 170
    unary operators for, 170
Confidentiality request attribute flag, 440–441, 451
configuration manager. See registry
Connect access right, 313
console sessions, 83, 416–417
    creating user desktops, 398
    impersonation tokens, 137
    Remote Desktop Services, 74–75
    separation of named objects, 76–77
    session ID, 102, 405
    Windows logon process, 92
constrained delegation (Service for User), 480, 484–491
    Kerberos-only, 485–486, 490
    protocol transition, 486–488, 490
    resource-based, 489–491
constructors, 8
ContainerInherit ACE flag, 156, 167, 193–194, 202
context tracking mode, 106
ControlAccess access right, 366, 378
    control access rights, 376–379, 394
    control flags, 144–145, 166, 173, 182, 193–194, 215, 381
    Dacl, 144–146, 166, 181–182, 194, 215
    RmControlValid, 149
    Sacl, 144–145, 166, 181
    SelfRelative, 149–151
    ServerSecurity, 213–214
    TrustedForDelegation, 381, 482
    TrustedToAuthenticateFor Delegation, 381
ConvertFrom-commands, 155–156, 163, 173, 502, 509
ConvertTo-NtSecurityDescriptor command, 218
Copy-commands, 41, 107–108, 140
CreateAccount access right, 319–320
CreateAlias access right, 315
CreateChild access right, 366–368
CreateDirectories property, 267
CreateDomain access right, 313
CreateGroup access right, 315, 317
CreatePrivilege access right, 319
CreateSecret access right, 319
CreateUser access right, 315
creator security descriptors, 180
assigning during resource creation, 180–188
inheritance rules, 215
Credential Guard, 484
credential manager, 514–517
CredSSP protocol, 510–513
Critical ACE flag, 156, 167, 208
cross-domain authentication, 477–479
cryptographic derivation process, 431–433
CSRSS (Client Server Runtime Subsystem), 71
CSV files, 20
CTS (ciphertext-stealing mode), 466
CVE security issues
2014-6324, 475
2014-6349, 278
2018-0748, 184
2018-0983, 212
2019-0943, 57, 271
2020-1472 (Zerologon), 403
2020-1509, 523
2020-17136, 225
2021-34470, 368

D
DAC (discretionary access control), 36, 143
Dacl control flags, 144–146, 166, 181–182, 194, 215
DACLs. See discretionary access control lists
Dacl security information flag, 211
DAP (Directory Access Protocol), 342
Data buffer flag, 500, 502
Data Encryption Standard (DES), 332–333
Datagram Transport Layer Security (DTLS) protocol, 506
Data Protection API (DPAPI), 322, 516
DCOM Server Process Launcher, 93
Delegate flag, 483
delegation, 479–480
constrained, 480, 484–491
unconstrained, 480–484
Delegation impersonation level, 105–107
Delete access right, 36, 168, 369
DeleteChild access right, 366, 369
DeleteTree access right, 366, 369
Denied ACEs, 153–154, 158, 167, 243, 255
DeniedCallback ACEs, 154, 167
DeniedCallbackObject ACEs, 154
DeniedObject ACEs, 154, 167, 252–253, 255
deny/callback ACEs, 243
DES (Data Encryption Standard), 332–333
DesiredAccess parameter, 30, 36, 79
Desktop objects, 71–72
desktop window manager (DWM) process, 92, 405
DHCP (Dynamic Host Configuration Protocol), 537, 540
Diffie-Hellman key exchange, 477, 508
Directory Access Protocol (DAP), 342
Directory objects, 28, 169, 219
Disable-NtTokenPrivilege command, 114
discretionary access checks, 228, 230, 241–243
discretionary access control (DAC), 36, 143
discretionary access control lists (DACLs), 145–146
control flags, 144–146, 166, 181–182, 194, 215
default, 186
inheritance rules, 215
DistinguishedName attribute, 351
distinguished names, 349–351
dllMain function, 66
DLLs, 65–69, 119
API sets, 67–68
delay loaded, 67
_DLL file extension, 69
export forwarding, 66
hijacking, 68–69
loading new libraries, 65–66
NTDLL, 65–66
searching for, 68–70
untrusted, 66
viewing imported APIs, 66–67
DNS. See Domain Name System
domain authentication, 300–304
domain forests, 302–304
temporary network domains, 301–302
local authentication, 299–301
LsaLogonUser API, 403–404
domain forests, 302–304
global catalog, 303–304
multiple, 304
trust relationships, 303
DomainLocal group scope, 346–347
Domain Name System (DNS), 302, 344, 536
Active Directory domain
collection, 344–345
virtual machines, 540, 544
domain policy remote service, 312, 318–324
access rights, 319
account objects, 319–321
connecting to, 318–319
name lookup and mapping, 323–324
secret objects, 321–322
trusted domain objects, 322–323
domain security policies, 282
done state, 430
DOS device paths, 83–87
canonicalization, 84–85
displaying symbolic links, 83–84
DOS device map prefix, 83
maximum path lengths, 85–87
path separators, 84
path types, 84–85
double hop problem, 435
double type, 5
DPAPI (Data Protection API), 322, 516
drawing resource objects, 71
DTLS (Datagram Transport Layer Security) protocol, 506
Duplicate access right, 100
DWM (desktop window manager) process, 92, 405
Dynamic Access Control, 255
Dynamic Host Configuration Protocol (DHCP), 537, 540
E
ECB (electronic code book), 333
Edit- commands, 158–159, 190, 364
Effective pseudo token handle, 108
effective token mode, 106
electronic code book (ECB), 333
Empty buffer flag, 500
Enabled attribute, 110, 114
EnabledByDefault attribute, 110, 114
Enable-NTTokenPrivilege command, 114
temporary access checks, 249–260
central access policy, 255–260
object type access checks, 249–255
temporary authentication capability, 520–523
temporary network domains, 301–302.
See also Active Directory
domain controllers, 301–302
group policies, 302
EnumerateDomains access right, 313–314
EnumerateUsers access right, 287
EPA (Extended Protection for Authentication), 444
escape characters, 7–8
Event Tracing for Windows (ETW), 292
Everyone ACEs, 965
explicit credentials, 437, 522–523
explicit token impersonation, 107
Export- commands, 20, 533
exporting data
to CLI XML format, 20–21
to CSV files, 20
to text files, 20
expressions, 5–8
Extended Protection for Authentication (EPA), 444
extended rights, 373–376
ExtendedSessionSecurity NTLM flag, 429–430
Extra buffer flag, 500

