INDEX

Numerics

128-bit certificates, 353
128-bit SuperCert, 352
3DES, 348

A

access, limiting on web servers, 170–174
   based on IP address, 180, 184
   secure authentication, 178–179
access lists
   extended, 447–448
   standard, 446–447
Account Policies
   NSA template, 102–103
   Windows NT 4, configuring, 66–68
ACEs (access control entries), 55
ACLs (access control lists)
   applying, 448
   DACLs, 441
   dynamic ACLs, Lock and Key, 452–456
   editing, 445
   first-level filtering, 449
   IP standard ACLs, 442
   protecting control plane, 450
   rules, 442
   inverse masks, 443
   named lists, 444
   numbered lists, 444
   sanity checking, 450
activating CBAC, 461–462
active FTP, 216
ActiveX controls
   Internet Exploder, 256
   protecting against dangerous content, 255–256
AD (Active Directory), 54
   forests, 84–85
   Global Catalog, 84
   objects, 84
   trees, 84–85
adding
   components to IE6, 321, 324
   third-party programs to IEAK base build, 294
addressing
   DHCP, 28
   DNS, 28
   NAT, 30–31
administrative users, vulnerability to malicious
   ActiveX controls, 256
Adware, 528
All Permissions permission (Windows NT 4), 57
anonymous user accounts for Serv-U FTP servers,
   232–233
AntiSpoofing, 499
APIs (application programming interfaces),
   255–256
appearance of IE6, customizing, 309–320
applets, 253
application developers, password security standards,
   40–41
application layer
   OSI reference model, 6
   TCP/IP model, 7
application mappings (IIS), deleting, 202
application protection, enabling on IIS, 200
applications
   adding to IE6, 321, 324
   AVPs, 527–529
   buffer overflow vulnerabilities, 526
   Ethereal, 224
   file extensions, suppressing, 116, 119
   helper applications, 251
   Outlook Express, configuring, 323
   applying, 113
   ACLs, 448
   control plane, protecting, 450
   first-level filtering, 449
   sanity checking, 450
   Internet Scanner policies, 78–83
   permissions to Windows NT 4 user accounts,
      56–62
   security policies, 47
   security templates to web servers, 101–116
   service packs, 517
ARP (Address Resolution Protocol) headers, 13
assigning web server operators, 208–210
asymmetric encryption, 349–350
   Message Digest, 351
asymmetric keys, 27
attacks
DDoS, 18
DoS, 18, 255
hackers, 34
auditing Windows NT 4, 70–74
authentication
Base64 encoded data, 174
CAs, responsibilities of, 352–353
IIS4, NT Challenge/Response, 178–179
LEAP, 525
passwords, defining security policies, 38–41
public/private key systems, 41
restricting access on web servers, 170–174, 178
automatic configuration of CBAC, 462, 466, 472, 475–482
automatic fixes with HFNetChk, 513–516
Automatic Update feature (Internet Explorer), disabling, 267
AVPs (Antivirus Programs), 527–529
OptOut, 529

B

banner ad companies, cookie abuse, 269
Base64 coded credentials
authentication data, 174
capturing, 569
decoding, 570–571
Basic page, source code, 577
bastion hosts, 436–437
belt and braces firewall architecture, 440
browser certificates, 421
installing, 425
requesting, 422, 425
browsers
CA compatibility, 378
cookies, 268
banner ad companies, 269
managing, 269
IE6
built-in error messages, customizing, 561–566
customizing, 309–324
setting home page, 312
zones, configuring, 259–267
IEAK
completing installation, 329
configuring, 285, 289, 293
customizing, 296–307
downloading, 271, 277–278
installing, 280–284
licensing, 272–275
managing multiple INS files, 342
policies, configuring, 323–326
Profile Manager, 336–340
plug-ins, 251
UAS, 314
buffer overflow vulnerabilities, 526
built-in error messages (IE), customizing, 561–566
bytecode, 252

