

Contents at a Glance

<i>Introduction</i>	xiv
Chapter 1 • A Systems Analysis Approach to Information Technology	1
Chapter 2 • Security as a Process	17
Chapter 3 • Understanding How Network Systems Communicate	31
Chapter 4 • Topology Security	83
Chapter 5 • Firewalls	111
Chapter 6 • Cisco's PIX Firewall	153
Chapter 7 • Intrusion Detection Systems	191
Chapter 8 • Authentication and Encryption	215
Chapter 9 • Virtual Private Networking	235
Chapter 10 • Viruses, Trojans, and Worms	257
Chapter 11 • Disaster Prevention and Recovery	277
Chapter 12 • The Wide World of Windows	315
Chapter 13 • Unix-Based Systems	379
Chapter 14 • The Anatomy of an Attack	415
Chapter 15 • Security Resources	439
Appendix A • Operating System Security Checklists	451
Appendix B • Sample Network Usage Policy	457
<i>Index</i>	465

Contents

<i>Introduction</i>	xiv
Chapter 1 • A Systems Analysis Approach to Information Technology	1
An Introduction to Systems Analysis	1
Define the Scope of the Problem	6
Determine Objectives, Constraints, Risks, and Cost	6
Applying Systems Analysis to Information Technology	9
The Nature of the Data	9
The Types of Technology	10
How the Organization Uses the System	10
How Individuals Use the System	10
Models and Terminology	10
Summary	16
Chapter 2 • Security as a Process	17
Survival of the Fittest: The Myth of Total Security	17
Risk Mitigation: Case Studies of Success and Failure	19
The Systems Development Life Cycle (SDLC): Security as a Process	
from Beginning to End	22
Conceptual Definition	22
Functional Requirement Determination	23
Protection Specifications Development	23
Design Review	24
Development and Acquisition	24
Component and Code Review	24
System Test Review	25
Certification	25
Implementation	26
Accreditation	27
Operation and Maintenance	27
Disposal	28
Steady As It Goes: Putting the “Constant” Back into Vigilance	28
Summary	29
Chapter 3 • Understanding How Network Systems Communicate	31
The Anatomy of a Frame of Data	31
Ethernet Frames	31
The Frame Header Section	33
A Protocol’s Job	36
The OSI Model	37
How the OSI Model Works	40
More on the Network Layer	42

Routers	42
Routing Tables	43
Static Routing	44
Distance Vector Routing	45
Link State Routing	51
Label Switching and MPLS	53
Connectionless and Connection-Oriented Communications	56
Connection-Oriented Communications	57
Connectionless Communications	59
Security Implications	60
Network Services	60
File Transfer Protocol (FTP): The Special Case	66
Other IP Services	68
Upper Layer Communications	80
Summary	81
Chapter 4 • Topology Security	83
Understanding Network Transmissions	83
Digital Communication	83
Electromagnetic Interference (EMI)	85
Fiber-Optic Cable	86
Bound and Unbound Transmissions	87
Choosing a Transmission Medium	89
Topology Security	90
LAN Topologies	90
Wide Area Network Topologies	95
Frame Relay	96
Asynchronous Transfer Mode (ATM)	98
Wireless	99
Basic Networking Hardware	99
Hubs	99
Bridges	100
Switches	102
Routers	105
A Comparison of Bridging/Switching and Routing	107
Layer-3 Switching	108
Summary	109
Chapter 5 • Firewalls	111
Defining an Access Control Policy	112
Definition of a Firewall	113
When Is a Firewall Required?	114
Dial-In Modem Pool and Client-Initiated VPN	114
External Connections to Business Partners	114
Between Departments	114
Hosts	114
Firewall Functions	114
Static Packet Filtering	115

Dynamic Packet Filtering	123
Stateful Filtering	128
Proxy Servers	129
Firewall Types	133
Which Firewall Functions Should I Use?	133
Which Type Should I Choose?	134
Server-Based Firewalls	135
Appliance-Based Firewalls	141
Additional Firewall Considerations	142
Address Translation	142
Firewall Logging and Analysis	145
Virtual Private Networks (VPNs)	147
Intrusion Detection and Response	147
Integration and Access Control	148
Third-Party Tools	148
You Decide	149
Firewall Deployment	149
Summary	152
Chapter 6 • Cisco's PIX Firewall	153
An Overview of PIX	153
Installing PIX	154
Installing PDM	156
Configuring PDM	159
Configuring PIX	161
Configuring PIX Security	165
The Access Rules Tab	166
AAA Rules	172
Filter Rules	175
Translation Rules	179
Monitoring	187
Summary	189
Chapter 7 • Intrusion Detection Systems	191
IDS Types	191
Network Intrusion Detection System	192
System Integrity Verifier	193
Log File Monitor	193
Honeypot	194
NIDS Limitations	195
Teardrop Attacks	195
Other Known NIDS Limitations	197
NIDS Countermeasures	200
Host-Based IDS	202
NIDS Fusion	204
Snort: A Popular NIDS	205
Snort Rules	206