F
FailedAccess ACE flag, 156, 168
Fast User Switching feature, 75, 417
File objects, 30, 41, 162, 169
ForceAccessCheck attribute flag, 224–225
ForcePasswordChange access right, 316
ForegroundColor parameter, 16
functions, 13–14

G
GDI32 library, 70–71
GenericAll access value, 37, 250–252, 254
GenericExecute access value, 37, 235
generic mapping, 39, 181
  assigning security descriptors during resource creation, 181, 185
to existing resources, 206–207
kernel-mode access checks, 222
mandatory integrity level check, 235
mapping tables, 37
user-mode access checks, 225
GenericRead access value, 37, 39, 235
Generic Security Services Application Program Interface (GSSAPI), 476
GenericWrite access value, 37, 235
GetAliasMembership access right, 315
GetObject method, 59
GetPrivateInformation access right, 319
global catalog, 303–304, 352–353
Global group scope, 346–347
golden tickets, 462–463
Google Chrome web browser, 117
GrantedAccessMask property, 39
GroupByAddress parameter, 58
Group-Object command, 19, 58
group policies, 256–257, 409
Active Directory, 384–386
authentication to known web proxies, 521
enterprise network domains, 301–302
Group security information flag, 157, 183
GSSAPI (Generic Security Services Application Program Interface), 476
GSS_ functions, 476

H
handles, 30, 35–42
access masks, 36–40
closing, 40
displaying handle tables, 39–40
duplication, 40–41
duplicating unnamed, 187–188
duplication access checks, 269–272
finding open handles by name, 57
finding token handles to impersonate, 139–140
handle tables, 35
handles (continued)
   pseudo, 48, 108–109
   registry, 80
   windows, 73
Handles property, 18–19
hash-based message authentication
codes (HMACs), 429
hashtable type, 5
highestAvailable UAC execution
level, 126
HKEY_CLASSES_ROOT handle, 90
Hyper-V, 47, 537–538

I
IBM OS/2 operating system, 64, 85
Identification impersonation level, 105–106, 136
Identify request attribute flag, 519–520
identity tokens, 519–520
Id property, 14, 284
IIS (Internet Information Services) web
server, 414
Image type, 53
Impersonate access right, 100, 104, 107
Impersonation impersonation level, 105
Impersonation pseudo token
   handle, 108
impersonation tokens, 104–107
   explicit token impersonation, 107
   impersonation context, 104
   SQoS, 104–107
Import commands, 5, 20, 65–66
importing data, 20–21
InfoOnly parameter, 47, 314
InformationClass parameter, 43
inheritance, 215
   auto-inheritance, 181
   behavior, 197
dangers, 212
   flags, 182, 194
   parent security descriptors,
   188–194
Inherit attribute flag, 42
Inherited ACE flag, 156, 158, 167, 212
InheritedObjectType GUID, 169,
   203–205
InheritOnly ACE flag, 156, 167
initialization vectors, 329–330
Initialize access right, 313
InitialOwner parameter, 32, 79
input/output (I/O) manager, 24–25,
   45–47
device drivers, 45
displaying device objects, 46
listing drivers, 47
opening device objects and
displaying volume path, 46–47
Install- commands, 4, 545
Int64 security attribute type, 260
Integrated Windows Authentication
   (IWA), 424
Integrity attribute flag, 112–113
IntegrityEnabled attribute, 112
integrity levels, 102, 112, 124, 137
interactive authentication, 397–419,
   458–464
   AP-REP message, 464
   AP-REQ message, 464
   AS-REP message, 459–461
   AS-REQ message, 458
   creating new processes with
tokens, 412–413
   creating user desktops, 398–399
   initial user authentication,
   458–462
   KDC service, 458
   LsaLogonUser API, 399–412
network service authentication,
   463–465
   pre-authentication data, 458
   privilege attribute certificates, 459
   Service logon type, 413–414
   service principal names, 460
   TGS-REP message, 461–462
   TGS-REQ message, 460–461
ticket granting servers, 459
ticket granting tickets, 459
tickets, 458
   worked examples, 414–419
Internet Explorer, 118–119
Internet Information Services (IIS)
   web server, 414
int type, 5
Invoke-commands, 14, 105
I/O manager. See input/output manager
ISE (PowerShell Integrated Scripting Environment), 261
IsFiltered flag, 128, 269
IsRestricted flag, 269
IWA (Integrated Windows Authentication), 424