C

Caesar ciphers, 348
calculating inverse masks, 443
capturing Base64 coded credentials, 569
CAs (certification authorities)
certificate issuance, 392
chaining, 360
CRLs, maintaining, 360
requesting, 368
for IIS4 web servers, 369–378
for IIS5 web servers, 379–387, 391
responsibilities of, 352–353
trusting, 416–420
verification of identity, 353
CBAC (content-based access control), 457–460
activating, 461–462
automatic configuration, 462–466, 472–482
Certificate Server (Microsoft), installing, 361–363, 367
certificates
contents, 354
installing
on IIS4, 395–405
on IIS5, 407, 411, 414
on web servers, 394
SSL, 354
types of, 352
CGI script timeouts, configuring, 207
chaining CAs, 360
Chapman firewall architecture, 439
characteristics of effective passwords, 39
CIA (Confidentiality, Integrity, Availability), 34
Cisco PIX Firewall, 484
architecture, 487
comparing to IOS Firewall, 485–487
configuring, 487–490
PDM, configuring, 490–500, 506
Cisco Wireless LAN Extensible Authentication Protocol, 525
classic firewall design, 438–439
client installation, FTP Voyager, 242–245
commercial scanners, inherent risks of using, 80
completing IEAK installation, 329
components of Windows NT 4 file system security, 55
Computer Security Institute, 435
concatenation, Denial of Service attacks, 255
configuring
Cisco PIX Firewall, 487–490
PDM, 490–500, 506
IEAK
customization, 296–307
gathering setup information, 285, 289
policies, 323–326
specifying setup parameters, 293
IIS session timeout, 207
Outlook Express, 323
PCs for zone detection, 257–259
Internet zone, 259–265
Intranet zone, 265–267
Window NT 4 security
account policies, 66–68
auditing, 70–74
disabling unnecessary services, 76
group rights, 68–69
connections
Internet Connection Sharing, 535
TCP flags, 16–18
Control field (802.2 LLC sublayer), 11
control plane, 450
cookies, 268–269
Corporate restrictions (Profile Manager)
configuring, 338–340
CPS (Certification Practice Statement), 353
creating
security policies, 44–45
policy review team, 45
topics to include, 46
Serv-U anonymous user accounts, 232–233
user accounts for web servers, 174–178
critical updates for Windows products, 510
CRLs (Certificate Revocation Lists), maintaining, 354–360
customizing
built-in error messages, 561–566
IE6, 309–320
adding components, 321, 324, 332
home page, 312
IEAK, 296–307

D

DAC (Discretionary Access Control), 53
DACLS (Discretionary Access Control Lists), 53–55, 441
DAD (Disclosure, Alteration, Denial), 34
dangerous content
ActiveX, 255–256
Java, 252–253
JavaScript, 254–255
VBScript, 255
data link layer (OSI reference model), 6
headers, 8
Ethernet II, 8–9
IEEE 802.3, 9
LLC sublayer, 10
data plane, 450
databases
Metabase (IIS5), relocating, 187, 192, 196
Microsoft Knowledge Base, 515
datagrams, 7
DDoS (Distributed Denial of Service) attacks, 18
Debug Programs right, 69
decoding Base64 coded credentials, 570–571
defining security policies, 36
examples, 42–44
password-related, 37–40
for application developers, 40–41
for remote access users, 41
deleting
sample applications on IIS, 204–207
unnecessary application mappings (IIS), 202
Developer Certificates, 353
development servers versus web servers, 167
DHCP (Dynamic Host Control Protocol), 28
directory permission, applying to Windows NT 4 users, 65
disabling
Automatic Update feature on Internet Explorer, 267
source-routing on Cisco routers, 12
unnecessary Windows NT 4 services, 76
DMZ (demilitarized zone), 437
DNS (Domain Name System), 28
DNSSEC, 28
document root, locating on web servers, 168
domains, 54
DoS (Denial of Service) attacks, 18, 255
  Syn Flood, thwarting, 483–484
dotted decimal notation, 28
downloading IEAK, 271, 277–278
DSAP (Destination Service Access Point) field,
  (802.2 LLC sublayer), 10
dumb terminals, 23–25
dynamic ACLs, Lock and Key, 452–456