Before You Begin	209
Configuring Snort	211
Snort Alert Example	213
Suggestions for Using Snort	213
Summary	214
Chapter 8 • Authentication and Encryption	215
The Need for Improved Security	215
Passively Monitoring Clear Text	217
Clear Text Protocols	218
Good Authentication Required	218
Session Hijacking	218
Verifying the Destination	219
Encryption 101	220
Methods of Encryption	221
Encryption Weaknesses	224
Government Intervention	227
Good Encryption Required	227
Solutions	228
Data Encryption Standard (DES)	228
Advanced Encryption Standard (AES)	228
Digital Certificate Servers	229
IP Security (IPSEC)	229
Kerberos	230
PPTP/L2TP	231
EAP (Extensible Authentication Protocol)	231
Remote Access Dial-In User Service (RADIUS)	231
RSA Encryption	232
Secure Shell (SSH)	232
Secure Sockets Layer (SSL)	232
Security Tokens	233
Simple Key Management for Internet Protocols (SKIP)	234
Summary	234
Chapter 9 • Virtual Private Networking	235
VPN Basics	235
VPN Usage	237
Selecting a VPN Product	240
VPN Product Options	242
VPN Alternatives	243
Setting Up a VPN	244
Preparing the System	244
Our VPN Diagram	244
Configuring the VPN Server	245
Configuring the VPN Client	250
Testing the VPN	253
Summary	256

Chapter 10 • Viruses, Trojans, and Worms	257
Viruses: The Statistics	257
What Is a Virus?	258
Replication	258
Concealment	261
Bomb	263
Social-Engineering Viruses	263
Worms	264
Trojan Horses	267
Preventive Measures	268
Access Control	268
Checksum Verification	268
Process Monitoring	269
Virus Scanners	270
Heuristic Scanners	271
Application-Level Virus Scanners	272
Deploying Virus Protection	272
Protecting the Desktop Systems	273
Protecting the Server Operating Systems	274
Protecting the Unix-Based System	275
Summary	276
Chapter 11 • Disaster Prevention and Recovery	277
Disaster Categories	278
Network Disasters	278
Media	278
Topology	280
LAN Topology	280
WAN Topologies	284
Single Points of Failure	286
Saving Configuration Files	288
Server Disasters	290
Uninterruptible Power Supply (UPS)	290
RAID	291
Redundant Servers	293
Clustering	294
Data Backup	295
Application Service Providers	298
Server Recovery	298
Extreme Disasters	299
Nondestructive Testing	301
Document Your Procedures	301
VERITAS Storage Replicator	301
VSR Planning	302
Installing VSR	303
Configuring VSR	304
Configuring Replication	308
Summary	313

Chapter 12 • The Wide World of Windows	315
NT Overview	315
Active Directory	317
The Domain Structure	320
Storing Domain Information	320
Domain Trusts	321
User Accounts	321
Working with SIDs	321
The Security Account Manager in Windows NT	322
Configuring Group Policies for Windows 2000	323
Other Registry-Based Extensions	328
Configuring User Manager Policies for Windows NT	331
Policies and Profiles	335
The File System	339
Share Permissions	340
File Security	341
Logging	344
Configuring Event Viewer	344
Reviewing the Event Viewer Logs	345
Auditing System Events	346
Security Patches	347
Available IP Services	348
Computer Browser	349
DHCP Relay Agent	349
Microsoft DHCP Server	349
Microsoft DNS Server	349
Microsoft Internet Information Server (IIS)	350
Microsoft TCP/IP Printing	350
Network Monitor Agent and Tools	351
RIP	351
RPC Configuration	351
Simple TCP/IP Services	352
SNMP Service	352
Windows Internet Naming Service (WINS)	352
Packet Filtering with Windows NT	353
Enabling Packet Filtering	353
Configuring Packet Filtering	354
A Final Word on Ports	356
Securing DCOM	356
Selecting the DCOM Transport	357
Limiting the Ports Used by DCOM	358
DCOM and NAT	359
Ports Used by Windows Services	360
Additional Registry Key Changes	361
Producing a Logon Banner	361
Hiding the Last Logon Name	362
Securing the Registry on Windows NT Workstation	362
Securing Access to Event Viewer	363
Cleaning the Page File	363

Windows 2000	364
File System Permissions	364
Encrypting File System	364
Kerberos Version 5	366
Public Key Certificate Services	370
IPsec	372
Smart Cards	373
Windows .NET	374
The .NET Security Policy	375
Policy Tools	376
Policy Recommendations	376
Summary	377
Chapter 13 • Unix-Based Systems	379
Unix History	379
FreeBSD	380
Linux	381
The Unix File System	382
Understanding UID and GID	382
File Permissions	382
Account Administration	386
The Password File	386
The Group File	389
PAM (Pluggable Authentication Module)	391
Limit Root Logon to the Local Console	393
Optimizing the Unix Kernel	393
Running make	394
Changing the Network Driver Settings	402
IP Service Administration	403
IP Services	403
inetd and xinetd	407
Working with Other Services	410
TCP Wrapper	411
Unix Checklist Overview	412
Preinstallation	412
System Configuration	412
Summary	414
Chapter 14 • The Anatomy of an Attack	415
Collecting Information	415
The whois Command	416
The nslookup Command	418
Search Engines	420
Probing the Network	421
The traceroute Command	421
Host and Service Scanning	423
Passive Monitoring	426
Checking for Vulnerabilities	427

Launching the Attack	429
Hidden Accounts	430
MITM (Man in the Middle)	430
Buffer Overflows	432
SYN Attack	433
Teardrop Attacks	433
Smurf	434
Brute Force Attacks	436
Physical Access Attacks	437
Summary	438
Chapter 15 • Security Resources	439
Information from the Vendor	439
3COM	440
Cisco	440
Linux	441
Microsoft	442
Novell	442
Sun Microsystems	443
Third-Party Channels	443
Vulnerability Databases	444
Websites	446
Mailing Lists	447
Newsgroups	448
Summary	449
Appendix A • Operating System Security Checklists	451
Appendix B • Sample Network Usage Policy	457
<i>Index</i>	465