J
John the Ripper, 496

K
KDC service. See key distribution center service
Kerberos, 457–497
    AP-REP message decryption, 476–477
    AP-REQ message decryption, 469–476
    CredSSP protocol, 512
cross-domain authentication, 477–479
deviation, 479–491
double hop problem, 435
golden tickets, 462–463
interactive authentication, 458–464
PKINIT, 477
    via PowerShell, 465–469
service principal names, 443
silver tickets, 465
U2U authentication, 491–493
    worked examples, 493–496
Kerberos Credential (KRB-CRED), 483
Kerberos-only delegation (Service for User to Proxy), 485–486, 490
KERNEL32 library, 64–65
KERNELBASE library, 64–65
kernel-mode access checks, 222–225
    access mode, 223–224
    memory pointer checking, 224–225
    parameters, 222
KernelObjects OMNS directory, 75
key distribution center (KDC) service
cross-domain authentication, 478
decrypting AP-REQ message, 473, 475
initial user authentication, 458, 477
Kerberos-only delegation, 485
network service authentication, 463–464
protocol transition delegation, 486–487
resource-based delegation, 490
U2U authentication, 491
unconstrained delegation, 481
KeyExchange flag, 441
key version numbers, 467
KeywordsDisplayNames property, 290
KnownDlls OMNS directory, 69–70
KRB-CRED (Kerberos Credential), 483

L
LAN Manager (LM), 306, 327
Less Privileged AppContainers (LPACs), 246
linked tokens, 126–129, 262
List access right, 366–367, 369
ListAccounts access right, 315
ListGroups access right, 316
ListMembers access right, 318
ListObject access right, 366, 369
LM (LAN Manager), 306, 327
    local authentication, 299–301, 398
    local domains, 300
    LsaLogonUser API, 401–402
    user database, 305
LocalCall flag, 436
local domain configuration, 300, 305–311
    LSA policy database, 309–312
    user database, 305–309
local loopback authentication, 435–436
locally unique identifiers (LUIDs), 102–103
Local Security Authority (LSA), 305, 309–324
  extracting system keys, 327–328
  logon account rights, 310–311
  privilege account rights, 310
  remote services, 311–324
Local Security Authority Subsystem (LSASS), 26, 92
  creating tokens, 131–133
  enumerating SIDs, 175–176
  finding resources with audit ACEs, 295
  linked tokens, 128
  logon sessions, 102
local security policies, 282
logon account rights, 310–311, 415–416
LogonId attribute, 111, 405
logon types, 400, 402, 408–412
  Network logon type, 409–411
  NewCredentials logon type, 438
  Service logon type, 413–414
LogonUI process, 92, 398
LongPathsEnabled value, 87
long type, 5
Lookup access right, 315
LookupDomain access right, 313–314
LookupNames access right, 319, 323
lowbox tokens, 120–122, 246–249, 273, 520–523
LPACs (Less Privileged AppContainers), 246
LParam parameter, 74
lpMutexAttributes parameter, 78
lpName parameter, 78
LSA. See Local Security Authority
LsaLogonUser API, 399–414
  accessing from PowerShell, 410–412
  creating user desktops, 398–399
  domain authentication, 403–404
  local authentication, 401–402
  logon and console sessions, 404–406
  logon types, 400
  protocol transition delegation, 489
security packages, 400–401
token creation, 407–410
LSASS. See Local Security Authority Subsystem
LuaToken flag, 128, 140
LUIDs (locally unique identifiers), 102–103
M
mandatory access checks (MACs), 228–237
  access filter ACEs, 233–235
  lowbox tokens, 247–248
  mandatory integrity level check, 235–237
  process trust level check, 231–233
mandatory access control, 102, 143
Mandatory attribute, 110
Mandatory Integrity Control (MIC), 230
mandatory integrity level check, 235–237
mandatory label ACEs, 154, 167
  access strings, 172
  assigning security descriptors during resource creation, 201–203
  integrity level SIDs, 172
MandatoryLabel security authority, 112
mandatory policy values, 161
MapGenericRights parameter, 39
MapWrite access, 52, 58
MD4 hashes, 306, 432
MD5 hashes, 329, 431, 466
memory manager, 49–54
  finding writable and executable memory, 60–61
  NtVirtualMemory commands, 49–51
pagefiles, 49
prefix, 25
Section objects, 51–54
virtual memory space, 49
memory pointer checking, 224–225
message integrity codes (MICs), 425, 429, 433
message loops, 73
Microsoft Visual Studio, 261, 538
ModifyState access, 42, 270–271
Mutant objects, 29–30, 181, 187, 193
mutual authentication, 464
MutualAuth flag, 483
MutualAuthRequired flag, 469

