

TABLE OF CONTENTS

INTRODUCTION	IX	Cybersecurity Resources	50
		Frameworks	50
		Regulations	52
		Legislation	53
		Standards	53
		Benchmarks/Secure Configuration Guides	54
		Information Sources	54
PART 1		SUMMARY	55
SECURITY FUNDAMENTALS	1	KEY TERMS	56
MODULE 1		REVIEW QUESTIONS	57
INTRODUCTION TO SECURITY	3	CASE PROJECTS	61
What Is Information Security?	5		
Understanding Security	5		
Defining Information Security	5		
Who Are the Threat Actors?	7		
Script Kiddies	8		
Hacktivists	9		
State Actors	9		
Insiders	10		
Other Threat Actors	10		
Vulnerabilities and Attacks	11		
Vulnerabilities	11		
Attack Vectors	14		
Social Engineering Attacks	15		
Impacts of Attacks	21		
SUMMARY	22		
KEY TERMS	23		
REVIEW QUESTIONS	24		
CASE PROJECTS	30		
MODULE 2			
THREAT MANAGEMENT AND CYBERSECURITY RESOURCES	33		
Penetration Testing	34		
Defining Penetration Testing	34		
Why Conduct a Test?	35		
Who Should Perform the Test?	35		
Rules of Engagement	37		
Performing a Penetration Test	39		
Vulnerability Scanning	42		
What Is a Vulnerability Scan?	42		
Conducting a Vulnerability Scan	43		
Data Management Tools	47		
Threat Hunting	49		
		Cybersecurity Resources	50
		Frameworks	50
		Regulations	52
		Legislation	53
		Standards	53
		Benchmarks/Secure Configuration Guides	54
		Information Sources	54
		SUMMARY	55
		KEY TERMS	56
		REVIEW QUESTIONS	57
		CASE PROJECTS	61
		PART 2	
		ENDPOINT SECURITY	63
		MODULE 3	
		THREATS AND ATTACKS ON ENDPOINTS	65
		Attacks Using Malware	66
		Imprison	67
		Launch	69
		Snoop	73
		Deceive	75
		Evade	76
		Application Attacks	77
		Scripting	78
		Injection	78
		Request Forgery	80
		Replay	80
		Attacks on Software	81
		Adversarial Artificial Intelligence	
		Attacks	83
		What Are Artificial Intelligence (AI) and Machine Learning (ML)?	84
		Uses in Cybersecurity	84
		Risks in Using AI and ML in Cybersecurity	85
		SUMMARY	86
		KEY TERMS	88
		REVIEW QUESTIONS	88
		CASE PROJECTS	93

MODULE 4

ENDPOINT AND APPLICATION DEVELOPMENT SECURITY	95
Threat Intelligence Sources	96
Categories of Sources	97
Sources of Threat Intelligence	99
Securing Endpoint Computers	101
Confirm Boot Integrity	101
Protect Endpoints	103
Harden Endpoints	107
Creating and Deploying SecDevOps	112
Application Development Concepts	114
Secure Coding Techniques	115
Code Testing	115
SUMMARY	118
KEY TERMS	120
REVIEW QUESTIONS	120
CASE PROJECTS	125

MODULE 5

MOBILE, EMBEDDED, AND SPECIALIZED DEVICE SECURITY	127
Securing Mobile Devices	129
Introduction to Mobile Devices	129
Mobile Device Risks	134
Protecting Mobile Devices	136
Embedded Systems and Specialized Devices	140
Types of Devices	140
Security Issues	144
SUMMARY	145
KEY TERMS	147
REVIEW QUESTIONS	148
CASE PROJECTS	152

PART 3

CRYPTOGRAPHY	155
---------------------	------------

MODULE 6

BASIC CRYPTOGRAPHY	157
Defining Cryptography	158
What Is Cryptography?	158
Cryptography Use Cases	160
Limitations of Cryptography	162
Cryptographic Algorithms	164
Hash Algorithms	165
Symmetric Cryptographic Algorithms	166
Asymmetric Cryptographic Algorithms	168
Cryptographic Attacks and Defenses	172
Attacks on Cryptography	173
Quantum Cryptographic Defenses	174
Using Cryptography	175
Encryption through Software	175
Hardware Encryption	177
Blockchain	178
SUMMARY	180
KEY TERMS	181
REVIEW QUESTIONS	181
CASE PROJECTS	187

MODULE 7

PUBLIC KEY INFRASTRUCTURE AND CRYPTOGRAPHIC PROTOCOLS	191
Digital Certificates	192
Defining Digital Certificates	192
Managing Digital Certificates	194
Types of Digital Certificates	197
Public Key Infrastructure (PKI)	202
What Is Public Key Infrastructure (PKI)?	202
Trust Models	202
Managing PKI	204
Key Management	205

