

CONTENTS AT A GLANCE

	<i>Introduction</i>	xxv
Part I	Network Security Fundamentals	1
Chapter 1	A Systems Approach to Information Networks <i>Adapted from Mastering™ Network Security, Second Edition by Chris Brenton and Cameron Hunt ISBN 0-7821-4142-0</i>	3
Chapter 2	Security as a Process <i>Adapted from Mastering™ Network Security, Second Edition by Chris Brenton and Cameron Hunt ISBN 0-7821-4142-0</i>	25
Chapter 3	A Bird's-Eye View of Topology Security <i>Adapted from Mastering™ Network Security, Second Edition by Chris Brenton and Cameron Hunt ISBN 0-7821-4142-0</i>	45
Chapter 4	Authentication and Encryption <i>Adapted from Mastering™ Network Security, Second Edition by Chris Brenton and Cameron Hunt ISBN 0-7821-4142-0</i>	83
Part II	Operating Systems and Servers	111
Chapter 5	Windows 2000 Security <i>Adapted from Windows® 2000 Server: 24seven™ by Matthew Strebe ISBN 0-7821-2669-3</i>	113
Chapter 6	Living with Windows XP Professional Strict Security <i>Adapted from Mastering™ Windows® XP Professional, Second Edition by Mark Minasi ISBN 0-7821-4114-5</i>	181

Chapter 7	Securing Your NetWare 6 Network <i>Adapted from Mastering™ NetWare® 6 by James E. Gaskin</i> <i>ISBN 0-7821-4023-8</i>	207
Chapter 8	Linux System Installation and Setup <i>Adapted from Linux Security by Ramón J. Hontañón</i> <i>ISBN 0-7821-2741-X</i>	251
Chapter 9	Linux System Monitoring and Auditing <i>Adapted from Linux Security by Ramón J. Hontañón</i> <i>ISBN 0-7821-2741-X</i>	285
Chapter 10	Samba Security Considerations <i>Adapted from Linux Samba Server Administration</i> <i>by Roderick W. Smith</i> <i>ISBN: 0-7821-2740-1</i>	317
Part III	Firewalls	371
Chapter 11	Understanding Firewalls <i>Adapted from Firewalls 24seven™, Second Edition</i> <i>by Matthew Strebe and Charles Perkins</i> <i>ISBN 0-7821-4054-8</i>	373
Chapter 12	Packet Filtering <i>Adapted from Firewalls 24seven™, Second Edition</i> <i>by Matthew Strebe and Charles Perkins</i> <i>ISBN 0-7821-4054-8</i>	405
Chapter 13	Network Address Translation <i>Adapted from Firewalls 24seven™, Second Edition</i> <i>by Matthew Strebe and Charles Perkins</i> <i>ISBN 0-7821-4054-8</i>	421
Chapter 14	Windows Firewalls <i>Adapted from Firewalls 24seven™, Second Edition</i> <i>by Matthew Strebe and Charles Perkins</i> <i>ISBN 0-7821-4054-8</i>	445
Chapter 15	Unix Firewalls <i>Adapted from Firewalls 24seven™, Second Edition</i> <i>by Matthew Strebe and Charles Perkins</i> <i>ISBN 0-7821-4054-8</i>	471