effective password characteristics, 39
emphasizing security to staff, 552
  passwords, 553
  physical security, 552–553
  procedural security, 554
  telephone security, 554–555
enabling
  basic authentication on web servers, 172–178
  High protection on IIS, 201
  Windows NT 4 auditing, 70–74
encryption
  asymmetric, 349–351
  asymmetric keys, 27
  symmetric, 348
  WEP, 524
enforcing password security policies, 41
ephemeral ports, 16
error messages (IE)
  customizing, 561–565
  testing, 566
establishing PORT mode FTP sessions, 218–223
Ethereal, 224
  capturing Base64 encoded credentials, 569
Ethernet II data link headers, 8–9
Event Log (NSA template), 108
examples of security policies, 42–44
Execute permission (IIS5), managing, 199
extended ACLs, 442, 447–448
extensions, suppressing, 116, 119
external networks, 436
extranets, 436

fields
  of ARP headers, 13
  of Ethernet II data link headers, 8–9
  of IEEE 802.3 headers, 9
  of IP headers, 11–12
  of TCP headers, 14
  of UDP headers, 18
file extensions, suppressing, 116, 119
file system event logging (Windows NT 4),
  enabling, 70
File System page (NSA template), 113–116
firewalls
  bastion host, 437
  belt and braces architecture, 440
  Chapman architecture, 439
  classic design, 438–439
  DMZ, 437
  PIX, 484
    architecture, 487
    configuring, 487–500, 506
    versus IOS Firewall, 485–487
  separate server subnet, 440
  trusted networks, 438
first-level filtering, 449
fixes
  automating, 513–516
  mailing lists, 512
service packs
  applying, 517
  updating Windows 2000 to
    Service Pack 3, 519–523
SRPs, 516
  when to apply, 512
flags (TCP), 16–18
forests (AD), 84–85
formalization of RFC process, 224
frames, 7
FTP (File Transfer Protocol)
  operation of, 215
  PASV mode, session establishment, 221–223
  PORT mode, 215–216
session establishment, 218–221
session termination, 221
related RFCs, 225
secure FTP, 225
securing transactions, 224
Serv-U servers
  installing, 226–241
  testing, 246
  user types, 235
Voyager client
  installing, 242–245
  testing, 246
Full Control permission (Windows NT 4), 57

G

gateways, 12
gathering IEAK setup information, 285, 289
Global Catalog, 84
Graham-Leach-Billey Act, 34
group permissions, applying to Windows NT 4 user accounts, 60–62
group rights (Windows NT 4), configuring, 68–69

