

CONTENTS IN DETAIL

ACKNOWLEDGMENTS	xxi
------------------------	------------

INTRODUCTION	xxiii
---------------------	--------------

Who Should Read This Book?	xxiv
What's New in This Edition?	xxiv
About This Book	xxiv

PART I CORE PRINCIPLES

1 WHAT IS CYBERSECURITY?	3
-------------------------------------	----------

Defining Cybersecurity	4
When Are You Secure?	4
Models for Discussing Security Issues	6
The Confidentiality, Integrity, and Availability Triad	6
The Parkerian Hexad	7
Attacks	9
Classification of Attacks	9
Threats, Vulnerabilities, and Risks	11
Defense in Depth	12
Summary	15
Review Questions	16
Project #1: Testing Password Entropy	17

2 THE THREAT LANDSCAPE	19
-----------------------------------	-----------

State Actors	20
Intergovernmental Organizations	20
State-Sponsored Actors	20
Non-State Actors	21
Security Researchers	21
Corporations	21
Criminal Groups	22
Malware Authors	22
Hacktivists and Patriot Hackers	23

Autonomous Actors	23
Attribution	25
Threat Actor Skill Levels	25
Summary	26
Review Questions	27
Project #2: Classifying Edward Snowden	27

3 IDENTIFICATION AND AUTHENTICATION 29

Identification	30
Who We Claim to Be	30
Identity Verification	30
Identity Falsification	31
Authentication	31
Factors	31
Multifactor Authentication	33
Mutual Authentication	34
Common Identification and Authentication Methods	34
Passwords	35
Biometrics	35
Hardware Tokens	39
Summary	39
Review Questions	40
Project #3: Hashing Passwords	41

4 AUTHORIZATION AND ACCESS CONTROLS 43

What Are Access Controls?	44
Implementing Access Controls	45
Access Control Lists	46
Capabilities	50
Access Control Models	51
Discretionary	51
Mandatory	51
Rule-Based	52
Role-Based	52
Attribute-Based	52
Multilevel	53

Physical Access Controls	56
Summary	57
Review Questions	58
Project #4: Finding Confused Deputies in the Wild	59

5

AUDITING AND ACCOUNTABILITY

61

Accountability	62
Security Benefits of Accountability	63
Nonrepudiation	64
Deterrence	64
Intrusion Detection and Prevention	64
Admissibility of Records	65
Auditing	65
Choosing What to Audit	65
Logging	66
Monitoring	67
Auditing with Assessments	67
Summary	69
Review Questions	69
Project #5: Working with Audit Logs	69

6

CRYPTOGRAPHY

73

The History of Cryptography	74
The Caesar Cipher	74
Cryptographic Machines	75
Kerckhoffs's Principles	78
Modern Cryptographic Tools	79
Keyword Ciphers and One-Time Pads	80
Symmetric and Asymmetric Cryptography	81
Hash Functions	84
Digital Signatures	85
Certificates	86
Protecting Data at Rest, in Motion, and in Use	87
Protecting Data at Rest	87
Protecting Data in Motion	88
Protecting Data in Use	89
Summary	90
Review Questions	90
Project #6: Encrypting and Decrypting with PGP	91

PART II ARCHITECTURE, INFRASTRUCTURE, AND SYSTEM SECURITY

7		
SECURITY ARCHITECTURE		97
A City Planning Metaphor	98	
Structure, Patterns, and Intent	98	
Built-in vs. Bolted-on Security	98	
Foundational Architectural Principles	99	
Least Privilege	99	
Separation of Duties	100	
Secure Defaults	100	
Simplicity and Clarity	101	
Zero Trust	101	
Layered Design	102	
Trust Boundaries	102	
Defining Security Zones	103	
Designing with Boundaries in Mind	104	
Risk-Driven Architecture	105	
Risk Scoring	105	
Risk Tiers	106	
Threat Modeling	106	
Frameworks for Enterprise Security Architecture	107	
Summary	107	
Review Questions	108	
Project #7: Assessing a Real Security Architecture		108

8		
NETWORK SECURITY		111
Protecting Networks	112	
Designing Secure Networks	112	
Using Firewalls	113	
Implementing Network Intrusion Detection Systems	115	
Protecting Network Traffic	116	
Using Virtual Private Networks	116	
Protecting Data over Wireless Networks	117	
Using Secure Protocols	117	
Network Security Tools	118	
Wireless Protection Tools	118	
Scanners	119	
Packet Sniffers	119	
Honeypots	120	
Firewall Tools	121	
Summary	121	

Review Questions	122
Project #8: Experimenting with Honeytokens	122

9
OPERATING SYSTEM SECURITY **125**

Operating System Hardening	126
Removing All Unnecessary Software	126
Removing All Unessential Services	127
Altering Default Accounts	128
Limiting Privilege	129
Performing Updates	129
Turning On Logging and Auditing	130
Protecting Against Malware	130
Anti-Malware Tools	131
Executable Space Protection	131
Software Firewalls and Host Intrusion Detection	132
Operating System Security Tools	133
Scanners	133
Vulnerability Assessment Tools	134
Exploit Frameworks	135
Summary	137
Review Questions	137
Project #9: Scanning with Zenmap	138

10
MOBILE, EMBEDDED, AND INTERNET OF THINGS SECURITY **141**

Mobile Device Security	142
Protections	142
Security Issues	143
Embedded Device Security	145
Uses	146
Security Issues	147
Internet of Things Security	148
What Is an IoT Device?	148
Security Issues	150
Summary	152
Review Questions	152
Project #10: Auditing App Permissions	152

11
APPLICATION SECURITY **157**

Software Development Vulnerabilities	158
Buffer Overflows	159
Race Conditions	160

