A
Acceptable Use Policy, 46
access control, 42–43
access policies, 42–43
components of, 42
defined, 42, 56
role-based, 171
access control lists (ACLs)
Cisco firewalls, 91
functions of, 45, 85
and packet filters, 84–85
access layer, Cisco network model, 27–28
access points
rogue access points, 162–164
WarDriving, 155–160
acknowledgment number, TCP header, 33
active/active HA firewall cluster, 103–104
active/passive HA firewall cluster, 103
Adaptive Security Appliance (ASA), 92
address object, defined, 97
Address Resolution Protocol (ARP)
ARP poisoning, 204–205
ARP spoofing, 156
WEP key, cracking, 165
address spoofing, OSI data-link layer, 24
Advanced Encryption Standard (AES), 108–110, 152, 161
Aggregator, Border Gateway Protocol attribute, 38
Aircrack, 152, 155
AirDefense, 162
AirMagnet, 162, 191–192
Aironet chipsets, 154
Airport/Airport Extreme cards, 156
AirSnort, 152
alternative minimum tax (ATM), 14
anomaly detection, and intrusion detection/prevention, 138
anti-replay, 124
anti-x protocols, 89, 92
AppDetectivePro, 196–197
Apple OS X
WarDriving tools, 156
wireless cards/chipsets, 153–154
appliances, firewalls, 95–96
application layer
OSI model, 25
TCP/IP model, 25
threats to, 25
Application Layer Gateway (ALG), and firewalls, 87
application proxy, 88–89
application scanning, 195
area border routers (ABR), 35, 36
area-id, 36
Aruba, IDS capability, 162
AS_PATH, Border Gateway Protocol attribute, 38, 39
ASP IIS buffer overflow, 140
asymmetric encryption
asymmetric encryption, Public-Key Cryptography Standards (PKCS), 110–111
Atheros chipsets, 153
ATOMIC_AGGREGATE, Border Gateway Protocol attribute, 38
attacks, 140–145
ARP poisoning, 204–205
Back Orifice Trojan, 140–141
bot exploits, 141–142
buffer overflows, 142
categories of, 140–142
decomposing, materials for, 142
denial-of-service (DoS) attacks, 140, 172
event correlation, 142
exploits, 140
flooding, 172
policy violations, 140
reconnaissance, 140
TCP host sweeps, 141
and wireless. See wireless attacks
worms, 141
attributes, Border Gateway Protocol, 37
audits, 177–178
methods, 178
authentication
Authentication Header (AH), 117–119
ESP header, 115
Internet Key Exchange (IKE), 121–122
revoking, 111–112
as security objective, 170
Authentication Header (AH), 117–119
fields in, 118
tunnel mode, 111, 117
transport mode, 119
availability
as core security value, 43
defined, 43
role-based access control, 171
autonomous system boundary routers (ASBR), 35
autonomous systems (ASs), 36–37
backbone
backbone area, 36
Cisco network model, 26–27
routers, 35–36
backup, 54–55
partial and incremental, 55
backup designated router, 36
banner grabbing, 205
tools, 188–190
Bastille program, 194
BGP protocol, 34
BiDiBLAH, 200, 204
BitTorrent
as policy violation, 140
triggers, 142
block ciphers, 108
bonus, employees, 6
border firewalls, 46
Border Gateway Protocol (BGP), 34, 36–39
attributes, 37–38
compared to Open Shortest Path
First, 37
components of, 36–37
prefixes, 37
routing filters, 39
UPDATE message, 37
bot exploits 141–142
bridges
Bridge Identification (BID), 29–30
Spanning Tree Protocol (STP), 29–30
broadcast domain, compared to
collision domain, 30
Broadcom chipsets, 153
brute force, 140
buffer overflows
elements of, 142
as exploit, 140
OSI application layer, 25
protection against, 142
bump-in-the-wire (BITW), 130

