



# CompTIA® Security+ Guide to Network Security Fundamentals

## Fifth Edition

**Mark Ciampa, Ph.D.**



---

Australia • Brazil • Japan • Korea • Mexico • Singapore • Spain • United Kingdom • United States

# Brief Contents

INTRODUCTION . . . . .	xiii
CHAPTER 1	
<b>Introduction to Security . . . . .</b>	<b>1</b>
<b>PART I     Threats</b>	<b>47</b>
CHAPTER 2	
<b>Malware and Social Engineering Attacks . . . . .</b>	<b>49</b>
CHAPTER 3	
<b>Application and Networking-Based Attacks . . . . .</b>	<b>91</b>
<b>PART II     Application, Data, and Host Security</b>	<b>135</b>
CHAPTER 4	
<b>Host, Application, and Data Security . . . . .</b>	<b>137</b>
<b>PART III     Cryptography</b>	<b>181</b>
CHAPTER 5	
<b>Basic Cryptography . . . . .</b>	<b>183</b>
CHAPTER 6	
<b>Advanced Cryptography . . . . .</b>	<b>227</b>
<b>PART IV     Network Security</b>	<b>267</b>
CHAPTER 7	
<b>Network Security Fundamentals . . . . .</b>	<b>269</b>
CHAPTER 8	
<b>Administering a Secure Network . . . . .</b>	<b>311</b>
<b>PART V     Mobile Security</b>	<b>357</b>
CHAPTER 9	
<b>Wireless Network Security . . . . .</b>	<b>359</b>
CHAPTER 10	
<b>Mobile Device Security . . . . .</b>	<b>403</b>

<b>PART VI</b>	<b>Access Control and Identity Management</b>	<b>439</b>
<hr/>		
CHAPTER 11	<b>Access Control Fundamentals</b> . . . . .	<b>441</b>
CHAPTER 12	<b>Authentication and Account Management</b> . . . . .	<b>477</b>
<b>PART VII</b>	<b>Compliance and Operational Security</b>	<b>521</b>
<hr/>		
CHAPTER 13	<b>Business Continuity</b> . . . . .	<b>523</b>
CHAPTER 14	<b>Risk Mitigation</b> . . . . .	<b>565</b>
CHAPTER 15	<b>Vulnerability Assessment</b> . . . . .	<b>605</b>
APPENDIX A	<b>CompTIA SY0-401 Certification Exam Objectives</b> . . . . .	<b>645</b>
APPENDIX B	<b>Downloads and Tools for Hands-On Projects</b> . . . . .	<b>663</b>
APPENDIX C	<b>Security Websites</b> . . . . .	<b>665</b>
APPENDIX D	<b>Selected TCP/IP Ports and Their Threats</b> . . . . .	<b>669</b>
APPENDIX E	<b>Information Security Community Site</b> . . . . .	<b>673</b>
GLOSSARY	. . . . .	<b>675</b>
INDEX	. . . . .	<b>685</b>

# Table of Contents

INTRODUCTION . . . . .	xiii
CHAPTER 1	
<b>Introduction to Security . . . . .</b>	<b>1</b>
<b>Challenges of Securing Information . . . . .</b>	<b>5</b>
Today's Security Attacks . . . . .	5
Difficulties in Defending Against Attacks . . . . .	8
<b>What Is Information Security? . . . . .</b>	<b>11</b>
Understanding Security . . . . .	11
Defining Information Security . . . . .	13
Information Security Terminology . . . . .	14
Understanding the Importance of Information Security . . . . .	17
<b>Who Are the Attackers? . . . . .</b>	<b>21</b>
Cybercriminals . . . . .	21
Script Kiddies . . . . .	22
Brokers . . . . .	23
Insiders . . . . .	23
Cyberterrorists . . . . .	24
Hactivists . . . . .	24
State-Sponsored Attackers . . . . .	24
<b>Attacks and Defenses . . . . .</b>	<b>25</b>
Steps of an Attack . . . . .	26
Defenses Against Attacks . . . . .	27
<b>Chapter Summary . . . . .</b>	<b>30</b>
<b>Key Terms . . . . .</b>	<b>30</b>
<b>Review Questions . . . . .</b>	<b>32</b>
<b>Hands-On Projects . . . . .</b>	<b>35</b>
<b>Case Projects . . . . .</b>	<b>41</b>
<b>References . . . . .</b>	<b>43</b>
<b>PART I      Threats . . . . .</b>	<b>47</b>