Input Validation Attacks	161
Authentication Attacks	162
Authorization Attacks	162
Cryptographic Attacks	163
Web Security	163
Client-Side Attacks	163
Server-Side Attacks	164
Database Security	166
Protocol Issues	167
Unauthenticated Access	168
Arbitrary Code Execution	168
Privilege Escalation	169
Application Security Tools	169
Sniffers	169
Web Application Analysis Tools	171
Fuzzers	172
Summary	173
Review Questions	174
Project #11: Linking CWEs with CVEs	174

12

AI SECURITY

177

Foundations of AI	177
What Is AI, Really?	178
AI vs. Machine Learning vs. Deep Learning	179
Large Language Models and Generative AI	180
AI Risk and Vulnerability	180
Input Manipulation and Model Behavior Exploits	181
Training and Model Integrity Risks	182
Data Leakage and Output-Handling Issues	183
Designing Safer AI Systems	184
Securing the AI Life Cycle	184
Making Models Understandable and Auditable	186
Understanding a Moving Target	187
Responsible AI Security Practices	187
Ethics and Policy	187
Bias and Fairness Risks	188
Transparency and Accountability	188
How AI Is Changing Security Operations	189
Summary	190
Review Questions	191
Project #12: Exploring Slaughterbots and Malicious AI	191

PART III SECURITY OPERATIONS AND MANAGEMENT

13 SECOPS, THE SOC, AND INCIDENT RESPONSE 195

The Role of the SecOps Team	196
Security Monitoring in the SOC	196
Choosing What to Monitor	196
Aggregating Logs in the SIEM	197
Designing Alerts	197
Engineering Detections	198
Tuning Alerts	199
Detecting Identity Misuse	199
The IAM Life Cycle	200
Signs of Identity Misuse	200
Incident Response	201
What Counts as an Incident?	201
The Incident Life Cycle	201
Summary	203
Review Questions	204
Project #13: Calculating Vulnerability Severity	204

14 GOVERNANCE, RISK, AND COMPLIANCE 209

Governance	210
Accountability Structures and the RACI Matrix	211
Governance Frameworks	211
The Risk Management Life Cycle	212
Identifying Assets	212
Identifying Threats	212
Assessing Vulnerabilities	213
Assessing Risks	214
Mitigating Risks	214
Compliance	215
Types of Compliance	216
US Government Compliance	217
Industry-Specific Compliance	218
International Regulatory Environments	220
Frameworks for Compliance	220
Modern Regulatory Challenges	222
Cloud Environments	222
AI	224
Cryptocurrency	225

Summary	225
Review Questions	226
Project #14: Creating a Cryptocurrency Compliance Plan	226

15
VULNERABILITY ASSESSMENTS AND PENETRATION TESTING 229

Vulnerability Assessments	229
Mapping and Discovery	230
Scanning	231
Overcoming Technological Challenges	232
Penetration Testing	233
The Penetration Testing Process	234
Types of Penetration Tests	235
Targets	236
Bug Bounty Programs	238
Technological Challenges	239
Does Testing Really Mean You’re Secure?	239
Is Your Testing Realistic?	240
Can You Detect Your Own Attacks?	241
Has Your Security Evolved?	242
Can You Afford to Fix Security Holes?	243
Summary	243
Review Questions	244
Project #15: Scanning a System for Vulnerabilities	244

PART IV
HUMAN FACTORS AND PROFESSIONAL DEVELOPMENT

16
SOCIAL ENGINEERING 249

Gathering Information for Social Engineering Attacks	250
Human Intelligence	250
Open Source Intelligence	250
Other Kinds of Intelligence	255
Types of Social Engineering Attacks	256
Pretexting	256
Phishing and Spear Phishing	256
Tailgating	257
Other Common Attacks	258
Preventing and Mitigating Social Engineering	260
Summary	261
Review Questions	261
Project #16: Designing Your Own Shodan	262

17	SECURITY AWARENESS	263
Mitigating User Risks	264	264
Password Hygiene	264	264
Social Engineering and Phishing Tactics	265	265
Safe Network Usage	265	265
Malware Avoidance	266	266
Physical Security and Clean Desk Policies	266	266
Designing a Security Awareness Program	266	266
Building Partnerships	266	266
Tailoring the Training	267	267
Communicating Regulations and Policy	268	268
Communicating Security Awareness	269	269
Instructor-Led Training	269	269
Computer-Based Training	269	269
Gamification, Incentives, and Engagement	270	270
Visuals and Messaging	270	270
Evaluating Training Effectiveness	271	271
Developing Effectiveness Metrics	271	271
Counting the Number of Incidents	272	272
Testing Users	273	273
Summary	273	273
Review Questions	274	274
Project #17: Exploring the 2023 MGM Resorts Attack	274	274

18	SO YOU WANT TO BE A SECURITY PROFESSIONAL	277
Three Paths into Security	277	277
The Experience-First Path	278	278
The Education-First Path	278	278
The Hybrid Path	279	279
Training and Certifications	280	280
Generalist vs. Specialist: Choosing Your Focus	281	281
The Generalist Approach	281	281
The Specialist Approach	282	282
The Middle Ground	282	282
Careers and Roles	282	282
Defenders	282	282
Offensive Security	283	283
Security Governance, Risk, and Compliance	283	283
Builders and Engineers	283	283
Soft Skills in Security	284	284
Writing	284	284
Communicating Verbally and Visually	285	285
Working Within Security Teams	286	286
Engaging Across Disciplines	286	286

Summary	286
Review Questions	287
Project #18: Knowing Your Audience.....	288

NOTES	289
--------------	------------

INDEX	297
--------------	------------