C
Cain & Able, 195
California
Anti-Phishing Act of 2005 (SB 355), 73
Assembly Bill (AB 1950), 73
Security Breach Information Act
(SB 1386), 72
Canvas, 201
Carrier Sense Multiple
Access/Collision Detection
(CSMA/CD), 30
Center for Internet Security (CIS)
benchmark tools, 193
and best practices, 125
Central Intelligence Agency (CIA)
Director of Central Intelligence
Directives (DCID) 6/3, 69–71
role in security, 81
certificates
Certificate Authority (CA), 110–111
certificate revocation list (CRL), 111–112
digital certificates, 111
Online Certificate Status Protocol
(OSCP), 112
Check Point Software
Technologies, firewalls, 93–94, 96, 99
checksum
TCP header, 33
UDP header, 33
child care, 4–5
chopping attacks, 152, 160–161
Cisco firewalls, 91–92
Adaptive Security Appliance
(ASA), 92
hardware-specific appliances, 95
limitations of, 92
PIX firewalls, 91
stand-alone management
products, 98
Cisco intrusion prevention
Intrusion Prevention System
Solution, 143
Security Agent, 144
Cisco network model, 22, 26–28
benefits to engineers, 26
layers, 26–28
switches, 27–28
Cisco wireless technology
IDS capability, 162
Lightweight Extensible
Authentication Protocol, 152
WiFi Protected Access (WPA), 152
classful routing, compared to
classless routing, 34
classification, data, 49–50
classless Inter-Domain Routing
(CIDR), 132
versus classful routing, 34
routing protocols, types of, 34
client broadcasting
rogue clients, 163
WarDriving, 155–160
client-to-site VPN, 129–130
Clinton, Bill, 73, 185
collision domain, compared to
collision domain, 30
command-line interface (CLI), and
stand-alone firewall
management, 97–98
commercial information security,
regulations, legislation,
guidance, 72
Common Vulnerabilities and
Exposures (Mitre Web
page), 179
communication, IT security
professional, 51–52
Communities, Border Gateway
Protocol attribute 38
confidential classification, 50
confidentiality, defined, 56
confidentiality, integrity,
availability (CIA)
as core security value, 43
declared, 170
as security objective, 170–171
confidentiality mode algorithms,
ESP header, 116
confidentiality-only service, ESP
header, 115
Configuration Management
documents, 46–47
cookie corruption, OSI application
layer, 25
Core Impact, 200–201
core layer, Cisco network model,
26–27
cost-of-living salary adjustment, 14
CoWPAtty, 152
Crypto kit, 111
Cygwin, 203
data, TCP header, 33
data classification, 49–50
importance of, 57
and security, 49–50
Federal Information Processing Standards (FIPS)

Data Encryption Standard (DES), 109
data labeling
defined, 57
and security, 50
data offset, TCP header, 33
Data Protection Act 1998, 168
data-link layer
OSI model, 24
threats to, 24
deep inspection, 136–137
Deep Packet Inspection, 89
Defense Intelligence Agency (DIA), Director of Central Intelligence Directives (DCID) 6/3, 69–71
Defense Technical Information Center (DTIC), Web site, 71
defense-in-depth security
aspects of, 44–45
defined, 22
and OSI model, 28
denial-of-service (DoS) attacks
OSI session layer, 25
OSI transport layer, 25
process of, 172
types of, 140
Deny All/Allow by Exception, 43, 55
Department of Defense (DoD)
DoD 8100.1 directive, 169
DoD 8500.1 directive, 71, 169
DoD 8500.2 directive, 71
Information Assurance Certification and Accreditation Process, 169
destination port
TCP header, 32
UDP header, 33
DICE, 9
dictionary attacks, 152, 161
Diffie-Hellman key agreement protocol
predefined
groups/generators/keys, 122
Public-Key Cryptography Standards, 111
digital signatures, Internet Key Exchange (IKE), 122
Director of Central Intelligence Directives (DCID) 6/3, 69–71
DISA IAVA system, 185
disassociation, 156, 162
discretionary attributes, Border Gateway Protocol, 37–38
distance-vector routing protocols (DVRPs), 35
distributed firewall management, 97, 98
distribution layer, Cisco network model, 27
DITSCAP process, 184
DMZ (demilitarized zone), 101–102
classic design, 101–102
limitations of, 102
single-firewall DMZ, 102
Do Not Fragment (DF), 128, 132
documentation
creating, participants in, 53
enforcing adherence to documents, 54
types of documents, 53
DriverLoader, 153
due care, 60
due diligence, 60, 81
E
EDE (encrypt, decrypt, encrypt), 109
eDonkey, 140
education, Family Education Rights and Privacy Act, 76–77, 168
EEE (encrypt, encrypt, encrypt), 109
eEye Retina Network Security Scanner, 193
egress interface, 99–100
Elliptic Curve Cryptography, 111
e-mail
POP3, 204
worms/Trojan horses, 141
employee benefits, types of, 3–8
Encapsulating Security Payload (ESP)
header, fields in, 114–115
transport mode, 117
tunnel mode, 116, 132
encryption
asymmetric encryption, 110–112
block and stream ciphers, 108
Internet Key Exchange (IKE), 121
symmetric key encryption, 108–110
Enhanced Interior Gateway Routing Protocol (EIGRP), 34
enumeration tools, 188–190
environmental analysis, 172–173
error logs, 142
ethereal analyzer, 142
ethical issues, 50–54
hack back, 50–51
Ettercap, 199–200
European Union Data Protection Directive (EUDPD), 168
European Union Data Retention laws, 168
event correlation
elements of, 142
protection against, 142
exploits, types of, 140
exposure analysis, 172–173
Extended Communities, Border Gateway Protocol attribute 38
Extensible Authentication Protocol (EAP)
types of, 162
wireless support, 161, 162, 165
external gateway protocol (EGP), 38
F
false positives/false negatives, intrusion detection systems (IDSs), 139
Family Education Rights and Privacy Act (FERPA), 76–77, 168
Federal Information Processing Standards (FIPS), 63–65, 169
minimum-security requirements for federal information/information systems (FIPS200), 64–65
for security categorization of federal information/information systems (FIPS199), 63–64
Federal Information Security Management Act (FISMA) of 2002