Chapter 16	Linux Network-Layer Firewalls <i>Adapted from Linux Security by Ramón J. Hontañón</i> <i>ISBN 0-7821-2741-X</i>	497
Part IV	Cisco Security Specialist (CSS1) Highlights	531
Chapter 17	PIX Firewall Basics <i>Adapted from CSS1™/CCIP™: Cisco® Security Specialist Study Guide by Todd Lammler, Tom Lancaster, Eric Quinn, and Justin Menga</i> <i>ISBN 0-7821-4049-1</i>	533
Chapter 18	PIX Firewall Configuration <i>Adapted from CSS1™/CCIP™: Cisco® Security Specialist Study Guide by Todd Lammler, Tom Lancaster, Eric Quinn, and Justin Menga</i> <i>ISBN 0-7821-4049-1</i>	565
Chapter 19	Introduction to Virtual Private Networks <i>Adapted from CSS1™/CCIP™: Cisco® Security Specialist Study Guide by Todd Lammler, Tom Lancaster, Eric Quinn, and Justin Menga</i> <i>ISBN 0-7821-4049-1</i>	613
Chapter 20	Introduction to Cisco VPN Devices <i>Adapted from CSS1™/CCIP™: Cisco® Security Specialist Study Guide by Todd Lammler, Tom Lancaster, Eric Quinn, and Justin Menga</i> <i>ISBN 0-7821-4049-1</i>	643
Chapter 21	Installing Cisco Secure IDS Sensors and IDSMs <i>Adapted from CSS1™/CCIP™: Cisco® Security Specialist Study Guide by Todd Lammler, Tom Lancaster, Eric Quinn, and Justin Menga</i> <i>ISBN 0-7821-4049-1</i>	663
Chapter 22	Sensor Configuration <i>Adapted from CSS1™/CCIP™: Cisco Security Specialist Study Guide by Todd Lammler, Tom Lancaster, Eric Quinn, and Justin Menga</i> <i>ISBN 0-7821-4049-1</i>	731
Part V	Security-Related MCSE Highlights	757
Chapter 23	Evaluating the Impact of the Security Design on the Technical Environment <i>Adapted from MCSE: Windows® 2000 Network Security Design Study Guide, Second Edition by Gary Govanus and Robert King</i> <i>ISBN: 0-7821-2952-8</i>	759

Chapter 24	Designing Security Baselines	793
	<i>Adapted from MCSE: Windows® 2000 Network Security Design Study Guide, Second Edition by Gary Govanus and Robert King ISBN: 0-7821-2952-8</i>	
Chapter 25	Designing the Security Solution	837
	<i>Adapted from MCSE: Windows® 2000 Network Security Design Study Guide, Second Edition by Gary Govanus and Robert King ISBN 0-7821-2952-8</i>	
	Glossary of Networking Terms	875
	<i>Adapted from the Network+™ Study Guide, Third Edition by David Groth ISBN 0-7821-4014-9</i>	
	<i>Index</i>	921

CONTENTS

Introduction

xxv

Part I ► Network Security Fundamentals 1

Chapter 1 □ A Systems Approach to Information Networks 3

An Introduction to Systems Analysis	4
Define the Scope of the Problem	10
Determine Objectives, Constraints, Risks, and Cost	11
Applying Systems Analysis to Information Technology	15
The Nature of the Data	16
The Types of Technology	16
How the Organization Uses the System	16
How Individuals Use the System	16
Models and Terminology	17
What's Next	24

Chapter 2 □ Security as a Process 25

Survival of the Fittest: The Myth of Total Security	26
Risk Mitigation: Case Studies of Success and Failure	29
The Systems Development Life Cycle (SDLC): Security as a	
Process from Beginning to End	33
Initiation	33
Development and Acquisition	36
Implementation	38
Operation and Maintenance	41
Disposal	41
Steady As It Goes: Putting the "Constant" Back into Vigilance	42
What's Next	43

Chapter 3 □ A Bird's-Eye View of Topology Security 45

Understanding Network Transmissions	46
Digital Communication	46
Electromagnetic Interference (EMI)	48

Remote Access Dial-In User Service (RADIUS)	106
RSA Encryption	107
Secure Shell (SSH)	107
Secure Sockets Layer (SSL)	108
Security Tokens	108
Simple Key Management for Internet Protocols (SKIP)	110
What's Next	110

Part II ► Operating Systems and Servers 111

Chapter 5 □ Windows 2000 Security 113

Security Theory	115
A Cryptographic Primer	117
Encryption Algorithms	119
Generating Keys	126
Uses of Encryption	127
Windows 2000 Local Security	133
Security Identifiers	134
Resource Access	135
NTFS File System Permissions	140
Encrypting File System	142
Windows 2000 Network Security	145
Active Directory	146
Kerberos Authentication and Domain Security	146
Group Policies	152
Share Security	160
Network Layer Encryption	164
Summary	178
What's Next	179

Chapter 6 □ Living with Windows XP Professional Strict Security 181

Understanding User Accounts in Windows XP Professional	182
Understanding User Rights	185
Creating a User Account	187
Creating a Group Account	190
Setting Permissions	192
Setting Share-Level Permissions	192
Types of File and Folder Permissions	194