N
Nagle algorithm, 448
NAT (network address translation), 537
Negotiate security package, 401,
503–505
initializing, 503–505
security mechanisms, 504
specifying credentials, 504
NegotiateStream class, 445
NetCredentialsOnly flag, 413
Netlogon protocol, 342, 403
network address translation (NAT), 537
network authentication, 421–455
credentials, 407
lowbox tokens, 520–523
NTLM network authentication, 422–438
NTLM relay attacks, 438–445
worked example, 445–454
Network Level Authentication
(NLA), 511
Network logon type, 409–411
NewCommands, 8, 12–13, 46, 51–53,
56, 81, 85, 88–89, 132–133,
157, 251, 273, 306–307,
309, 325, 361, 381,
389–390, 424, 500, 507,
537, 539
NewCredentials logon type, 438
NewFunction, 189, 232, 538–539
NewGuid static method, 8
NLA (Network Level
Authentication), 511
None ACE flag, 193
NoPropagateInherit ACE flag, 156, 167,
193–194
NoRightsUpgrade flag, 188, 270–271
Notification access right, 319
Nt (Zw) prefix, 24, 29–30, 224
NtAccessCheck system calls, 225–227,
249, 254, 291
NtAdjust system calls, 110, 114–115
NtAllocate system calls, 49–50,
102, 409
NtChallengeResponse system call, 433
NtCloseObjectAuditAlarm system call, 291
NtCreate system calls, 29–30, 55, 77,
116, 120, 132
NTDLL (NT Layer dynamic link
library), 65–66
NtDuplicate system calls, 41, 107
NtFilterToken system call, 117
NtFreeVirtualMemory system call, 49
NT hashes, 306, 326–327, 332, 334
NtImpersonate system calls, 106–107
NTLM (NT LAN Manager)
flags, 425, 427
network authentication, 422–438
authentication tokens, 423
bypassing proxy check, 523–524
cracking user passwords, 428–429
CredSSP protocol, 512
cryptographic derivation
process, 431–433
explicit credentials, 437
impersonating tokens,
437–438
local administrators, 430–431
local loopback authentication,
435–436
Negotiate security package,
503–505
pass-through authentication,
434–435
variants of, 422
via PowerShell, 423–430
relay attacks, 438–445
active server challenges, 440
channel binding, 444–445
example of, 439
signing and sealing, 440–443
target names, 443
security package, 401
NtLoadDriver system call, 45, 116
NtMake system calls, 40–41
NtMapViewOfSection system call, 51
NtObjectManager module, xx,
356, 359
NtOpen system calls, 100, 291
NtPrivilegeCheck system call, 115
NtQuery system calls, 30, 39, 47, 49, 126, 179–180
NtReadVirtualMemory system call, 49
NtSecurityDescriptor attribute, 358, 380
NtSetInformation system calls, 107, 128, 131–132, 135
NtSetSecurityObject system call, 205–206
NTSTATUS codes, 32–35, 77–78
NtWriteVirtualMemory system call, 49
NullSession request attribute flag, 518

O
ObjectAccess audit category, 284–285
ObjectAttributes parameter, 30–31
OBJECT_ATTRIBUTES structure, 30–32
ObjectClass attribute, 351, 355
ObjectInherit ACE flag, 156, 167
object manager, 24, 180–181
  displaying object types, 27–28
DOS device paths, 83–84
finding owners, 216–218
NTSTATUS codes, 32–35
object directories, 29
object handles, 35–42
object manager namespace, 28
  automating access checks, 275–276
  permanent objects, 40–41
registry, 55
traversal checking, 266–267
Win32 registry paths, 80–82
prefix, 24
system calls, 29–32
  Query and Set system calls, 42–45
ObjectName parameter, 31–32, 291
objects
  accessing properties, 8
attribute flags, 32
creating, 8
directories, 29
displaying, 14–17, 27
filtering, 18–19
finding shared objects, 57–59
  grouping, 19
handles, 30, 35–42, 187–188
invoking methods, 8
naming, 31
permanent, 40–41
sorting, 18–19
object type access checks, 249–255
ObjectType GUID, 169, 203–205
ObjectTypes parameter, 249, 251–253
Oem NTLM flag, 427
OkAsDelegate flag, 481–483
OMNS. See object manager namespace under object manager
operators, 6, 14, 18
  infix, 171
  unary, 170
Oracle VirtualBox, 537
organizational units, 385–386
Out commands, 16–17, 20, 54, 60
Owner attribute, 111
owner check, 184, 240–241
Owner security information flag, 184

P
pagefiles, 49
Paging parameter, 16
Parameter command, 11
parameters, 9, 11
parent security descriptors, 180, 182, 185–203
  inheritance rules, 215
  setting both creator and parent, 195–200
  setting neither creator nor parent, 185–188
  setting parent only, 188–195
pass-the-hash technique, 306
pass-through authentication, 434–435
PassThru parameter, 17, 285
Password-Based Key Derivation Function 2 (PBKDFv2)
  algorithm, 471
password encryption keys (PEKs)
  decrypting, 328–330
  decrypting password hashes, 330–332
Path parameter, 9
PDC (primary domain controller) emulator, 345
Persistent attribute flag, 40
per-user audit policies, 285–287
PIDs (process IDs), 47–48
pipeline (|), 9
PkgParams buffer flag, 500–501
PKINIT (Public Key Initial Authentication), 477
Plug and Play (PnP) manager, 45
POSIX, 64, 85, 145
PowerShell, 3–21
configuring, 4–5
discovering commands, 10
displaying and manipulating objects, 14–17
equivalent SDK names, 38
executing commands, 9–10
exporting data, 20–21
expressions, 5–8
filtering objects, 17–19
functions, 13–14
getting help, 10–13
grouping objects, 19
Integrated Scripting Environment, 261
line breaks, xxviii
modules, 4–5
operators, 6
script execution policy, 4–5
sorting objects, 18–19
string character escapes, 7–8
string interpolation, 7
style conventions for examples in book, xxvii–xxviii
types, 5–6, 8
variables, 6–7
versions of, 3–4
pre-authentication data, 458–459
PreviousMode value, 223–224
primary domain controller (PDC) emulator, 345
Primary tokens, 100, 108, 133–134
Principal parameter, 249–250
print Shell verb, 90–91
printto Shell verb, 90–91
privilege attribute certificates (PACs), 408
cross-domain authentication, 478–479
decrypting AP-REQ message, 472–475
delegation, 487
golden tickets, 462
initial user authentication, 458–462
network service authentication, 464
silver tickets, 465
privilege checks, 238–239
process and thread manager, 24, 47–48
displaying processes and threads, 47–48
opening processes and threads, 48
prefix, 25
process and thread IDs, 47
process creation, 87–91
command line parsing, 88–89
Shell APIs, 89–91
process IDs (PIDs), 47–48
ProcessName property, 14, 19
Process objects, 18, 42
Process parameter, 49
ProcessTrustLabel ACEs, 154, 167
process trust level checks, 231–233
property sets, 251, 373–376
ProtectedDacl security information flag, 210–211, 364
ProtectedData class, 516
protected objects, 381–382
protected processes, 231–233
ProtectedSacl security information flag, 210
ProtectFromClose attribute, 42
Protect-LsaContextMessage command, 441
protocol transition delegation (Service for User to Self), 486–488, 490
Proxy Auto-Configuration (PAC) scripts, 521
pseudo handles, 48, 108–109
Public Key Initial Authentication (PKINIT), 477
Q
Query access right, 100
QueryInformation class, 45
QueryInformation system call verb, 30
QueryLimitedInformation access right, 49, 61
QueryMiscPolicy access right, 287
QuerySource access right, 100
Query system call, 42–45
QuerySystemPolicy access right, 287
QueryUserPolicy access right, 287
QueryValue access right, 322