Federal Information Security Management Act (FISMA) of 2002, 63, 81, 184

Federal Information Technology Security Assessment Framework (FITSAF), 175

Federal regulations
national security systems, 69–71
non-national security, 63–68
See also regulations, legislation, guidance

File Transfer Protocol (FTP), and firewalls, 87
FIN packet, 87
financial services industry, Gramm-Leach-Bliley Act (GLBA), 74–75, 169

Financial Services Modernization Act. See Gramm-Leach-Bliley Act (GLBA)

fingerprints
hash functions, use of, 112
reconnaissance threat, 140

firewalls, 83–104
appliances, 95–96
application proxy, 88–89
border firewalls, 46
Check Point, 93–94, 96, 99
Cisco, 91–92, 95, 98
configuration components, 97
deployment, basic, 99–101
distributed management, 97, 98
DMZ (demilitarized zone), 101–102
Firewall-1, 93
Fortinet, 94
global management, 97, 98–99
high availability types, 103–104
ingress and egress interfaces, 99–100
intrusion prevention systems, 90
intrusion protection systems
proximity, 144–146
Jupiter Networks, 92–93, 95, 98, 99
and layered defense strategy, 45–46
Microsoft ISA server, 88–89
NetScreen/NetScreen Security Manager (NSM), 92–93
Network Address Translation, 90
object-oriented management, 97
open-source technologies, 94
packet filters, 84–86
PIX firewalls, 91
Secure Computing, 89
secure routers, 96
security policy, 97
server-based, 96
SnortSam, 145
SonicWALL, 94, 98
stand-alone management, 96–98
stateful firewalls, 85–88
Unified Threat Management, 89–90
Virtual Private Network (VPN), 90
WatchGuard, 94

and Web filtering, 89
flags, TCP header, 33
flapping, route flapping, 37
flexible scheduling, 4
flooding, 172
For Official Use Only (FOUO)
traffic, 127
forensics, hash functions, use of, 112
Fortinet, firewalls, 94
four-way handshake, 87
frames
 corrupt, runts, 30
OSI data-link layer, 24
FreeBSD, 93
frequency interception (WarDriving), OSI physical layer, 24
full backup, 54

Gauntlet firewall, 89
Generic Router Encapsulation, Virtual Private Network, creating, 90
global firewall management, 97–99
Global Pro, 93
Google, BiDIBLAH, 200, 204
Gramm-Leach-Bliley Act (GLBA), 74–75, 169
graphical user interface (GUI), distributed firewall management, 98
guidance, defined, 60, 81
See also regulations, legislation, guidance

Guide for Mapping Types of Information and Information Systems to Security Categories (NIST SP 800-60), 68

H
hack back, 50–51
handshake
four-way, 87
three-way, 31–32
hash functions, Virtual Private Network, 112
headers
TCP headers, 32–33
UDP headers, 32–33
headhunters, 9
health care
health care, Health Insurance Portability and Accountability Act, 73–74, 168–169
health insurance, plans, types of, 5–6
Health Insurance Portability and Accountability Act (HIPAA), 73–74, 168–169
Hello packets, 36
Hermes chipset, 153
Hermes wireless drivers, 154
high availability (HA) firewall clusters, 103–104
active/active cluster, 103–104
active/passive cluster, 103
HMO (Health Maintenance Organization), 5–6
Homeland Security Presidential Directive (HSPD), 73, 185
host(s)
host disabling, 140
host evaluations, 193
host IDS, 136
host scans and sweeps, 140–141
HostAP drivers, 155
secure configuration, and layered defense strategy, 46
Hotbar, 140
Hotjobs, 9
housing, and relocating, 16
HTML code inspection threat, OSI presentation layer, 25