H

hackers, Script Kiddiez, 34
headers, 7
data link, 8
  Ethernet II, 8–9
  IEEE 802.3, 9
  LLC sublayer, 10
network layer, 11
  ARP, 13
  IP, 11–12
transport layer, 14
  ICMP, 20–21
  TCP, 14–18
  UDP, 18–19
helper applications, 251
HFNetChk
  automating security fixes, 513–516
  installing, 513
hidden web form fields, unauthorized manipulation, 526
hierarchical structure of AD, 84–85
High protection (IIS), enabling, 201
HIPPA (Health Insurance Privacy and Portability Act), 34
hoaxes, 529
home page (IE6), setting, 312
host-based firewalls. See personal firewalls
hosting multiple web servers, 212–213
hotfixes. See fixes
HTML (Hypertext Markup Language), 25
HTTP (Hypertext Transfer Protocol), 25
HTTPS (HTTP/SSL), 26
ICMP (Internet Control Message Protocol)
  Ping-of-Death messages, 12–13
  type codes, 20–21
identifying potential hackers, 34
IE6 (Internet Explorer 6)
  Automatic Update feature, disabling, 267
  components, installing 321, 324, 332
  customizing, 309–320
  error messages
    built-in error, customizing, 561–566
    testing, 566
  setting home page, 312
  UAS, extending, 314
  zones, configuring, 259–263, 267
IEAK (Internet Explorer Administration Kit)
  completing installation, 329
  customizing, 296–307
downloading, 271–278
  gathering setup information, 285, 289
  installing, 280, 284
  licensing, 272, 275
  managing multiple INS files, 342
  policies, configuring, 323–326
  Profile Manager
    CAB files, 341
    corporate restrictions, 338–340
    launching, 336–338
    specifying setup parameters, 293
IEEE 802.11b specification
  LEAP, 525
  MAC sublayer headers, 9
  WEP, 524
  WLAN risks, 524
IIS4
  application mappings, deleting, 202
  application protection, 200
authentication, NT Challenge/Response, 178–179
certificates, installing, 395–405
CGI script timeouts, configuring, 207
enabled basic authentication, 172–178
High protection, enabling, 201
installing on NT-4, 125–132
managing logging options, 169
NT-4 Option Pack, installing, 123
requesting CAs, 369–378
sample applications, deleting, 204, 207
IIS5
certificates, installing, 407, 414
installing, 134
issuing CAs, 392
Metabase, 187–196
requesting CAs, 379, 382–391
Windows 2000 installation, 135, 138, 146
Windows XP installation, 153–156, 162–164
implementing security policies, 47
importance of security, emphasizing to staff, 552
passwords, 553
physical security, 552–553
procedural, 554
telephones, 554–555
increasing user awareness, 555
INS files (IEAK), managing, 342
installing
browser certificates, 425
certificates
on IIS4, 395–405
on IIS5, 407–414
customized error messages, 564
FTP Voyager clients, 242–245
HFNetChk, 513
IE6 custom components, 332
IEAK, 280–284
IIS4
NT-4 Option Pack, 123–128, 132
IIS5, 134
on Windows 2000, 135–138, 146
on Windows XP, 153–164
Microsoft Certificate Server, 361–363, 367
security templates, 86, 89, 93
Serv-U FTP servers, 226–237, 240–241
ZoneAlarm Pro 3.0, 530, 535–542
internal networks, 438
Internet Connection Sharing, 535
Internet Explorer, 256
Internet Explorer. See IE6
Internet layer (TCP/IP model), 7
Internet Scanner, securing Windows NT 4 Web Server, 77–80
Internet zone security configuration, 259–265
intranets servers (Windows NT 4), applying permissions to users, 61–62
Intranet zone security configuration, 265–267
inverse masks, 443
IP extended ACLs, 442, 447–448
IP header fields, 11–12
IP standard access lists, 446–447
IPSec
transport mode, 21
tunnel mode, 21
ISO (International Organization for Standardization)
OSI reference model. See OSI reference model
issuing CAs for IIS5 Web servers, 392
IUSR_machine-name user account, removing permissions, 179

J
Java
protecting against dangerous content, 252–253
Sandbox, 253
JavaScript
protecting against dangerous content, 254–255
resource management, 254

K
Kensington Lock Slot, 552
keys, asymmetric, 27
Klez virus, 509

L
L5 NT Web Server policy (Internet Scanner), 78
laptops, Kensington Lock Slot, 552
launching IEAK Profile Manager, 336–338
layers of OSI reference model, 6
data link layer
Ethernet II data link headers, 8–9
headers, 8–10
IEEE 802.3 headers, 9
network layer
ARP headers, 13
headers, 11
IP headers, 11–12
transport layer, 14
ICMP header, 20–21
TCP header, 14–18
UDP header, 18–19
layers of TCP/IP model, 7
LEAP (LAN Extensible Authentication Protocol), 525
legislative security measures, 34
USA Patriot Act, 509
licensing IEAK, 272, 275
limiting access on web servers, 170–174, 178
based on IP address, 180, 184
secure authentication, 178–179
LiveScript, 254
LLC (Logical Link Control) sublayer, 8
Control field, 11
DSAP field, 10
SSAP field, 10
Local Policies (NSA template), 104, 107
locating
document root on web servers, 168
patches and service packs, 510
Lock and Key, 452–456
logging. See auditing
logs, maintaining on web servers, 169
ls command (UNIX), 220