R
rainbow tables, 429
RC4 encryption algorithm, 327–328, 331, 442, 466, 470
RDP (Remote Desktop Protocol), 75, 77
RDS (Remote Desktop Services), 74, 77
ReadAccount access right, 316
Read- commands, 49–51, 307, 410
ReadControl access right, 36, 178, 240–241
ReadGeneral access right, 316
ReadGroupInformation access right, 316
ReadInformation access right, 318
ReadLogon access right, 316
ReadOnly buffer flag, 501
ReadOnly protection state, 49
ReadOnlyWithChecksum buffer flag, 501
ReadOtherParameters access right, 315
ReadPasswordParameters access right, 314–315
ReadPreferences access right, 316
ReadProp access right, 366, 370
Read-TlsRecordToken function, 532
Receive- functions, 448
referral tickets, 478–479
regedit application, 80
registry (configuration manager), 24, 55–56
attachment points, 56
hives, 56
keys and values, 55–56
prefix, 25
relative distinguished names, 349–350
relative identifiers (RIDs), 26, 112
AppContainer and lowbox tokens, 120–121
cycling, 323, 336–337
mandatory integrity level checks, 235
SID structure, 146–149
user database, 306–308
relative security descriptors, 149–151, 163–164
RemainingAccess value, 229–230
remote access check protocol, 389–390
Remote Credential Guard, 513
Remote Desktop Protocol (RDP), 75, 77
Remote Desktop Services (RDS), 74, 77
remote procedure calls (RPCs), 55, 104
Remote Procedure Call Subsystem (RPCSS), 92–93
Remote Server Administration Tools (RSAT), 343–344
Remove- commands, 49–52, 56, 115, 308–309, 311, 324, 369, 416
RemoveMember access right, 318
Renewable flag, 472
requireAdministrator UAC execution level, 126
Reserve state value, 50
Reset-Win32SecurityDescriptor command, 211
Resolve- functions, 238, 240, 244
Resource attribute, 113, 408
ResourceAttribute ACEs, 154, 167
resource-based delegation, 489–491
resource manager flags, 144–145, 149
Restricted Admin mode, 513–514, 525
RestrictedKrbHost class, 467–468
restricted tokens, 117–119, 244–245
turn keyword, 13
RIDs. See relative identifiers
RmControlValid control flag, 149
RootDirectory parameter, 31–32
Root Directory System Agent Entry (RootDSE), 350
RPCs (remote procedure calls), 55, 104
RSAT (Remote Server Administration Tools), 343–344
RtlNewSecurityObjectEx system call, 182
Rubeus, 496
S
S4U. See constrained delegation
S4U2proxy (Service for User to Proxy), 485–486, 490
S4U2self (Service for User to Self), 486–488, 490
SaclAutoInherit auto-inherit flag, 209–210
Sacl control flags, 145, 166, 181
SACLs. See security access control lists
SAM. See security account manager
database; security account manager remote service
sandbox tokens, 117–122, 244–249
access checks, 272–274
lowbox tokens, 120–122, 246–249
restricted tokens, 117–118, 244–245
write-restricted tokens, 119
SAS (secure attention sequence), 399
SCM (service control manager), 92–93
ScopedPolicyId ACEs, 154, 167
script blocks, 14, 18
SDDL format. See Security Descriptor Definition Language format
SDK (software development kit), 38, 110, 112
SDKName property, 38, 161
Search-Win32SecurityDescriptor command, 212–213
SeAssignPrimaryTokenPrivilege privilege, 116
SeAuditPrivilege privilege, 116
SeBackupPrivilege privilege, 116, 123
SeBatchLogonRight account right, 311, 402, 416
SeChangeNotifyPrivilege privilege, 116, 267
secpol.msc command, 282
SeCreateTokenPrivilege privilege, 116, 123, 132
Section objects, 217
creating sections and mapping to memory, 51–52
finding shared, 57–59
finding writable, 278–279
listing mapped files with names, 53
mapping and viewing loaded images, 53–54
modifying mapped sections, 59–60
secure attention sequence (SAS), 399
secure channel, 506–510
encrypting and decrypting application data, 508–509
extracting server TLS certificates, 530–533
inspecting connection information, 508
setting up, 506–507
TLS record structure, 507
Secure Sockets Layer (SSL) protocol, 506–507
SecureString class, 307
security access control lists (SACLs), 145–146
control flags, 144–145, 166, 181
global, 292–293
resource, 288–291
security access tokens
administrator users, 122–124
assigning, 133–138
converting/duplicating, 107–108
creating, 131–133
groups, 109–113
impersonation tokens, 104–107, 136–138
integrity levels, 102
primary tokens, 100–104, 133–136
privileges, 113–117
pseudo token handles, 108–109
sandbox tokens, 117–122
security attributes, 130–131, 172
Int64 security attribute type, 260
User Account Control, 124–130
worked examples, 138–141
security account manager (SAM)
database, 312, 324–334
accessing through registry, 325–334
security account manager (continued)
pre-Active Directory enterprise network configuration, 342
security account manager (SAM)
remote service, 312–318
access rights, 313
alias objects, 318
domain objects, 314
group objects, 317
user objects, 315–316
SECURITY_ATTRIBUTES structure, 78–79
security auditing, 281–295
audit policy security, 287–293
security event log, 282–286
worked examples, 287–295
security authority, 147
MandatoryLabel, 112
World, 219
SecurityBuffer class, 500
security buffers, 500
with authentication context, 501–502
with signing and sealing, 502–503
SECURITY database, 324, 334–336
Security Descriptor Definition Language (SDDL)
format, 26, 165–173
access strings, 168–169, 172
ACE flag strings, 167
ACL flag strings, 166
conditional expressions, 170–171
converting security descriptors to, 165
mandatory label integrity level SIDs, 172
ObjectType GUIDs used in AD, 169
security attribute SDDL type strings, 172
SID aliases, 166, 547–549
splitting components, 165
type strings mapped to ACE types, 167
SecurityDescriptor objects, 151, 157
security descriptors, 143–220
absolute and relative, 149–151
access control lists, 151–156
assigning
during resource creation, 180–205
to existing resources, 205–208
components of, 144–146