CHAPTER 2	
<b>Malware and Social Engineering Attacks . . . . .</b>	<b>49</b>
<b>Attacks Using Malware . . . . .</b>	<b>51</b>
Circulation/Infection . . . . .	53
Concealment . . . . .	58
Payload Capabilities . . . . .	59
<b>Social Engineering Attacks . . . . .</b>	<b>66</b>
Psychological Approaches . . . . .	67
Physical Procedures . . . . .	73
<b>Chapter Summary . . . . .</b>	<b>74</b>
<b>Key Terms . . . . .</b>	<b>76</b>
<b>Review Questions . . . . .</b>	<b>78</b>

Hands-On Projects . . . . . 81

Case Projects . . . . . 86

References . . . . . 90

CHAPTER 3

**Application and Networking-Based Attacks . . . . . 91**

Application Attacks . . . . . 93

    Server-Side Web Application Attacks . . . . . 94

    Client-Side Application Attacks . . . . . 101

    Impartial Overflow Attacks . . . . . 107

Networking-Based Attacks . . . . . 109

    Denial of Service (DoS). . . . . 109

    Interception . . . . . 111

    Poisoning . . . . . 113

    Attacks on Access Rights . . . . . 117

Chapter Summary . . . . . 118

Key Terms . . . . . 120

Review Questions . . . . . 122

Hands-On Projects . . . . . 125

Case Projects . . . . . 132

**PART II Application, Data, and Host Security 135**

---

CHAPTER 4

**Host, Application, and Data Security . . . . . 137**

Securing the Host . . . . . 139

    Securing Devices . . . . . 139

    Securing the Operating System Software . . . . . 148

    Securing with Antimalware . . . . . 153

Securing Static Environments . . . . . 155

Application Security . . . . . 157

    Application Development Security . . . . . 157

    Application Hardening and Patch Management . . . . . 160

Securing Data . . . . . 161

Chapter Summary . . . . . 164

Key Terms . . . . . 166

Review Questions . . . . . 168

Hands-On Projects . . . . . 172

Case Projects . . . . . 177

References . . . . . 179

**PART III**    **Cryptography****181**

## CHAPTER 5

<b>Basic Cryptography</b> . . . . .	<b>183</b>
<b>Defining Cryptography</b> . . . . .	185
What Is Cryptography? . . . . .	186
Cryptography and Security . . . . .	187
<b>Cryptographic Algorithms</b> . . . . .	189
Hash Algorithms . . . . .	190
Symmetric Cryptographic Algorithms . . . . .	194
Asymmetric Cryptographic Algorithms . . . . .	199
<b>Using Cryptography</b> . . . . .	206
Encryption Through Software . . . . .	206
Hardware Encryption . . . . .	208
<b>Chapter Summary</b> . . . . .	209
<b>Key Terms</b> . . . . .	211
<b>Review Questions</b> . . . . .	213
<b>Hands-On Projects</b> . . . . .	216
<b>Case Projects</b> . . . . .	224
<b>References</b> . . . . .	226

## CHAPTER 6

<b>Advanced Cryptography</b> . . . . .	<b>227</b>
<b>Digital Certificates</b> . . . . .	229
Defining Digital Certificates . . . . .	230
Managing Digital Certificates . . . . .	231
Types of Digital Certificates . . . . .	235
<b>Public Key Infrastructure (PKI)</b> . . . . .	240
What Is Public Key Infrastructure (PKI)? . . . . .	240
Public Key Cryptography Standards (PKCS) . . . . .	240
Trust Models . . . . .	240
Managing PKI . . . . .	244
<b>Key Management</b> . . . . .	246
Key Storage . . . . .	246
Key Usage . . . . .	247
Key Handling Procedures . . . . .	247
<b>Cryptographic Transport Protocols</b> . . . . .	249
Secure Sockets Layer (SSL) . . . . .	249
Transport Layer Security (TLS) . . . . .	249
Secure Shell (SSH) . . . . .	250
Hypertext Transport Protocol Secure (HTTPS) . . . . .	251
IP Security (IPsec) . . . . .	251
<b>Chapter Summary</b> . . . . .	253
<b>Key Terms</b> . . . . .	254
<b>Review Questions</b> . . . . .	255
<b>Hands-On Projects</b> . . . . .	258
<b>Case Projects</b> . . . . .	264
<b>References</b> . . . . .	265

**PART IV Network Security****267**

## CHAPTER 7

<b>Network Security Fundamentals</b> . . . . .	<b>269</b>
<b>Security Through Network Devices</b> . . . . .	272
Standard Network Devices . . . . .	272
Network Security Hardware . . . . .	279
<b>Security Through Network Technologies</b> . . . . .	289
Network Address Translation (NAT) . . . . .	290
Network Access Control (NAC) . . . . .	291
<b>Security Through Network Design Elements</b> . . . . .	293
Demilitarized Zone (DMZ) . . . . .	293
Subnetting . . . . .	293
Virtual LANs (VLANs) . . . . .	296
Remote Access . . . . .	297
<b>Chapter Summary</b> . . . . .	297
<b>Key Terms</b> . . . . .	299
<b>Review Questions</b> . . . . .	300
<b>Hands-On Projects</b> . . . . .	304
<b>Case Projects</b> . . . . .	309

