CompTIA Security+™ Certification Study Guide

(Exam SY0-301)

Glen E. Clarke

New York Chicago San Francisco Lisbon London Madrid
Mexico City Milan New Delhi San Juan Seoul Singapore Sydney Toronto

CONTENTS

Preface ..... *xxvii*
Acknowledgments ..... *xxxi*
Introduction ..... *xxxiii*

1 Networking Basics and Terminology 1

Understanding Network Devices and Cabling 2
Looking at Network Devices 2
Understanding Network Cabling 10
Exercise 1-1: Reviewing Networking Components 19
Understanding TCP/IP 19
Reviewing IP Addressing 20
Exercise 1-2: Understanding Valid Addresses 25
Understanding TCP/IP Protocols 26
Exercise 1-3: Viewing Protocol Information with Network Monitor 37
Application Layer Protocols 42
A Review of IPv6 49
Exercise 1-4: Identifying Protocols in TCP/IP 52
Network Security Best Practices 52
Device Usage 52
Cable and Protocol Usage 54
✓ Two-Minute Drill 57
Q&A Self Test 59
Self Test Answers 62

2 Introduction to Security Terminology 65

Goals of Information Security 66
Confidentiality 66
Integrity 69
Availability 70
Accountability 71

Understanding Authentication and Authorization 72
Identification and Authentication 72
Authorization 73
Understanding Security Principles and Terminology 76
Types of Security 76
Least Privilege, Separation of Duties, and Rotation of Duties .. 77
Concept of Need to Know 79
Layered Security and Diversity of Defense 79
Due Care, Due Diligence 80
Vulnerability and Exploits 80
Looking at Security Roles 81
System and Data Owner 81
Custodian 81
User 81
Security Officer 82
Exercise 2-1: Security Terminology 82
✓ Two-Minute Drill 84
Q&A Self Test 87
Self Test Answers 91

3 Security Policies and Standards 95

Introduction to Security Policies 96
Structure of a Policy 97
Identifying Types of Policies 98
Understanding Regulations and Standards 99
Looking at Security Policies 101
Policies Affecting Users 101
Policies Affecting Administrators 103
Exercise 3-1: Reviewing a Security Policy 104
Policies Affecting Management 105
Other Popular Policies 107
Human Resource Policies 108
Hiring Policy 108
Termination Policy 109
Mandatory Vacations 110
Security-Related HR Policies 110
Exercise 3-2: Creating a Security Policy 111

User Education and Awareness 111
General Training 112
User Habits 114
Threat Awareness 115
Use of Social Network and P2P 116
Exercise 3-3: Designing a Training Program 117
✓ Two-Minute Drill 119
Q&A Self Test 121
Self Test Answers 125

4 Types of Attacks 129

Understanding Social Engineering 130
Social Engineering Overview 130
Popular Social Engineering Attacks 130
Preventing Social Engineering Attacks 135
Identifying Network Attacks 136
Popular Network Attacks 136
Exercise 4-1: DNS Poisoning by Modifying the Hosts File . 144
Exercise 4-2: Performing a Port Scan 147
Other Network Attacks 148
Preventing Network Attacks 149
Looking at Password Attacks 150
Types of Password Attacks 150
Exercise 4-3: Password Cracking with LC4 152
Preventing Password Attacks 154
Understanding Application Attacks 156
Popular Application Attacks 156
Exercise 4-4: SQL Injection Attacks 158
Exercise 4-5: Exploiting an IIS Web Server with Folder Traversal 161
Other Application Attacks 162
Preventing Application Attacks 163
✓ Two-Minute Drill 165
Q&A Self Test 167
Self Test Answers 171

5 System Security Threats 175

Identifying Physical Threats 176
Snooping 176
Theft and Loss of Assets 177
Human Error 179
Sabotage 179
Looking at Malicious Software 179
Privilege Escalation 180
Viruses 180
Exercise 5-1: Looking at the NetBus Trojan Virus 182
Other Malicious Software 189
Protecting Against Malicious Software 194
Threats Against Hardware 195
BIOS Settings 195
USB Devices 195
Cell Phones 197
Exercise 5-2: Exploiting a Bluetooth Device 197
Removable Storage 201
Network Attached Storage 201
PBX 203
✓ Two-Minute Drill 206
Q&A Self Test 208
Self Test Answers 211

6 Mitigating Security Threats 215

Understanding Operating System Hardening 216
Uninstall Unnecessary Software 217
Disable Unnecessary Services 220
Exercise 6-1: Disabling the Messenger Service 222
Protect Management Interfaces and Applications 223
Disable Unnecessary Accounts 224
Patch System 225
Password Protection 226
System Hardening Procedures 227
Network Hardening 227
Exercise 6-2: Hardening a Network Switch 230
Tools for System Hardening 231