converting
to and from relative descriptors, 163–164
to SDDL format, 165
creating, 157–158
formatting, 159–163
inheritance behavior, 214–215
ordering ACEs, 158–159
reading, 178–179
SDDL format, 165–173
server security descriptors and compound ACEs, 213–214
SID structure, 146–149
standardization, 362
structure of, 144
Win32 security APIs, 208–213
worked examples, 173–176, 216–219
security event log, 282–286
audit events and event IDs, 282
audit policy subcategories, 284
configuring
per-user audit policy, 285–286
system audit policy, 282–285
displaying category GUIDs, 284
setting policy and viewing resulting policy list, 284–285
top-level audit policy categories, 283
security identifiers (SIDs), 26–27, 81, 146–149
administrator users, 124
aliases, 166, 547–549
arbitrary owner, 184
asserted identities, 489–490
assigning tokens, 137
capability, 120–121
capability groups, 121
components of, 146–147
creating tokens, 132–133
device groups, 113
enumerating, 175–176
fixed logon sessions, 102
group, 145
integrity levels, 112
logon types, 408–409, 414
lowbox tokens, 120–122
machine, 306
mandatory label integrity level, 172
manually parsing binary, 173–175
owner, 145
process trust level, 231–232
pseudo token handles, 109
querying Administrators group SID, 148
replacing CREATOR OWNER
and CREATOR GROUP SIDs, 200
restricted tokens, 117–118
SDDL SID alias mapping, 547–549
SELF SID, 249–250, 379–380
token groups, 111–113
tokens, 101
SecurityInformation flags, 178, 205–206
Dacl, 211
Group, 157, 183
Owner, 184
ProtectedDacl, 210–211, 364
ProtectedSacl, 210
UnprotectedDacl, 210–211
UnprotectedSacl, 210
security packages (security support providers), 400–401, 499–533
anonymous sessions, 518–519
authentication audit event log, 524–527
credential manager, 514–517
CredSSP, 510–513
identity tokens, 519–520
Negotiate, 401, 503–505
network authentication with lowbox token, 520–523
Remote Credential Guard, 513
Restricted Admin mode, 513–514
secure channel, 506–510
security buffers, 500–503
worked examples, 527–533
Security Quality of Service (SQoS), 32, 104–107
context tracking mode, 106
effective token mode, 106
impersonation levels, 104–106
SECURITY_QUALITY_OF_SERVICE structure, 104, 107
Security Reference Monitor (SRM), 24–27
access checks, 25
process, 221–263
use cases, 265–280
access tokens, 25
audit events, 26
components of, 25
Local Security Authority Subsystem, 26
prefix, 24
security access tokens, 99–141
security auditing, 281–295
security descriptors, 143–176
security identifiers, 26–27
SECURITY_SQOS_PRESENT flag, 107
SECURITY_SUBJECT_CONTEXT structure, 222, 272
Security Support Provider Interface (SSPI), 424, 440, 476, 500, 518
security support providers. See security packages
SeDebugPrivilege privilege, 116, 123
SeDenyBatchLogonRight account right, 311, 402
SeDenyInteractiveLogonRight account right, 311, 402
SeDenyNetworkLogonRight account right, 311, 402
SeDenyRemoteInteractive account right, 402
SeDenyRemoteInteractiveLogonRight logon right, 311
SeDenyServiceLogonRight account right, 311, 402
SeEnableDelegationPrivilege privilege, 381
SeFastTraverseCheck function, 268
SeImpersonatePrivilege privilege, 116, 123
SeInteractiveLogonRight account right, 311, 402
SeIsTokenAssignableToProcess function, 134
Select-HiddenValue function, 95–96
Select-Object command, 14–15, 17
Self access right, 366, 378–379
SelfRelative control flag, 149–151
SeLoadDriverPrivilege privilege, 116, 123
SeMachineAccountPrivilege privilege, 380
Send- functions, 448–449
SeNetworkLogonRight account right, 311, 402
sequence numbers, 442
SeRelabelPrivilege privilege, 117, 123, 202, 239
SeRemoteInteractiveLogonRight account right, 311, 402
SeRestorePrivilege privilege, 116, 123, 219
ServerAdmin access right, 319
Server Message Block (SMB), 105, 422, 380, 439–440, 442
ServerSecurity control flag, 213–214
service control manager (SCM), 92–93
Service for User. See constrained delegation
Service for User to Proxy (aka S4U2proxy or Kerberos-only delegation), 485–486, 490
Service for User to Self (aka S4U2self or protocol transition delegation), 486–488, 490
Service logon type, 413–414
service principal names (SPNs), 443
authentication
cross-domain, 478
with explicit credentials, 522
initial user, 460–462
Kerberos authentication in PowerShell, 466
to known web proxies, 522
network service, 463–464
U2U, 491–493
bypassing proxy check, 523–524
decrypting AP-REQ message, 469–470
delegation, 482, 484, 486, 488–490
SeServiceLogonRight account right, 311, 402
Session 0 Isolation feature, 76
Session Manager Subsystem (SMSS), 92
Session objects, 75
SeTakeOwnershipPrivilege privilege, 117, 123, 239
SetAuditRequirements access right, 319
SeTcbPrivilege privilege, 116, 123
Set- commands, 44, 49–51, 56, 110, 135, 209–210, 286–288, 469, 486, 489, 539
SetDefaultQuotaLimits access right, 319
SeTimeZonePrivilege privilege, 115–116
SetInformation class, 30, 45
SetMiscPolicy access right, 287
SeTrustedCredmanAccessPrivilege privilege, 516–517
Set system call, 42–45, 99
SetSystemPolicy access right, 287
SetUserPolicy access right, 287
SetValue access right, 322
SHA256 algorithm, 121–122
SHA384 algorithm, 508
shatter attacks, 76
SHELL32 library, 89
Shell APIs, 89–91
shell verbs, 91
Show- commands, 60, 100, 104, 131, 162
ShowWindow parameter, 11–12
Shutdown access right, 313
sibling tokens, 134–135
SID aliases, 166, 548–549
SIDs. See security identifiers
SignatureType property, 55
signing and sealing
NTLM relay attacks, 440–443
security buffers, 502–503
silver tickets, 465
Simple and Protected Negotiation Mechanism (SPNEGO) protocol, 503–505
SingleHost flag, 429
SkipTokenGroups flag, 389
SMB (Server Message Block), 105, 422, 439–440, 442
SMSS (Session Manager Subsystem), 92
INDEX