M

MAC (Media Access Control) sublayer, 8
mailing lists for security fix updates, 512
maintaining
CRLs, 354–356, 360
secure logs on web servers, 169
malware, 527–528
managing
cookies, 269
IIS5 execute permissions, 199
multiple IEAK INS files, 342
multiple web server site hosting, 212–213
web server user account permissions, 197–198
maximum length field (buffer overflows), unauthorized manipulation, 526
members of policy review teams, 45
Message Digest, 351
Metabase (IIS5), relocating, 187, 192, 196
Microsoft VBScript, 255

O

OAK compiler, 252–253
operating systems
Windows 2000, IIS5 installation, 135, 138, 146
Windows NT 4 event logging, enabling, 70
Windows XP, IIS5 installation, 153–164
Operators (IIS), assigning, 208–210
OptOut, 529
OSI reference model, 6
upper layer protocols
DHCP, 28
DNS, 28
HTTP, 25
packet filtering, 437
ACLs, 442
  applying, 448–450
  control plane, protecting, 450
  editing, 445
  extended, 447–448
  rules, 442–444
  standard, 446–447
CBAC, 457–460
  activating, 461–462
  automatic configuration, 462–466, 472–477, 480–482
DACLs, 441
  Lock and Key, 452–456
packets, 7
  IP, security considerations, 12
passphrases, 41
Password Never Expires option (Windows), 175
passwords, 39
  defining security policies, 37–41
  emphasizing importance to staff, 553
  mnemonic, 553
  versus passphrases, 41
PASV mode FTP, 215
  session establishment, 221–223
PAT (Port Address Translation), 31
patches, 510. See also fixes
  automating with HFNetChk, 513, 516
  locating, 510
  mailing lists, 512
  SRPs, 516
PC zone detection, configuring, 257–267
PDM (PIX Device Manager), configuring, 490–500, 506
PDUs (Protocol Data Units), 26
permissions, 53
  All Permissions, 57
  applying to Windows NT 4 user accounts, 56–62
  directory permissions, applying to Windows NT 4 users, 65
  Execute (IIS5), managing, 199
  for web server user accounts, managing, 197–198
persistent cookies, 268
  banner ad companies, 269
  managing, 269
Personal Certificates, 353
personal firewalls, 529–530
  ZoneAlarm Pro 3.0
    installing, 530, 535–542
    operation, 544–546
physical layer (OSI reference model), 6
Ping-of-Death, 12–13
PIX Firewall, 484
  architecture, 487
  configuring, 487–490
  PDM, configuring, 490–500, 506
  versus IOS Firewall, 485–487
plug-ins, 251
policies
  emphasizing security to staff, 552–553
  IEAK, configuring, 323, 326
policy review team members, 45
port 20
  establishing PORT mode FTP sessions, 220–221
  terminating PORT mode FTP sessions, 221
PORT mode FTP, 215–216. See also PASV mode FTP
  session establishment, 218–220
  port 20, 220–221
  session termination, port 20, 221
port numbers, 16
  UDP, 19
ports, public access, 524
presentation layer (OSI reference model), 6
private addresses, 30
private keys, 349
privileged users, vulnerability to malicious ActiveX controls, 256
proactive security administration, 509
procedural security, emphasizing importance to staff, 554
Profile Manager
   CAB files, 341
   corporate restrictions, 338–340
   launching, 336–338
programming languages, OAK, 252–253
prohibiting access on web servers based on source
   IP address, 180, 184
protecting against dangerous content
   ActiveX, 255–256
   Java, 252–253
   JavaScript, 254–255
   VBScript, 255
public access ports, 524
public addresses, 30
public key, 349
public/private key systems, 41
pwd command (UNIX), 219