ICAT project, 179–180
ICSA Labs, 113
identification as core security value, 43 defined, 43
impact, components of, 48
inbound packet processing, ESP header, 116
Incident Response Procedures, 46
incremental backups, 55
indicators, threat assessment, 177
Information Assessment Methodology (IAM), 174–175
Information Assurance and Training Program (IATRP), 182
information security, 41–57
assessing/managing. See risk management; risk assessment; security posture
backups, 54–55
daily tasks, 54–55
historical view, 167–169
layered defense, 45–47
objectives of, 170–172
patches, 54
perimeter security, 55
professionals. See IT security professionals
tools for. See tools virus protection, 55
Information Systems Security Assessment Framework (ISSAF), 175
Information Systems Security Association (ISSA), 168
information types
data classification, 49
data labeling, 50
INFOSEC Evaluation Methodology (IEM), 174–175, 182, 187–188
INFOSEC Posture Rating (IPR), 182, 185
ingress interface, 99–100
inline mode, 137
inline sensors, 137
Instant Messenger (IM), bot exploits, 141–142
Institute of Electrical and Electronics Engineers (IEEE), wireless standards (802.11 a/b/g/i/n), 150–151, 166
integrity as core security value, 43 defined, 43, 56, 171
as security objective, 170–171
integrity protection, Internet Key Exchange (IKE), 121
Intel chipsets, 154
intelligence systems. See national security systems
Interior Gateway Routing Protocol (IGRP), 34
internal gateway protocol (IGP), 38
International Information Systems Security Certification Consortium (ISC2), 168
International Standards Organization (ISO)
Code of Practice for Information Security Management (ISO 17799) (ISO 27001), 77–78
and OSI model, 23, 25
risk assessment approach, 175
Internet, job search tools, 9
Internet Control Message Protocol (ICMP)
and firewalls, 87
and packet filtering, 85
Internet Key Exchange (IKE), 119–124
aggressive mode, 122
functions of, 119
IKEv1 and IKEv2 compared, 120–121
lifetime of key, 124
main mode, 121–22
Phase II, 123
quick mode, 123
Security Associations, 119–124
Internet layer, TCP/IP model, 25
Internet Protocol V6 (IPv6), 131–132
Internet Relay Chat (IRC)
blocking by default, 204
bot exploits 141–142
Internet Security and Acceleration Server (ISA), 88–89
Internetwork Operating System (IOS), 91
Internetwork Protocol (IP), 24
interviews. See job interview; technical interview
intrusion detection and prevention, 135–146
See also intrusion detection systems (IDS); intrusion prevention systems (IPS)
intrusion detection systems (IDS), 135–146
compared to intrusion prevention systems, 136
challenges implementing, 139–140
deeep inspection, 136–137
detection methods, 138
false positives/false negatives, 139
functions of, 135–136
host IDS, 136
and layered defense strategy, 46
limitations of, 139
network IDS, 136
operation and OSI layers, 137–138
operation and TCP/IP layers, 137–138
vendors/product lines, 143–144
wireless-specific, 162
intrusion prevention systems (IPS)
compared to intrusion detection systems, 136
compared to UTM, 90
deep inspection, 136–137
deployment, location for, 144–146
inline and passive sensor modes, 137
and layered defense strategy, 46
McAfee IntruShield, 137
prevention methods, 136–137
intrusion prevention systems (IPS) (continued)

personal traits for, 2
reacting to incidents, 51
schools/programs in, 2
training, security awareness, 52–53
ITU-T.X.509 certificate, 111

job interviews, 10–15
attire for, 12
basic etiquette, 13
difficult questions, examples of, 10, 18–19
on-site, 12–13
phone interviews, 10–11
preparation for, 11–12
salary discussion, 12–15
technical questions. See technical interview

job search, 7–18
accepting/rejecting offer, 16–17
employee attributes, positive headhunters, 9
interviews. See job interviews; technical interview
networking, 8–9
online tools, 9
post-offer letter contingencies, 17
recruiters from company, 8–9
relocating, 16
résumé, 7–8
thank-you follow up, 13

John the Ripper, 195

Jupiter Networks
firewalls, 92–93
global firewall management, 99
hardware-specific appliances, 95
intrusion prevention systems, 143
SSL VPNs, 131
stand-alone management products, 98

K

Kazaa, 140
key bundles, Triple Data Encryption Algorithm, 109
key management, Internet Key Exchange (IKE), 119–123
keyloggers, OSI application layer, 25
KisMAC, 156, 166, 191
Kismet, 156–159, 166, 191
access points, recognizing, 157–158
client broadcasting, recognizing, 158–159

L

labeling of data, 50
layered defense strategies, 45–47

layers
Cisco network model, 26–28
networks, reasons for, 28–29
OSI model, 23–25

learning tools, 201–203
Least Privilege, 42, 43
defined, 56
legislation
defined, 60
See also regulations, legislation, guidance

length field, UDP header, 33
Lightweight Extensible Authentication Protocol (LEAP), 152, 162

Linux
firewalls, 96
WarDriving tools, 156, 157
wireless cards/chipsets, 153–154
wireless drivers, 154–155, 166
LOCAL_PREF, Border Gateway Protocol attribute, 38

loops, eliminating with Spanning Tree Protocol, 29–30

M

MADWIFI driver, 153, 154
mandatory attributes, Border Gateway Protocol, 37–38
man-in-the-middle attacks
OSI session layer, 25
OSI transport layer, 25
wireless, 155, 162, 164
Maximum Transmission Unit (MTU)
data-link layer, 24
size adjustments, 128–129