software development kit (SDK), 38, 110, 112
Sort-Object command, 18–19
split-token administrator, 124, 126, 128–129, 262
SPNEGO (Simple and Protected Negotiation Mechanism) protocol, 503–505
SPNs. See service principal names
SQoS. See Security Quality of Service
SRM. See Security Reference Monitor
SSL (Secure Sockets Layer) protocol, 506–507
SSPI (Security Support Provider Interface), 424, 440, 476, 500, 518
Start-command, 88, 276, 325
static methods, 8
Stream buffer flag, 500
StreamHeader buffer flag, 500, 509
StreamTrailer buffer flag, 500, 509
strings
  ANSI, 79
  character escapes, 7–8
  double-quoted, 7
  interpolation, 7
  secure, 307
  single-quoted, 7
  wide, 79
string type, 5
Structural category attribute, 354
SuccessfulAccess ACE flag, 156, 168
superiors, 367–368
SymbolicLink objects, 28–29
SymbolicLinkTarget property, 28–29
system audit policy, 282–285, 287
system calls
  common verbs, 30
  status codes, 34
  Win32 APIs and, 77–80
system processes, 91–93
  Local Security Authority Subsystem, 92
  service control manager, 92–93
  Session Manager Subsystem, 92
  Windows logon process, 92
SystemProcessInformation class, 47
T
TargetInfo flag, 427
TargetTypeDomain flag, 427
TargetTypeServer flag, 427
Task Scheduler service, 93
TCB (trusted computing base), 116
TCP, 446, 532
tcpClient objects, 452
TCP/IP, 47, 342
tcplisent class, 451
termServices, 77
test-AccessFilter check, 231
test-functions, 250, 393
test-MandatoryIntegrityLevel check, 231
test-ProcessTrustLevel check, 231
tgs-REP message. See ticket granting service reply message
tgs-REQ message. See ticket granting service request message
tGs. See ticket granting servers
tGT-REP (ticket granting ticket reply) message, 491–493
tGT-REQ (ticket granting ticket request) message, 491–492
tGTs. See ticket granting tickets
thread affinity, 73
thread IDs (TIDs), 47–48
Thread objects, 27, 48, 203
ticket granting servers (TGSs)
  cross-domain authentication, 478–479
decrypting AP-REQ message, 469
degaintenance, 479–482, 485
initial user authentication, 459–461
Kerberos authentication in PowerShell, 466
network service authentication, 464
ticket granting service reply (TGS-REP) message
  initial user authentication, 458, 461–462
Kerberos authentication in PowerShell, 466
ticket granting service reply (continued)
  network service authentication, 464
ticket granting service request
  (TGS-REQ) message
delegation, 479, 481, 485
initial user authentication, 458
Kerberos authentication in
  PowerShell, 466
network service authentication,
  463–464
U2U authentication, 492
ticket granting ticket reply (TGT-REP)
  message, 491–493
ticket granting ticket request (TGT-
  REQ) message, 491–492
ticket granting tickets (TGTs)
delegation, 479–485
initial user authentication, 459–461
network service authentication,
  463–464
U2U authentication, 491–493
TIDs (thread IDs), 47–48
TLS protocol. See Transport Layer
  Security protocol
ToCharArray method, 8
token access checks, 227–228, 230,
  237–241
owner check, 240–241
privilege check, 238–239
Token buffer flag, 500–502
TokenLinkedToken class, 126, 128
Token objects
  creating, 407–410
  creating new processes with,
    412–413
  requesting for authenticated
    users, 430
Token Viewer application, 100–101, 103
Transport Layer Security (TLS)
  protocol
channel binding, 444–445
CredSSP, 511–512
extracting certificates, 530–533
secure channel, 506–510
traversal checks, 266–269
limited checks, 267–269
SeChangeNotifyPrivilege
  privilege, 267
Traverse access right, 266–269
TrustAdmin access right, 319
trusted computing base (TCB), 116
TrustedForDelegation control flag,
  381, 482
TrustedToAuthenticateForDelegation
  control flag, 381
TrustedToAuthForDelegation flag,
  487–489
TrustProtected ACE flag, 156, 168
trust relationships, 303–304, 322,
  477–479
TS Service Security Package (TSSSP),
  511–512
Type objects, 27
types, 5, 8
U
  U2U (User-to-User) authentication,
    491–493
UAC. See User Account Control
UIPI (User Interface Privilege
  Isolation), 76, 129
UMFD (user-mode font driver) process,
  92, 405
unconstrained delegation, 480–484
Unicode NTLM flag, 427
UNICODE_STRING structure, 31,
  85–86
Universal group scope, 347, 354
Unprotect- commands, 441, 446,
  471, 476
UnprotectedDacl security information
  flag, 210–211
UnprotectedSacl security information
  flag, 210
Unprotect- functions, 328–331
Update- commands, 4–5,
  427–428
UPNs (user principal names), 345
UseForDenyOnly attribute, 111–112
USER32 library, 70–71
User Account Control (UAC), 93,
  124–126, 409
elevation type, 126–129
execution levels, 126
filtering, 416
linked tokens, 126–129
Index