Q-R

reactive security administration, 509
Registry page (NSA template), 113
relocating IIS Metabase, 187–196
remote access users, password security standards, 41
   removing
      sample applications on IIS, 204–207
      unnecessary application mappings (IIS), 202
unnecessary Windows NT 4 services, 76
renaming Windows NT 4 user accounts, 69–70
requesting
   browser certificates, 422, 425
   CAs, 368
      for IIS4 Web servers, 369–378
      for IIS5 Web servers, 379–391
resource management, JavaScript, 254
responsibilities of CAS, 352–353
Restricted Access page source code, 577
Restricted Groups page (NSA template), 109
Restricted Sites zone, 267
restricting access on web servers, 170–184
reversing patches and service packs, 510
RFCs (Requests for Comments), 12, 224
   FTP-related, 225
RhinoSoft Serv-U servers
   installing, 226–241
   user types, 235
RhinoSoft Voyager clients, installing, 242–245

rights, 53
   assigning to Windows NT 4 groups, 68–69
   Debug Program, 69
risk analysis, 35
   identifying potential hackers, 34
   threat reduction techniques, 35
risks
   of performing development work on web
      servers, 167–168
   to WLANs, 524
routers, packet filtering, 437

S

SACL (System Access Control List), 53
SAM (Security Accounts Manager), 55
sample applications, deleting on IIS, 204, 207
Sandbox (Java), 253
sanity checking, 450
SAs (security associations), 21
SAT (Security Access Token), 55–56
scanners, Internet Scanner, securing Windows NT 4
   Server, 78–80
screened subnets, 437
Script Kiddie, 34
secure FTP, 225
testing, 246
security policies
   creating, 44–45
   defining, 36–37
   examples, 42–44
   implementing, 47
   password-related, defining, 38–41
   topics to include, 46
security templates
   modifying for web servers, 101–116
   NSA template
      Account Policies, 102–103
      Event Log, 108
      File System page, 113–116
      Local Policies, 104, 107
      Registry page, 113
      Restricted Groups page, 109
      System Services page, 110–112
Win2k/XP, 85–86
   analyzing the server, 95–98
   configuring the server, 99
   installing, 86–89, 93
seminars for increasing user awareness, 555
separate services subnet, 440
servers (FTP), Serv-U installation, 226–241
service packs, 510. See also fixes
  applying, 517
  automatically updating, 513–516
  locating, 510
  mailing lists, 512
  reversing on Windows XP, 510
  updating Windows 2000 Server to Service Pack 3, 519–523
  unpacking, 518
Serv-U FTP servers
  anonymous accounts, creating, 232–233
  installing, 226–241
  testing, 246
  use types, 235
session cookies, 268
  banner ad companies, 269
  managing, 269
session layer (OSI reference model), 6
Shavlik Technologies, 517
shims, IPSec, 21
SID (security identifier), 55
signed applications, 256
signed JavaScript applications, 254
signing, 354
SMS (System Management Server), 523
source code
  for WSFG home page, 575
  of Basic page, 577
  of Normal page, 576
  of Restricted Access page, 577
  of SSL-Test page, 578
source-routing, disabling on Cisco routers, 12
specifying IEAK setup parameters, 293
Spyware, 528
SRPs (Security Rollup Patches), 516
SSAP (Source Service Access Point) field, 802.2
LLC sublayer, 10
SSID, 524
SSL (Secure Sockets Layer), 26–27
  certificates, 352–354
  securing FTP transactions, 224
SSL-Test page source code, 578
standard access lists, 446–447
standard ACLs, 442
standards, FTP-related RFCs, 224–225
stateful inspection, CBAC, 457–460
activating, 461–462
automatic configuration, 462–482
static NAT, 31
steganography, 347
Sun Microsystems, OAK programming language, 252–253
suppressing file extensions, 116, 119
symmetric key encryption, 348
Syn Flood attacks, thwarting, 483–484
System Services page (NSA template), 110–112
TCP header, 16–18
  fields, 14
  flags, 16–18
  port numbers, 16
TCP Intercept, thwarting Syn Flood attacks, 483–484
TCP protocols, FTP, 215
TCP Small Services, 16
TCP/IP model, 7. See also OSI reference model
telephone security, emphasizing importance to staff, 554–555
Telnet, 23–25
templates
  modifying for web servers, 101–116
  NSA template
    Account Policies, 102–103
    Event Log, 108
    File System page, 113–116
    Local Policies, 104–107
    Registry page, 113
    Restricted Groups page, 109
    System Services page, 110–112
    Windows 2K/XP), 85–86
  analyzing the server, 95–98
  configuring the server, 99
  installing, 86–93
terminating PORT mode FTP sessions, port 20, 221
  testing
    customized error messages, 566
    for hotfixes, 516
    secure FTP servers, 246
    web server user accounts, 175
Thawte certificate validation, 360
third-party applications, 251
threat reduction techniques, 35
thwarting Syn Flood attacks, 483–484
TLS (Transport Layer Security), 27
transactions (FTP), securing, 224
transport layer (OSI reference model), 6, 14
ICMP header, 20–21
TCP header, 14
flags, 16–18
port numbers, 16
UDP header, 18–19
transport layer (TCP/IP model), 7
transport mode (IPSec), 21
trees (AD), 84–85
Trojan horses, 528–529
trusted networks, 438
trusting CAs, 416, 419–420
tunnel mode (IPSec), 21
two-factor identification, 421
type codes (ICMP), 20–21
Type I class of service, 11
Type II class of service, 11

