

CONTENTS AT A GLANCE

Part I

General Security Concepts

1	Fundamental Security Concepts	3
2	Attacks, Motives, and Methods	35
3	Security Management and Standards	65

Part II

Detection and Device Management

4	Logging and Process Accounting	95
5	Solaris Auditing, Planning, and Management	121
6	Device, System, and File Security	151

Part III

Security Attacks

7	Denial of Service Attacks	179
8	Remote Access Attacks	217

Part IV

File and System Resources Protection

9	User and Domain Account Management with RBAC	255
10	Fundamentals of Access Control	281

Part V

Solaris Cryptographic Framework

11	Using Cryptographic Services	305
----	------------------------------	-----

Part VI

Authentication Services and Secure Communication

12	Secure RPC Across NFS and PAM	333
13	SASL and Secure Shell	355
14	Sun Enterprise Authentication Mechanism	375

Part VII

Appendixes

A	Final Test Study Guide	421
B	Final Test	445
C	Final Test Answers	473
D	Hands-On Exercises and Solutions	497
	Index	515

CONTENTS

<i>About the Contributors</i>	<i>v</i>
<i>Acknowledgments</i>	<i>xvii</i>
<i>Preface</i>	<i>xix</i>
<i>Introduction</i>	<i>xxiii</i>

Part I

General Security Concepts

I Fundamental Security Concepts	3
Describe Principles of Information Security	4
Confidentiality	4
Integrity	5
Availability	5
Identification	6
Authentication	6
Authorization	8
Accountability	8
Logs	9
Functionality vs. Assurance	9
Privacy	10
Non-repudiation	10
Explain Information Security Fundamentals and Define Good Security Architectures	13
Least Privilege	13
Defense in Depth	13
Minimization	14
Cost-Benefit Analysis	14
Risk-Control Adequacy	14
Compartmentalization	15
Keep Things Simple	15

	Fail Securely	15
	Secure the Weakest Link	16
	Use Choke Points	16
	Leverage Unpredictability	16
	Segregation of Duties	16
	Types of Controls	17
	Access Control Models	18
	Information Security Architectures	20
	✓ Two-Minute Drill	26
Q&A	Self Test	27
	Self Test Answers	32
2	Attacks, Motives, and Methods	35
	Describe Concepts of Insecure Systems, User Trust, Threat, and Risk	36
	Trust	38
	Threats	39
	Vulnerabilities	39
	Risks and Risk Management	40
	Explain Attackers, Motives, and Methods	43
	Types of Attackers	44
	Attack Motives	46
	Attack Methods	46
	Describe How Attackers Gain Information, and Describe Methods to Reduce Disclosure	51
	Top 10 UNIX Vulnerabilities	54
	✓ Two-Minute Drill	56
Q&A	Self Test	58
	Self Test Answers	62
3	Security Management and Standards	65
	Identify the Security Life Cycle and Describe Best Security Practices	66
	Security Management and Operations	66
	Security Life Cycle	67
	Security Awareness	69
	Security Policies, Procedures, and Guidelines	69
	Physical Security	71

Platform Security	72
Network Security	73
Applications Security	76
Describe the Benefits of Evaluation Standards	77
The Common Criteria (ISO 15408)	77
ISO 17799	79
Certification, Evaluation, and Accreditation	81
✓ Two-Minute Drill	83
Q&A Self Test	85
Self Test Answers	89

Part II

Detection and Device Management

4 Logging and Process Accounting	95
Identify, Monitor, and Disable Logins	96
Identifying, Disabling, and Monitoring Logins	98
Configure syslog, Customize the System Logging Facility, and Monitor and Control Superuser	106
Configuring syslog and Customizing the System Logging Facility	106
Monitoring and Controlling Superuser Access	109
✓ Two-Minute Drill	111
Q&A Self Test	113
Lab Question	115
Self Test Answers	116
Lab Answer	118
 5 Solaris Auditing, Planning, and Management	 121
Configure Solaris Auditing and Customize Audit Events	122
Solaris Auditing	123
Generate an Audit Trail and Analyze the Audit Data	136
✓ Two-Minute Drill	139
Q&A Self Test	141
Lab Question	144
Self Test Answers	145
Lab Answer	148

6	Device, System, and File Security	151
	Control Access to Devices by Configuring and Managing Device Policy and Device Allocation	152
	Device Policy	152
	Device Allocation	157
	Use the Basic Audit Reporting Tool to Create a Manifest and Check System Integrity	162
	Creating a Manifest	162
	Comparing Manifests	165
	✓ Two-Minute Drill	167
	Q&A Self Test	169
	Lab Question	171
	Self Test Answers	172
	Lab Answer	174