querying executable manifest information, 125
UI access, 129, 138–139
virtualization, 129–130
User-Account-Restrictions property set, 374–375
User-Change-Password access right, 377–378
user delegation rights, 381
user desktop creation, 398–399
User-Force-Change-Password access right, 377–378
User Interface Privilege Isolation (UIPI), 76, 129
user-mode access checks, 225
user-mode applications, 64–96
  DOS device paths, 83–87
  process creation, 87–91
  system processes, 91–93
Win32
  APIs, 64–70, 77–80
  GUI, 70–77
  registry paths, 80–82
  worked examples, 94–96
user-mode font driver (UMFD) process, 92, 405
user principal names (UPNs), 345
User-to-User (U2U) authentication, 491–493

V
variables
  enumerating all, 7
  predefined, 6–7
$VerbosePreference global variable, 454
View access right, 320
ViewAuditInformation access right, 319
ViewLocalInformation access right, 319–320
VirtualBox, 537
virtualization, 129–130, 484
VirtualizationEnabled property, 130
Visual Studio, 261, 538
VMS, 292

W
WarningAction parameter, 276
WebClient class, 522
Where-Object command, 17–19
wide strings, 79
wildcard syntax, 10–11, 15
Win32
  APIs, 64–70
    loading new libraries, 65–66
    searching for DLLs, 68–70
    security APIs, 208–213
    system calls and, 77–80
    viewing imported APIs, 66–67
  GUI, 70–77
    console sessions, 74–77
    kernel resources, 71–73
    modules, 70
    window messages, 73–74
  registry paths, 80–82
  handles, 80–81
  HKEY_CLASSES_ROOT handle, 90
  listing registry contents, 81–82
  opening keys, 81
WIN32K driver, 70–71
Win32Path parameter, 81
WIN32ULibrary, 70–71
window
  classes, 73
  messages, 73–74
  objects, 71–73
Windows authentication, 299–340
  Active Directory, 341–396
  domain authentication, 300–304
  interactive authentication, 397–419
  local domain configuration, 305–311
  network authentication, 299, 421–455
  remote LSA services, 311–324
  SAM database, 324–334
  SECURITY database, 334–336
  worked examples, 336–339
Windows domain network, 535–545
  configuration, 536
  virtual machines, 538–545
Windows Hyper-V, 47, 537–538
Windows Installer service, 93
Windows kernel, 23–61
  subsystems and components of, 24–56
Windows kernel (continued)
user-mode applications, 64–96
worked examples, 56–61
Windows operating system, xxviii
PowerShell testing environment setup, 3–21
user-mode applications, 64–96
Windows kernel, 23–56
Windows Subsystem for Linux, 64
WindowStation objects, 71–72
Windows Update service, 4, 93
Winlogon process, 75, 398–399, 408
WinRM protocol, 513
WinSock API, 47
WM_CLOSE message, 73
WM_GETTEXT message, 74
WM_TIMER message, 76
World security authority, 219
WParam parameter, 74
WriteAccount access right, 316, 318
Write-commands, 16, 49–50, 59, 291, 448, 454
WriteDac access right, 36, 205–206, 233, 235, 365
WriteGroupInformation access right, 316
WriteOtherParameters access right, 315
WriteOwner access right, 37, 117, 205–206, 239
WritePasswordParams access right, 314
WritePreferences access right, 316
WriteProp access right, 366, 370, 372, 375, 378
write-restricted tokens, 119
write-validated access rights, 378–379
X
X.509 certificates, 342, 507
XML, 20, 528–529
Z
Zerologon (CVE-2020-1472) security issue, 403
Zw (Nt) prefix, 24, 29–30, 224