IT security professionals
benefits of job, 3–6
communication skills, 51–52
daily security tasks, 54–55
documentation responsibilities, 53–54
job search, 7–18

IPW wireless drivers, 154
isolated probes, 140
ISS, intrusion detection/prevention systems, 144

IP address
and packet filtering, 85
packet forwarding by, 34
Port Address Translation, 90
IP security (IPsec), 113–131
anti-replay, 124
Authentication Header (AH), 117–119
complexity trap, eliminating, 127–128
complexity trap, impact of, 125–127
Encapsulating Security Payload, 113–117
framework (old and new), 114
hash functions, 112
Internet Key Exchange, 119–124
Internet Protocol V6 as alternative to, 131–132
key lifetime, 124
layer/stack of operation, 113
Maximum Transmission Unit (MTU) size, 128–129
Network Address Translation (NAT), 129
Perfect Forward Secrecy, 124
request for comments, 113
TLS/SSL as alternative to, 131
traffic flow security, 125
tunnel mode, 125
Virtual Private Network scenarios, 129–131
See also Virtual Private Network (VPN)

J
McAfee
- host intrusion prevention, 144
- intrusion prevention system, 137

Media Access Control
- Address (MAC)
  - multicast and HA firewall clusters, 103
  - parts of, 24
  - threats to, 25

Message Authentication Codes (MAC), Virtual Private Network, 112–113

Metasploit Framework, 200

Microsoft
- Microsoft Baseline Security Analyzer (MBSA), 194
- proxy technology, 88–89

MiniStumbler, 157

Mitre Web site, Common Vulnerabilities and Exposures, 179

modular interface cards, 91

Monster, 9

MULTI_EXIT_DISC, Border Gateway Protocol attribute, 38

Multiband Atheros Driver (MADWIFI), 153, 154

Multiple Spanning Tree Protocol (MSTP), 30

Multiprotocol Label Switching (MPLS), Virtual Private Network, creating, 90

MyDoom worm, 140

National Reconnaissance Organization (NRO), Director of Central Intelligence Directives (DCID) 6/3, 69–71

National Security Agency (NSA)
- Director of Central Intelligence Directives 6/3, 69–71
- Information Assurance and Training Program, 182
- INFOSEC Evaluation Methodology, 174–175, 182, 187–188
- INFOSEC Posture Rating, 182, 185
- risk assessment approaches, 174–175
- vulnerabilities, tracking methods, 182

National security systems, 69–71
- criteria for, 69
- defined, 69
- Department of Defense directives, 71
- Director of Central Intelligence Directives 6/3, 69–71

NDISWrapper, 153

Nessus, 192

NETBIOS attacks, OSI session layer, 25

NetScreen, 92–93

NetScreen Security Manager (NSM), 93, 99

NetStumbler, 153, 155–156, 166

network(s), 22–39
- Border Gateway Protocol (BGP), 36–39
- broadcast versus collision domain, 30
- Cisco model, 26–28
- classful versus classless routing, 34
- defense-in-depth concept, 22, 28
- fundamentals, understanding, 22
- layers, 28–29
- OSI model, 23–25
- OSPF network, diagram of, 35–36
- port numbers, 34
- port security, 30
- routed versus routing protocol, 34
- routing filters, 39
- sniffing tools, 197–99
- Spanning Tree Protocol (STP), 29–30
- TCP organization, 32–33
- TCP/IP model, 25–26
- UDP headers, 32–33
- Variable-Length Subnet Masking (VLSM), 34

Network Address Translation (NAT), 129

network IDS, 136

network layer
- Network Layer Reachability Information (NRLI), 37
- OSI model, 24
- TCP/IP model, 25
- threats to, 24

networking, and job search, 8–9

next header
- Authentication Header (AH), 118, 133
- ESP header, 115
- NEXT_HOP, Border Gateway Protocol attribute, 38
- NGSSQL Crack, 195
- NGSSquirrel, 197
- Nmap, 188–189
- non-repudiation
  - as core security value, 44
  - defined, 44
  - as security objective, 170
- North American Electric Reliability Council (NERC)
  - Critical Infrastructure Protection (CIP) standards, 76
  - role of, 76
- not-so-stubby area, 35
- N-Tier applications, 195

Object-oriented management, firewalls, 97

objects
- address object, 97
- defined, 97
- service object, 97
Office of Management and Budget (OMB)

Office of Management and Budget (OMB)
Circular A130, 68
federal automated information
resources security (Appendix
III), 68
scorecard, 182