U

UAS (User Agent String), extending on IE6, 314
UDP header
fields, 18
port numbers, 19
unauthorized manipulation
of URLs, 527
of web forms, 526
UNIX
ls command, 220
pwd command, 219
unpacking service packs, 518
untrusted certificates, trusting, 416–420
updating
Windows 2000 Server to Service Pack 3, 519–523
upgrading to IE6, 332
upper-layer protocols
DHCP, 28
DNS, 28
HTTP, 25
NAT, 30–31
SSL, 26–27
Telnet, 23–25
URLs, unauthorized manipulation, 527
USA Patriot Act, 509

user accounts
anonymous, creating for Serv-U FTP servers, 232–233
for web servers
managing permissions, 197–198
testing, 175
IIS5, managing permissions, 199
IUSR_machine-name, removing permissions, 179
Operators (IIS), assigning, 208, 210
restricting access to web servers, 174, 178
Windows NT 4
group rights, configuring, 68–69
policies, configuring, 66–68
renaming, 69–70
user awareness techniques, 555

V

VBScript, protecting against dangerous content, 255
viruses, 528
AVPs, 527–529
OptOut, 529
Klez, 509
Voyager FTP clients
installing, 242–245
testing, 246
vulnerabilities of passwords, 553

W

war dialing, 555
weak passwords, characteristics of, 39
web browsers, CA compatibility, 378
web forms, unauthorized manipulation of hidden fields, 526
web servers
assigning Operators, 208–210
certificates, installing, 394
CGI script timeouts, configuring, 207
document root, locating, 168
High protection, enabling, 201
IIS4
certificates, installing, 395–405
deleting sample applications, 204, 207
requesting CAs, 369–378
IIS5
application protection, 200
web servers

certificates, installing, 407, 411, 414
issuing CAs, 392
managing Execute permissions, 199
moving the Metabase, 187, 192, 196
requesting CAs, 379, 382–391
limiting access, 170–172
based on IP address, 180, 184
basic authentication, 172–178
secure authentication, 178–179
logging, 169
multiple site hosting, 212–213
performing development tasks, risks of, 167–168
removing unnecessary application mappings, 202
security templates, 113
applying, 101–113, 116
user accounts, managing permissions, 197–198
versus development servers, 167
web sites
Shavlik Technologies, 517
Windows critical updates, 510
well-known ports, 16
WEP (wireless encryption privacy), 524
WildCard Certificates, 353
Window NT 4
enabling auditing, 70–74
removing unnecessary services, 76
Windows 2000 Server
AD, 54
DAC, 53
IIS5, installing, 135, 138, 146
NTFS, 53
Windows 2000/XP
Internet Connection Sharing, 535
security templates, 85–86
analyzing the server, 95–98
configuring the server, 99
zone detection, configuring, 257–267