User Account Security	261
Good Passwords	264
Shadow Passwords	266
The <i>sudo</i> Utility	267
File and Directory Permissions	271
<i>suid</i> and <i>sgid</i>	271
The <i>umask</i> Setting	275
Limiting Core Dump Size	275
<i>syslog</i> Security	276
Filesystem Encryption	277
The Cryptographic File System	277
Practical Privacy Disk Driver	280
What's Next	283

Chapter 9 □ **Linux System Monitoring and Auditing** **285**

System Logging with <i>syslog</i>	286
<i>syslog.conf</i> File	287
<i>syslog</i> Server Security	290
System Log Monitoring	291
<i>swatch</i>	291
<i>logcheck</i>	296
<i>swatch</i> versus <i>logcheck</i>	301
File Integrity Auditing	302
<i>tripwire</i>	302
Password Auditing	311
John the Ripper	311
What's Next	315

Chapter 10 □ **Samba Security Considerations** **317**

Controlling Initial Access to Samba	318
Binding Samba to Specific Network Interfaces	318
Restricting Access by Computer	319
Authenticating Users by Username and Password	322
Encrypted versus Cleartext Passwords	329
Advantages and Drawbacks of Encrypted and Cleartext Passwords	329
Default Encryption for Versions of Windows	332
Using Samba's Encryption Policy	333
Samba's Password Support Programs	336
Setting the Windows Encryption Policy	340

File Ownership and Permissions	341
Evaluating Per-Share Ownership and Permissions	341
Evaluating Per-User Access Controls	343
Integrating ACLs with Samba	344
Samba over SSL	349
Configuring SSL	350
Creating Certificates	353
Configuring Samba to Use SSL	356
Configuring a Client to Use SSL	360
Samba in the Broader Security World	363
Ports Used by SMB/CIFS	364
Using <i>ipchains</i> or a Firewall to Block Samba Access	364
Running Samba through TCP Wrappers or <i>xinetd</i>	367
Non-Samba Servers	368
What's Next	369

Part III ► Firewalls **371**

Chapter 11 □ Understanding Firewalls **373**

Firewall Elements	374
Packet Filters	376
Network Address Translation	382
Proxies	383
Virtual Private Networks	386
Encrypted Authentication	387
Creating Effective Border Security	388
Comparing Firewall Functionality	390
Problems Firewalls Can't Solve	392
Border Security Options	394
What's Next	404

Chapter 12 □ Packet Filtering **405**

How Stateless Packet Filters Work	406
Protocol Filtering	406
IP Address Filtering	407
TCP/UDP Ports	408
Filtering on Other Information	410
Problems with Stateless Packet Filters	411
OS Packet Filtering	412

How Stateful Inspection Packet Filters Work	413
Hacking through Packet Filters	416
TCP Can Be Filtered Only in 0th Fragments	416
Low Pass Blocking Filters Don't Catch High Port Connections	417
Public Services Must Be Forwarded	417
Internal NATs Can Defeat Filtering	417
Best Packet Filtering Practices	418
Use a Real Firewall	418
Disable All Ports By Default	418
Secure the Base OS	418
What's Next	420

Chapter 13 □ **Network Address Translation** **421**

NAT Explained	422
Translation Modes	425
Router Configuration for NAT	431
Problems with NAT	434
Hacking through NAT	437
Static Translation = No Security	437
Internal Host Seduction	438
The State Table Timeout Problem	438
Source Routing through NAT	439
What's Next	443

Chapter 14 □ **Windows Firewalls** **445**

Checkpoint Firewall-1	447
Major Feature Set	448
Minor Feature Set	449
Interface	451
Security	453
Documentation	453
Cost and Support	454
Symantec Enterprise Firewall	455
Major Feature Set	455
Minor Feature Set	457
Security	458
Interface	459
Documentation	459
Cost and Support	460