Exercise 6-3: Creating a Security Template 236
Security Posture and Reporting 241
Establishing Application Security 243
Secure Coding Concepts 243
Application Hardening 245
Server Hardening Best Practices 247
All Servers 248
HTTP Servers 248
DNS Servers 248
Exercise 6-4: Limiting DNS Zone Transfers 250
DHCP Servers 251
SMTP Servers and FTP Servers 252
✓ Two-Minute Drill 254
Q&A Self Test 256
Self Test Answers 260

7 Implementing System Security 263

Implementing Personal Firewalls and HIDS 264
Personal Firewalls 264
Exercise 7-1: Configuring TCP Wrappers in Linux 279
Host-Based IDS 279
Protecting Against Malware 281
Patch Management 281
Using Antivirus and Anti-spam Software 289
Spyware and Adware 293
Phish Filters and Pop-up Blockers 293
Exercise 7-2: Manually Testing a Web Site for Phishing 297
Practicing Good Habits 297
Device Security and Data Security 298
Hardware Security 298
Mobile Devices 299
Data Security 302
Exercise 7-3: Configuring Permissions in Windows 2003 304
Understanding Virtualization and Cloud Computing 311
Virtualization and Security 311
Cloud Computing Issues 314
✓ Two-Minute Drill 316

Q&A Self Test 317
Self Test Answers 320

8 Securing the Network Infrastructure 323

Understanding Firewalls 324
Firewalls 324
Using IPTables as a Firewall 328
Exercise 8-1: Configuring IPTables in Linux 329
Using Firewall Features on a Home Router 332
Proxy Servers 336
Other Security Devices and Technologies 337
Using Intrusion Detection Systems 339
IDS Overview 339
Exercise 8-2: Using Snort—A Network-Based IDS 343
Honeypots and Honeynet 347
Protocol Analyzers 348
Network Design and Administration Principles 349
Subnetting and VLANs 349
Network Address Translation (NAT) 351
Network Access Control (NAC) 353
Network Administration Principles 354
Securing Devices 356
✓ Two-Minute Drill 359
Q&A Self Test 361
Self Test Answers 364

9 Wireless Networking and Security 367

Understanding Wireless Networking 368
Standards 369
Channels 371
Authentication and Encryption 372
Securing a Wireless Network 375
Security Best Practices 376
Vulnerabilities with Wireless Networks 382
Exercise 9-1: Cracking WEP with BackTrack 385
Configuring a Wireless Network 393
Configuring the Access Point 393

Configuring the Client 402
Infrared and Bluetooth 406
Infrared 406
Bluetooth 407
✓ Two-Minute Drill 409
Q&A Self Test 411
Self Test Answers 414

10 Authentication 417

Identifying Authentication Models 418
Authentication Terminology 418
Authentication Factors 419
Single Sign-on 421
Authentication Protocols 422
Windows Authentication Protocols 423
Remote Access Authentication 424
Authentication Services 425
Implementing Authentication 428
User Accounts 428
Tokens 429
Looking at Biometrics 430
Smartcard 431
✓ Two-Minute Drill 433
Q&A Self Test 434
Self Test Answers 436

11 Access Control 439

Introducing Access Control 440
Types of Security Controls 440
Implicit Deny 442
Review of Security Principles 443
Access Control Models 444
Discretionary Access Control 444
Mandatory Access Control 444
Role-Based Access Control 448
Exercise 11-1: Assigning a User the sysadmin Role 449
Rule-Based Access Control 450

Implementing Access Control 451
Using Security Groups 451
Exercise 11-2: Configuring Security Groups and Assigning Permissions 452
Rights and Privileges 454
Exercise 11-3: Modifying User Rights on a Windows System . 455
Securing Files and Printers 457
Access Control Lists (ACLs) 458
Group Policies 460
Exercise 11-4: Configuring Password Policies via Group Policies 462
Account Restrictions 463
✓ Two-Minute Drill 468
Q&A Self Test 469
Self Test Answers 472

12 Introduction to Cryptography 475

Introduction to Cryptography Services 476
Understanding Cryptography 476
Algorithms and Keys 479
Exercise 12-1: Encrypting Data with the Caesar Cipher .. 480
Other Cryptography Terms 484
Symmetric Encryption 487
Symmetric Encryption Concepts 487
Symmetric Encryption Algorithms 489
Exercise 12-2: Encrypting Data with the AES Algorithm . 490
Asymmetric Encryption 492
Asymmetric Encryption Concepts 492
Asymmetric Encryption Algorithms 495
Quantum Cryptography 495
Understanding Hashing 496
Hashing Concepts 496
Hashing Algorithms 497
Exercise 12-3: Generating Hashes to Verify Integrity 498
Identifying Encryption Uses 500
Encrypting Data 501
Encrypting Communication 502