## CHAPTER 8

<b>Administering a Secure Network</b> . . . . .	<b>311</b>
<b>Common Network Protocols</b> . . . . .	313
Internet Control Message Protocol (ICMP) . . . . .	314
Simple Network Management Protocol (SNMP) . . . . .	316
Domain Name System (DNS) . . . . .	317
File Transfer Protocols . . . . .	318
Storage Protocols . . . . .	320
NetBIOS . . . . .	323
Telnet . . . . .	323
IPv6 . . . . .	323
<b>Network Administration Principles</b> . . . . .	325
Device Security . . . . .	326
Monitoring and Analyzing Logs . . . . .	327
Network Design Management . . . . .	330
Port Security . . . . .	332
<b>Securing Network Applications and Platforms</b> . . . . .	333
IP Telephony . . . . .	334
Virtualization . . . . .	335
Cloud Computing . . . . .	337
<b>Chapter Summary</b> . . . . .	339
<b>Key Terms</b> . . . . .	341
<b>Review Questions</b> . . . . .	343
<b>Hands-On Projects</b> . . . . .	346
<b>Case Projects</b> . . . . .	354
<b>References</b> . . . . .	355

**PART V Mobile Security 357**

## CHAPTER 9

<b>Wireless Network Security</b> . . . . .	<b>359</b>
<b>Wireless Attacks</b> . . . . .	<b>361</b>
Bluetooth Attacks . . . . .	361
Near Field Communication (NFC) Attacks . . . . .	364
Wireless Local Area Network (WLAN) Attacks . . . . .	366
<b>Vulnerabilities of IEEE Wireless Security</b> . . . . .	<b>376</b>
Wired Equivalent Privacy (WEP) . . . . .	376
Wi-Fi Protected Setup (WPS) . . . . .	377
MAC Address Filtering . . . . .	377
Disabling SSID Broadcasts . . . . .	379
<b>Wireless Security Solutions</b> . . . . .	<b>379</b>
Wi-Fi Protected Access (WPA) . . . . .	380
Wi-Fi Protected Access 2 (WPA2) . . . . .	382
Additional Wireless Security Protections . . . . .	384
<b>Chapter Summary</b> . . . . .	<b>386</b>
<b>Key Terms</b> . . . . .	<b>388</b>
<b>Review Questions</b> . . . . .	<b>390</b>
<b>Hands-On Projects</b> . . . . .	<b>393</b>
<b>Case Projects</b> . . . . .	<b>399</b>
<b>References</b> . . . . .	<b>401</b>

## CHAPTER 10

<b>Mobile Device Security</b> . . . . .	<b>403</b>
<b>Types of Mobile Devices</b> . . . . .	<b>406</b>
Portable Computers . . . . .	406
Tablets . . . . .	408
Smartphones . . . . .	409
Wearable Technology . . . . .	409
Legacy Devices . . . . .	411
Mobile Device Removable Storage . . . . .	411
<b>Mobile Device Risks</b> . . . . .	<b>413</b>
Limited Physical Security . . . . .	414
Connecting to Public Networks . . . . .	415
Location Tracking . . . . .	415
Installing Unsecured Applications . . . . .	415
Accessing Untrusted Content . . . . .	417
Bring Your Own Device (BYOD) Risks . . . . .	417
<b>Securing Mobile Devices</b> . . . . .	<b>418</b>
Device Setup . . . . .	418
Device and App Management . . . . .	421
Device Loss or Theft . . . . .	422
<b>Mobile Device App Security</b> . . . . .	<b>423</b>
<b>BYOD Security</b> . . . . .	<b>423</b>
<b>Chapter Summary</b> . . . . .	<b>424</b>
<b>Key Terms</b> . . . . .	<b>426</b>
<b>Review Questions</b> . . . . .	<b>426</b>



Hands-On Projects . . . . . 430  
 Case Projects . . . . . 435  
 References . . . . . 437