Chapter 16 □ Linux Network-Layer Firewalls	497
Linux as a Firewall Platform	498
Packet Filtering	500
The Legacy: <i>ipfwadm</i> and <i>ipchains</i>	501
Using <i>ipchains</i>	501
<i>ipchains</i> Examples	504
The Present: Netfilter	506
Configuring Netfilter	506
<i>iptables</i>	508
Sample Firewall Scenarios	515
Single-Homed Dial-up Server	515
Dual-Homed Firewall: Public and Private Addresses	517
Trihomed Firewall with a Demilitarized Zone	520
Protecting against Well-Known Attacks	523
Network Address Translation	526
Configuring NAT Using <i>iptables</i>	527
What's Next	529
Part IV ► Cisco Security Specialist (CSS1) Highlights	531
Chapter 17 □ PIX Firewall Basics	533
Reviewing Firewall Technologies	534
Dual-Homed Gateways	534
Packet-Filtering Firewalls	535
Stateful Firewalls	537
Firewall Technology Combinations	538
Introducing the Cisco IOS Firewall Feature Set	540
Introducing the Secure PIX Firewall	541
PIX Firewall Features	542
PIX Firewall Components	543
PIX Firewall Operation	549
NAT Mechanisms	549
Packet Processing	550
The Adaptive Security Algorithm (ASA) and Security Levels	554
Using the PIX Command-Line Interface	556
CLI Access Methods	556
CLI Modes	557

RSA Encrypted Nonces	631
Certificate Authorities (CAs)	632
How IPSec Works	633
Defining Interesting Traffic	633
IKE Phase 1	634
IKE Phase 2	636
IPSec Task Flow	638
IPSec Troubleshooting	639
Traffic Delay Problems	639
Filtering Problems	640
NAT Problems	640
ACL Problems	640
What's Next	641

Chapter 20 □ Introduction to Cisco VPN Devices 643

Introducing the VPN 3000 Concentrators	644
VPN 3005 Concentrator	644
VPN 3015 through 3080 Concentrators	646
VPN Concentrator Client Support	648
Introducing the VPN Hardware Client	649
Configuring the Hardware Client with the Quick Configuration Utility	650
Managing the Hardware Client	655
Introducing the VPN Software Clients	656
Configuring the Unified Client	656
Configuring the SafeNet Client	660
What's Next	662

Chapter 21 □ Installing Cisco Secure IDS Sensors and IDSMs 663

Deploying Sensors	664
General Sensor Placement Considerations	664
Common Sensor Locations	665
Sensor Interfaces	666
Cisco Secure IDS 4200 Series Sensor Deployment	667
Cisco Catalyst IDSM Sensor Deployment	673
Installing and Configuring Cisco Secure IDS 4200 Series Sensors	675
Physically Installing the Sensor	675
Gaining Management Access	679

Domain Model	760
Trust Management	763
Security Policy Components	768
Security Identifiers	768
Security Configuration and Analysis	769
Data Encryption	769
Authentication	770
Single Sign-On	771
Two-Factor Authentication	772
Digital Signatures and Data Confidentiality	772
Nonrepudiation	773
Audit Logs	773
Physical Security	774
User Education	774
The Effect of Security Design on Existing Systems and Applications	776
Upgrading Client Systems	776
Client and Server Interoperability Requirements	777
Application Compatibility	778
Upgrades and Restructuring	780
Why Restructure Domains?	780
When to Restructure Domains	781
The Implications of Restructuring Domains	783
Analyzing the Technical Support Structure	785
Desktop Support Management	785
Network Management	786
Data Center Management	786
Security Requirements	787
Analyzing Existing and Planned Network and Systems Management	788
Change and Configuration Management Tools	788
What's Next	792

Chapter 24 □ Designing Security Baselines 793

Distributed Security Strategies	794
Authenticating All User Access	795
Applying Access Control	808
Uniform Security Policies	817
Providing Data Protection for Sensitive Data	819

Deploying Secure Applications	827
Managing Administration	834
What's Next	836
Chapter 25 □ Designing the Security Solution	837
Audit Policies	838
Establishing an Audit Policy	838
Implementing an Audit Policy	839
Best Practices when Auditing	843
Delegating Authority and Security Groups	845
Delegating Administration	847
Implementing Group Policy Security Settings	851
Account Policies	853
Local Computer Policies	854
Event Log Policies	855
Restricted Group Policies	855
System Services Policies	856
Registry Policies	857
Filesystem Policies	857
Public Key Policies	858
IP Security Policies on Active Directory	858
The Placement and Inheritance of Security Policies	859
Group Policy Hierarchy	859
Designing an Encrypting File System Strategy	860
Things to Know about EFS	861
EFS and the End User	862
Recovering Data	864
Best Practices When Using EFS	867
Tips for Using EFS	868
Designing Your Security Plan	869
Deployment Planning Checklist	870
What's Next	872
Glossary of Networking Terms	875
<i>Index</i>	921