Understanding Steganography 504
✓ Two-Minute Drill 506
Q&A Self Test 508
Self Test Answers 511

13 Managing a Public Key Infrastructure 513

Introduction to Public Key Infrastructure 514
Understanding PKI Terminology 515
Certificate Authority and Registration Authority 517
Repository 519
Managing a Public Key Infrastructure 519
Certificate Life Cycle 519
Certificate Revocation Lists 520
Other PKI Terms 521
Implementing a Public Key Infrastructure 523
How SSL Works 523
How Digital Signatures Work 524
Creating a PKI 524
Exercise 13-1: Installing a Certificate Authority 526
Exercise 13-2: SSL-Enabling a Web Site 530
Managing a PKI 539
✓ Two-Minute Drill 543
Q&A Self Test 544
Self Test Answers 546

14 Physical Security 549

Choosing a Business Location 551
Facility Concerns 551
Lighting and Windows 551
Doors, Windows, and Walls 552
Physical Access Controls 553
Exercise 14-1: Erasing the Administrator Password with a Live CD 554
Fencing and Guards 558
Hardware Locks 560
Access Systems 561

Physical Access Lists and Logs 563
Video Surveillance 563
Implementing Environmental Controls 565
Understanding HVAC 565
Shielding 566
Fire Suppression 566
✓ Two-Minute Drill 569
Q&A Self Test 570
Self Test Answers 573

15 Risk Analysis 575

Introduction to Risk Analysis 576
Risk Analysis Overview 576
Risk Analysis Process 577
Types of Risk Analysis 582
Qualitative 582
Exercise 15-1: Performing a Qualitative Risk Analysis 585
Quantitative 585
Exercise 15-2: Performing a Quantitative Risk Analysis .. 587
Risk Mitigation Strategies 588
Exercise 15-3: Identifying Mitigation Techniques 590
✓ Two-Minute Drill 592
Q&A Self Test 593
Self Test Answers 596

16 Disaster Recovery and Business Continuity 599

Introduction to Disaster Recovery and Business Continuity 600
Introduction to Business Continuity 600
Understanding Disaster Recovery 604
Backing Up and Restoring Data 607
Security Considerations with Tapes 608
Full, Incremental, and Differential Backups 608
Scheduling Backups 611
Backup Plan Example 612
Exercise 16-1: Backing Up and Restoring Data on a Windows Server 613

Implementing Fault Tolerance 617
RAID 0 617
RAID 1 623
RAID 5 626
Understanding High Availability 629
Clustering Services 630
Network Load Balancing 631
Redundant Hardware 631
✓ Two-Minute Drill 634
Q&A Self Test 636
Self Test Answers 639

17 Introduction to Computer Forensics 641

Working with Evidence 642
Types of Evidence 643
Collecting Evidence 643
Collecting Digital Evidence 647
Understanding the Process 647
Where to Find Evidence 652
Tools Used 653
Exercise 17-1: Using ProDiscover for Forensics Analysis .. 659
Exercise 17-2: Performing Cell Phone Forensics 665
Exercise 17-3: Looking at EXIF Metadata 673
Looking at Incident Response 673
Incident Response Team 673
First Responders 674
Damage and Loss Control 675
✓ Two-Minute Drill 677
Q&A Self Test 679
Self Test Answers 682

18 Security Assessments and Audits 685

Understanding Types of Assessments 686
Assessment Types 686
Assessment Techniques 696
Performing a Security Assessment 698

Performing a Penetration Test 699
Exercise 18-1: Profiling an Organization 701
Exercise 18-2: Using a Port Scanner 712
Performing a Vulnerability Assessment 718
Exercise 18-3: Performing a Vulnerability Scan with LANguard 721
✓ Two-Minute Drill 728
Q&A Self Test 730
Self Test Answers 734

19 Understanding Monitoring and Auditing 737

Introduction to Monitoring 738
Monitoring Tools 740
Useful System Commands 740
Performance Monitor 744
Protocol Analyzer and Sniffer 746
Exercise 19-1: Monitoring Network Traffic with Network Monitor 747
Implementing Logging and Auditing 750
Understanding Auditing 750
Exercise 19-2: Implementing Auditing in Windows 757
Understanding Logging 758
Exercise 19-3: Configuring Logging in IIS 759
Exercise 19-4: Configuring the Windows Firewall 761
Popular Areas to Audit 764
✓ Two-Minute Drill 767
Q&A Self Test 768
Self Test Answers 771

About the CD 773

Index 777