Online Certificate Status Protocol
(OSCP), 112

Open Information Security Risk
Assessment Guide, 175

Open Information Security Risk
Management Handbook, 175
Open Shortest Path First (OSPF)
compared to Border Gateway
Protocol, 37
components of, 35–36
diagram of model, 35–36
routing protocol, 34
Open System Interconnect (OSI)
model
and defense-in-depth security, 28
intrusion detection system, 137–138
layers, 23–25
open-source technologies
and buffer overflow exploits, 142
firewalls, 94
Operationally Critical Threat,
Asset, and Vulnerability
Evaluation (OCTAVE), 175
optional attributes, Border
Gateway Protocol, 37–38
options and padding, TCP
header, 33
OraScan, 197
Organizational Identifier
(OUI), 24
Origin code, Border Gateway
Protocol attribute, 38
Orinoco Classic Gold, 153
OSI model. See Open System
Interconnect (OSI) model
OSPF protocol, 34
outbound packet processing, ESP
header, 116
overtime, comp time, 3

P
packets
OSI network layer, 24
packet filters, 84–86
packet injection, 156, 162
packet sniffer, 133
pad len, ESP header, 115
padding, ESP header, 115
paid time off (PTO), 5
Parallels, 202
partial backups, 55
passive sensors, 137
password compliance testing
tools, 194–197
patches
testing, importance of, 54
vulnerability management,
181–182
path filters, 39
payload data, ESP header, 115
payload length, Authentication
Header (AH), 118
Payment Card Industry (PCI) Data
Security Standard,
78–79, 169
PC Anywhere, 204
penetration test
elements of, 177–178
testing tools, 199–201
Perfect Forward Secrecy
(PFS), 124
perimeter security, 55
PerVLAN spanning tree
(PVST/PVST+), 30
phishing, OSI application layer, 25
physical layer, OSI model, 24
PIX firewalls, 91
policy
defined, 60
layered defense strategy, 46–47
policy-based VPN, 131
violations, types of, 140
POP3, 204
port(s)
ARP poisoning, 205
for Microsoft SQL server, 204
numbers to know, 34
Port Address Translation (PAT), 90
port scanning tools, 188–190
scans and sweeps, 140
security, defined, 30
well-defined, 25
posture. See security posture
PPO (Preferred Provider
Organization), 5–6
prefixes
Border Gateway Protocol, 37
prefix filters, 39
presentation layer, threats to, 25
Pre-Shared Key (PSK)
Internet Key Exchange (IKE),
121–122
WiFi Protected Access, 152, 161
Presidential Decision Directive
(PDD)
PDD-1, 185
PDD-63 expiration, 73, 185
President’s Management Agenda
(PMA), 182
Prism chipset, 153
Privacy Act of 1974, 171
private key format, 111
PRO Wireless cards, 154
procedures, defined, 60
property tax, 16
protocol analysis
tcpdump, 144
WireShark Network Protocol
Analyzer, 144
protocol data unit (PDU), OSI
session layer, 25
Proventia Desktop, 144
Proventia Network Intrusion
Prevention System, 144
Provider-1, 99
public classification, 50
public companies, Sarbanes-Oxley
Act of 2002, 79, 81, 169
public key encryption, Internet
Key Exchange (IKE), 122
Public-Key Cryptography
Standards (PKCS), 110–111
RSA Labs controlled PKCS, list
of, 111
Quick mode, Internet Key
Exchange (IKE), 123

R
RADIUS, WIFI Protected Access
(WPA), 161
Rapid Spanning Tree Protocol
(RSTP), 30
RC4 streaming cipher, 108
realtor.com, 16
Recommended Security Controls for Federal Information Systems (NIST SP 800-53), 66–67, 81
reconnaissance threats, types of, 140
recruiters from company, 8–9
regulations, defined, 60
regulations, legislation, guidance, 59–81
changes over time, 61
definitions, 60
Family Education Rights and Privacy Act (FERPA), 76–77
Federal Information Processing Standards (FIPS), 63–65
Federal Information Security Management Act (FISMA) of 2002, 63, 81
Gramm-Leach-Bliley Act (GLBA), 74–75
Health Insurance Portability and Accountability Act (HIPAA), 73–74
importance to employers, 60–61, 80
National Institute of Standards and Technology (NIST), 65–68
national security systems, 69–71
North American Electric Reliability Council (NERC), 76
Office of Management and Budget (OMB) Circular A130, 68
Sarbanes-Oxley (SOX) Act of 2002, 79, 81, 169
SaveNow, 140
Secretary of Commerce, standards/guidance, role in, 62
Secure Computing, firewall, 89
Secure Platform (Splat), 93
secure routers, 96
Secure Sockets Layer (SSL) protocol, 25, 131
Security Agent, Cisco product, 144
Security Associations (SA) database, 123–124
functions of, 123, 133
Internet Key Exchange (IKE), 119–124

Index

Saint tools, 192–193
salary, 13–15
cost-of-living adjustment, 14
and geographic location, 14–15
target salary, 13–14
tax implications, 14–15
Sarbanes-Oxley (SOX) Act of 2002, 79, 81, 169
SaveNow, 140
scorecard, federal approach, 63, 182
Secretary of Commerce, standards/guidance, role in, 62
Secure Computing, firewall, 89
Secure Platform (Splat), 93
secure routers, 96
Secure Sockets Layer (SSL) protocol, 25, 131
Security Agent, Cisco product, 144
Security Associations (SA) database, 123–124
functions of, 123, 133
Internet Key Exchange (IKE), 119–124