Part III
Security Attacks

7	Denial of Service Attacks	179
	Differentiate Between the Types of Host-Based Denial of Service Attacks and Understand How Attacks Are Executed	180
	Program Buffer Overflow	181
	Malformed Packet Attacks and Flooding	183
	Establish Courses of Action to Prevent Denial of Service Attacks	194
	Preventing Stack-Based Buffer Overflow Attacks	195
	Preventing General DoS Attacks, Malformed Packet Attacks, and Flooding	197
	✓ Two-Minute Drill	207
	Q&A Self Test	209
	Lab Question	212
	Self Test Answers	213
	Lab Answer	216
8	Remote Access Attacks	217
	Identify, Detect, and Protect Against Trojan Horse Programs and Backdoors	218
	Securing the System from Trojans and Backdoors	219

Explain Rootkits that Exploit Loadable Kernel Modules	236
Rootkits and Loadable Kernel Modules	237
✓ Two-Minute Drill	240
Q&A Self Test	243
Lab Question	246
Self Test Answers	247
Lab Answer	250

Part IV

File and System Resources Protection

9 User and Domain Account Management with RBAC 255

Describe the Benefits and Capabilities of Role-Based Access Control (RBAC)	256
Authorization	257
Privilege	258
Privileged Application	260
Rights Profile	260
Role	260
Explain How to Configure and Audit Role-Based Access Control (RBAC)	261
Managing Rights and Roles	262
✓ Two-Minute Drill	270
Q&A Self Test	272
Lab Question	275
Self Test Answers	276
Lab Answer	279

10 Fundamentals of Access Control 281

Use UNIX Permissions to Protect Files	282
Listing and Securing Files and Directories	283
Use Access Control Lists to Set File Permissions	293
Working with ACLs	294
✓ Two-Minute Drill	296
Q&A Self Test	297

Lab Question	298
Self Test Answers	299
Lab Answer	301

Part V
Solaris Cryptographic Framework

11 Using Cryptographic Services	305
Explain How to Protect Files Using the Solaris Cryptographic Framework	307
Generating Symmetric Keys	307
Ensuring the Integrity of Files Using Checksum	308
Protecting Files with a Message Authentication Code (MAC)	312
Encrypting and Decrypting Files	314
Administer the Solaris Cryptographic Framework	315
Listing Available Providers	315
Preventing the Use of a User-Level Mechanism	318
✓ Two-Minute Drill	321
Q&A Self Test	323
Lab Question	325
Self Test Answers	326
Lab Answer	328

Part VI
Authentication Services and Secure Communication

12 Secure RPC Across NFS and PAM	333
Explain and Configure Secure RPC to Authenticate a Host and a User Across an NFS Mount	334
Generating the Public and Secret Keys	335
Configuring Secure RPC for NIS, NIS+, and NFS	338
Use the PAM Framework to Configure the Use of System Entry Services for User Authentication	341
Planning for PAM Implementation	342
✓ Two-Minute Drill	346
Q&A Self Test	349

Lab Question	350
Self Test Answers	351
Lab Answer	352
13 SASL and Secure Shell	355
Explain the Simple Authentication and Security Layer (SASL) in Solaris	356
SASL Overview and Introduction	356
Use Solaris Secure Shell to Access a Remote Host Securely Over an Unsecured Network	358
Solaris Secure Shell Authentication	359
Using Solaris Secure Shell—Key Generation	360
✓ Two-Minute Drill	367
Q&A Self Test	369
Lab Question	370
Self Test Answers	371
Lab Answer	374
14 Sun Enterprise Authentication Mechanism	375
Define the Sun Enterprise Authentication Mechanism and Configuration Issues	376
How SEAM Works	376
SEAM Preconfiguration Planning	379
Configure and Administer the Sun Enterprise Authentication Mechanism	384
Configuring KDC Servers	385
Configuring Cross-Realm Authentication	393
Configuring SEAM Network Application Servers	396
Configuring SEAM NFS Servers	398
Configuring SEAM Clients	401
Synchronizing Clocks Between KDCs and SEAM Clients	403
Increasing Security	404
✓ Two-Minute Drill	406
Q&A Self Test	409
Lab Question	410
Self Test Answers	411
Lab Answer	413

Part VII
Appendixes

A	Final Test Study Guide	423
B	Final Test	447
C	Final Test Answers	475
D	Hands-On Exercises and Solutions	499
	Exercises	500
	Solutions	502
	Index	515