**PART VI Access Control and Identity Management 439**

CHAPTER 11

**Access Control Fundamentals . . . . . 441**

**What Is Access Control? . . . . . 443**

        Access Control Terminology . . . . . 444

        Access Control Models . . . . . 445

        Best Practices for Access Control . . . . . 450

**Implementing Access Control . . . . . 453**

        Access Control Lists (ACLs) . . . . . 454

        Group Policies . . . . . 455

        Account Restrictions . . . . . 456

**Authentication Services . . . . . 457**

        RADIUS . . . . . 458

        Kerberos . . . . . 460

        Terminal Access Control Access Control System (TACACS) . . . . . 460

        Lightweight Directory Access Protocol (LDAP) . . . . . 461

        Security Assertion Markup Language (SAML) . . . . . 462

**Chapter Summary . . . . . 464**

**Key Terms . . . . . 465**

**Review Questions . . . . . 466**

**Hands-On Projects . . . . . 469**

**Case Projects . . . . . 473**

**Reference . . . . . 475**

CHAPTER 12

**Authentication and Account Management . . . . . 477**

**Authentication Credentials . . . . . 480**

        What You Know: Passwords . . . . . 481

        What You Have: Tokens, Cards, and Cell Phones . . . . . 492

        What You Are: Biometrics . . . . . 495

        What You Do: Behavioral Biometrics . . . . . 497

        Where You Are: Geolocation . . . . . 499

**Single Sign-On . . . . . 500**

        Microsoft Account . . . . . 500

        OpenID . . . . . 501

        Open Authorization (OAuth) . . . . . 501

**Account Management . . . . . 502**

**Chapter Summary . . . . . 504**

**Key Terms . . . . . 506**

**Review Questions . . . . . 507**

**Hands-On Projects . . . . . 511**

Case Projects . . . . .	518
References . . . . .	520

---

<b>PART VII</b>	<b>Compliance and Operational Security</b>	<b>521</b>
-----------------	--	------------

---

## CHAPTER 13

<b>Business Continuity . . . . .</b>	<b>523</b>
What Is Business Continuity? . . . . .	525
Disaster Recovery . . . . .	526
Disaster Recovery Plan (DRP) . . . . .	526
Redundancy and Fault Tolerance . . . . .	529
Data Backups . . . . .	537
Environmental Controls . . . . .	540
Fire Suppression . . . . .	540
Electromagnetic Interference (EMI) Shielding . . . . .	543
HVAC . . . . .	544
Incident Response . . . . .	545
Forensics . . . . .	545
Incident Response Procedures . . . . .	550
Chapter Summary . . . . .	551
Key Terms . . . . .	552
Review Questions . . . . .	554
Hands-On Projects . . . . .	557
Case Projects . . . . .	562
References . . . . .	564

## CHAPTER 14

<b>Risk Mitigation . . . . .</b>	<b>565</b>
Controlling Risk . . . . .	567
Privilege Management . . . . .	569
Change Management . . . . .	571
Incident Management . . . . .	572
Risk Calculation . . . . .	572
Reducing Risk Through Policies . . . . .	574
What Is a Security Policy? . . . . .	574
Balancing Trust and Control . . . . .	575
Designing a Security Policy . . . . .	576
Types of Security Policies . . . . .	579
Awareness and Training . . . . .	585
Compliance . . . . .	585
User Practices . . . . .	586
Threat Awareness . . . . .	586
Training Techniques . . . . .	590
Chapter Summary . . . . .	591
Key Terms . . . . .	592
Review Questions . . . . .	594
Hands-On Projects . . . . .	597

Case Projects . . . . .	601
Reference . . . . .	603
CHAPTER 15	
<b>Vulnerability Assessment . . . . .</b>	<b>605</b>
Assessing Vulnerabilities . . . . .	607
What Is Vulnerability Assessment? . . . . .	608
Assessment Techniques . . . . .	612
Assessment Tools . . . . .	614
Vulnerability Scanning vs. Penetration Testing . . . . .	621
Vulnerability Scanning . . . . .	621
Penetration Testing . . . . .	622
Third-Party Integration . . . . .	624
Mitigating and Deterring Attacks . . . . .	626
Creating a Security Posture . . . . .	626
Selecting Appropriate Controls . . . . .	626
Configuring Controls . . . . .	626
Hardening . . . . .	627
Reporting . . . . .	627
Chapter Summary . . . . .	628
Key Terms . . . . .	629
Review Questions . . . . .	631
Hands-On Projects . . . . .	634
Case Projects . . . . .	640
References . . . . .	643
APPENDIX A	
<b>CompTIA SY0-401 Certification Exam Objectives . . . . .</b>	<b>645</b>
APPENDIX B	
<b>Downloads and Tools for Hands-On Projects . . . . .</b>	<b>663</b>
APPENDIX C	
<b>Security Websites . . . . .</b>	<b>665</b>
APPENDIX D	
<b>Selected TCP/IP Ports and Their Threats . . . . .</b>	<b>669</b>
APPENDIX E	
<b>Information Security Community Site . . . . .</b>	<b>673</b>
GLOSSARY . . . . .	675
INDEX . . . . .	685