Security Associations (SA)

requirements
defined, 81
See also regulations, legislation, guidance
reserved
Authentication Header (AH), 118
TCP header, 33
résumé, 7–8
retirement packages, 6
return on investment (ROI), security program, 182–183
revoking certificates, 111–112
Rijndael, 110
RIPv2 protocol, 34
risk(s)
components of, 47–48, 57
defined, 47, 56
internal and external, 173
risk assessment, 172–180
environmental analysis, 172–173
exposure analysis, 172–173
Information Assessment Methodology, 174–175
INFOSEC Evaluation Methodology, 174–175
penetration test, 177–178
risk identification approaches, 172–174
risks, defining, 173–174
self-assessment, 173, 178, 184
threat scenarios, 173
threats assessment, elements of, 176–177
vulnerabilities assessment, 176, 178–179
risk management, 47–49
vulnerabilities, addressing, 48–49
See also security posture
robots, bot exploits, 141–142
rogue access points, 162–163
becoming by attacker, 164
detecting, 164
rogue clients, 163
role-based access control, 171
root authorization attempts, as exploit, 140
routers/routing
area border routers (ABR), 36
backbone routers, 35, 36
backup designated router, 36
classful versus classless routing, 34
designated router, 36
and layered defense strategy, 45–46
route dampening, 37
route flapping, 37
route maps, 39
route-based VPN, 130
routers, defined, 96
routing filters, types of, 39
routing protocols, types of, 34
secure routers, 96
static routing, 130
Routing Information Protocol (RIP), 34
RSA Data Security, public-key cryptography, 110
rules-based, and intrusion detection/prevention, 138
runts, corrupt frames, 30

S
Saint tools, 192–193
salary, 13–15
cost-of-living adjustment, 14
and geographic location, 14–15
target salary, 13–14
tax implications, 14–15
Sarbanes-Oxley (SOX) Act of 2002, 79, 81, 169
SaveNow, 140
scorecard, federal approach, 63, 182
Secretary of Commerce, standards/guidance, role in, 62
Secure Computing, firewall, 89
Secure Platform (Splat), 93
secure routers, 96
Secure Sockets Layer (SSL) protocol, 25, 131
Security Agent, Cisco product, 144
Security Associations (SA) database, 123–124
functions of, 123, 133
Internet Key Exchange (IKE), 119–124
security core values

servers
defined, 95
secure configuration, and layered
defense strategy, 46
server-based firewalls, 96

service object, defined, 97

session layer, OSI model, 25

Sidewinder G2 firewall, 89

signatures
defined, 90
and intrusion detection/prevention, 90, 138

Simple Network Management Protocol (SNMP), 97
Net-SNMP 189–190
SNMP scanning, 189

site-to-site tunnels, 129

sniffing
OSI data-link layer, 24
packet sniffer, 133
sniffing tools, 197–199

Snoop, 198

Snort
AirSnort, 152
intrusion detection/prevention systems, 144, 145
snort rules, 145
SnortSam, 145

SNScan, 189

software downloads,
fingerprints, 112

SolarWinds, 190

SonicWALL
firewall, 94
hardware-specific appliances, 95
stand-alone management products, 98

source port
TCP header, 32
UDP header, 33

span mode, 137

Spanning Tree Protocol (STP), 29–30
operation of, 29–30
types of, 30

spoofing, 156, 162

stand-alone firewall management, 96–98

standards
International Standards Organization (ISO 17799)
(ISO 27001), 78

Payment Card Industry (PCI) data security standard, 78–79
wireless, of IEEE, 150–151, 166

state cyber security laws, 72–73, 169

stateful firewalls, 86–88
Cisco, 91
limitations of, 88
operation of, 86–87

static routing, 130

stream ciphers, 108

stub area, 35

stub area flag, 36

summarization, Border Gateway Protocol (BGP), 38

supernetting
classless versus classful routing, 34
Variable-Length Subnet Masking (VLSM), 34

SuperScan, 188

Supervisory Control and Data Acquisition (SCADA) systems, 76

Surf Control, 89

Suru, 196

switches
Cisco network model, 27–28
and collision avoidance, 30
port security, 30
Spanning Tree Protocol (STP), 29–30

symmetric key encryption
Advanced Encryption Standard (AES), 108–110
Triple Data Encryption Algorithm (TDEA), 109

SYN/ACK packet, 86–87
TCP host sweeps, 140

T

tap mode, 137

taxation
alternative minimum tax (ATM), 14
deductions, figuring, resource for, 15
property tax, 16

Tcpdump Network Protocol Analyzer, 144, 198
Virtual Private Network (VPN)

TCP/IP. See IP address; Transmission Control Protocol (TCP); Transmission Control Protocol/Internet Protocol (TCP/IP)

Tech Expo USA, 9 technical interview on firewalls, 83–104 on intrusion detection and prevention (IDP), 135–146 on legislation/policies and procedures, 59–81 on networking, 22–39 on security, 41–57 on security posture, 172–185 on tools for job, 187–205 on Virtual Private Networks (VPN), 107–133 on wireless, 149–166

unicast, ESP header, 115
Unified Threat Management (UTM) Cisco firewall, 92 intrusion prevention, 90 operation of, 89–90
UPDATE message, Border Gateway Protocol (BGP), 37 urgent pointer, TCP header, 33
User Datagram Protocol (UDP), OSI transport layer, 24–25 users, and layered defense strategy, 46–47
utilities Critical Infrastructure Protection (CIP) standards, 76 North American Electric Reliability Council (NERC), 76 Water Infrastructure Security Enhancement, 76

Variable-Length Subnet Masking (VLSM), 34
Virtual PC, 202
Virtual Private Network (VPN) asymmetric encryption, 110–112 Check Point firewall, 93 client-to-site VPN, 129–130 hash functions, 112 Message Authentication Codes, 112–113
Virtual Private Network (VPN) (continued)

Virtual Private Network (VPN) (continued)
policy-based VPN, 131
protocols for creating, 90
route-based VPN, 130
site-to-site VPN, 129
symmetric key encryption, 108–110

Virtual Private Networks (VPN), 107–133

viruses
as exploit, 140
and layered defense strategy protection, 46
OSI application layer, 25
protection updates, importance of, 55

VMWare, 202
vulnerabilities
assessment, elements of, 176
Common Vulnerabilities and Exposures (Mitre Web page), 179
components of, 48
limiting/eliminating, 48–49
management of. See security posture
penetration test, 177–178
scanning tools, 192–194

W
WarDriving, 155–160
access points, recognizing, 157–158
active versus passive WLAN detection, 156, 164, 165
AirMagnet, 162, 191–192
client broadcasting, recognizing, 158–159
data, use for attacks, 159–160
handheld devices, 157
KisMAC, 156, 191
Kismet, 156, 157, 191
MiniStumbler, 157
NetStumbler, 155–156
Zaurus, 157
WatchGuard, firewalls, 94

Water Infrastructure Security Enhancement (WISE), 76
Web filtering, 89
Web server hijacking, OSI application layer, 25
WebInspect, 196
Websense, 89
WEP/WEPA hacking, OSI data-link layer, 24
wide area network (WAN) interface and routers, 93, 96
Jupiter routers, 93
WiFi Alliance, 151
WiFi Protected Access (WPA), 161–162
development of, 152
IEEE 802.11 standards, 150–151
passphrase, length of, 161, 166
Pre-Shared Key, 152, 161
vulnerabilities, 161
WPA Personal, 161
WPA-RADIUS, 161
WPS2, 161
Wikto, 196
window, TCP header, 33

Windows
WarDriving tools, 155, 157
wireless cards/chipsets, 153–154

WinDump, 198

Wired Equivalent Privacy (WEP)
chopping attacks, 152, 160–161
deployment strengths, 160
historical view, 151–152, 160
IEEE 802.11 standards, 150–151
WEP cracking, 156

wireless, 149–166
attacks/attack prevention. See wireless attacks
cards/chipsets, 153–154
Extensible Authentication Protocol (EAP), 162
IEEE standards, 150–151, 166
Linux drivers, 154–155
security, history of, 151–152

WiFi Alliance, 151
WiFi Protected Access (WPA), 161–162, 166
Wired Equivalent Privacy (WEP), 150–152, 160–161

wireless attacks
access points, recognizing, 156, 157–158
active versus passive detection, 156, 164, 165
chopping, 152, 160–161
client broadcasting, recognizing, 158–159
dictionary attacks, 152, 161
disassociation, 162
equivalent tools, 190–192
FMS attacks, 152
intrusion detection systems, 162
MAC address cloning, 162
man-in-the-middle attacks, 155, 162, 164
packet injection, 156, 162
rogue access points, 162–164
rogue client methods, 163
rogue devices, detecting, 164
spoofing, 156, 162
WarDriving, 155–160
with WarDriving data, 159–160
WEP key, cracking, 165
WLAN detection. See WarDriving
WPA passphrase cracking, 156

WireShark Network Protocol Analyzer, 142, 144, 198
wiretaps, OSI physical layer, 24

wlan-ng drivers, 155

worms
compared to Trojan horse, 141
as exploit, 140
OSI application layer, 25

wrapper programs, 153

Z
Zaurus, 157
zero-day attacks, and intrusion detection/prevention, 139
Zillow, 16
zones, Jupiter Networks firewalls, 92–93