Cryptographic Protocols	207
Secure Sockets Layer (SSL)	208
Transport Layer Security (TLS)	208
Secure Shell (SSH)	208
Hypertext Transport Protocol Secure (HTTPS)	209
Secure/Multipurpose Internet Mail Extensions (S/MIME)	209
Secure Real-time Transport Protocol (SRTP)	209
IP Security (IPsec)	210
Weaknesses of Cryptographic Protocols	210
Implementing Cryptography	211
Key Strength	211
Secret Algorithms	212
Block Cipher Modes of Operation	212
Crypto Service Providers	213
SUMMARY	214
KEY TERMS	215
REVIEW QUESTIONS	216
CASE PROJECTS	220

PART 4

NETWORK SECURITY 223

MODULE 8

NETWORKING THREATS, ASSESSMENTS, AND DEFENSES 225

Attacks on Networks	226
Interception Attacks	227
Layer 2 Attacks	228
DNS Attacks	231
Distributed Denial of Service Attack	233
Malicious Coding and Scripting Attacks	234
Tools for Assessment and Defense	236
Network Reconnaissance and Discovery Tools	237
Linux File Manipulation Tools	238
Scripting Tools	238
Packet Capture and Replay Tools	238
Physical Security Controls	240
External Perimeter Defenses	240
Internal Physical Security Controls	243
Computer Hardware Security	245

SUMMARY	246
KEY TERMS	248
REVIEW QUESTIONS	248
CASE PROJECTS	252

MODULE 9

NETWORK SECURITY APPLIANCES AND TECHNOLOGIES 255

Security Appliances	256
Firewalls	257
Proxy Servers	261
Deception Instruments	261
Intrusion Detection and Prevention Systems	263
Network Hardware Security Modules	264
Configuration Management	265
Security Technologies	266
Access Technologies	266
Technologies for Monitoring and Managing	269
Design Technologies	272
SUMMARY	276
KEY TERMS	278
REVIEW QUESTIONS	279
CASE PROJECTS	282

MODULE 10

CLOUD AND VIRTUALIZATION SECURITY 285

Cloud Security	286
Introduction to Cloud Computing	286
Securing Cloud Computing	292
Virtualization Security	298
Defining Virtualization	298
Infrastructure as Code	300
Security Concerns for Virtual Environments	302

Secure Network Protocols	304
Simple Network Management Protocol (SNMP)	304
Domain Name System Security Extensions (DNSSEC)	304
File Transfer Protocol (FTP)	305
Secure Email Protocols	306
Lightweight Directory Access Protocol (LDAP)	306
Internet Protocol Version 6 (IPv6)	307
Use Cases	307
SUMMARY	308
KEY TERMS	310
REVIEW QUESTIONS	311
CASE PROJECTS	315

MODULE 11

WIRELESS NETWORK SECURITY	317
Wireless Attacks	319
Bluetooth Attacks	319
Near Field Communication (NFC) Attacks	321
Radio Frequency Identification (RFID) Attacks	322
Wireless Local Area Network Attacks	323
Vulnerabilities of WLAN Security	331
Wired Equivalent Privacy	331
Wi-Fi Protected Setup	332
MAC Address Filtering	332
Wi-Fi Protected Access (WPA)	333
Wireless Security Solutions	334
Wi-Fi Protected Access 2 (WPA2)	334
Wi-Fi Protected Access 3 (WPA3)	336
Additional Wireless Security Protections	336
Installation	337
Configuration	338
Specialized Systems Communications	339
Rogue AP System Detection	339
SUMMARY	340
KEY TERMS	342
REVIEW QUESTIONS	342
CASE PROJECTS	347

PART 5

ENTERPRISE SECURITY 351

MODULE 12

AUTHENTICATION	353
Types of Authentication Credentials	354
Something You Know: Passwords	355
Something You Have: Smartphone and Security Keys	361
Something You Are: Biometrics	364
Something You Do: Behavioral Biometrics	368
Authentication Solutions	369
Password Security	370
Secure Authentication Technologies	373
SUMMARY	378
KEY TERMS	379
REVIEW QUESTIONS	380
CASE PROJECTS	386

MODULE 13

INCIDENT PREPARATION, RESPONSE, AND INVESTIGATION	389
Incident Preparation	390
Reasons for Cybersecurity Incidents	391
Preparing for an Incident	397
Incident Response	400
Use SOAR Runbooks and Playbooks	401
Perform Containment	401
Make Configuration Changes	402
Incident Investigation	402
Data Sources	402
Digital Forensics	405
SUMMARY	413
KEY TERMS	415
REVIEW QUESTIONS	415
CASE PROJECTS	420

MODULE 14

CYBERSECURITY RESILIENCE 423

Business Continuity 424

Introduction to Business Continuity 424

Resilience Through Redundancy 427

Policies 436

Definition of a Policy 436

Types of Security Policies 437

SUMMARY 444

KEY TERMS 445

REVIEW QUESTIONS 446

CASE PROJECTS 451

MODULE 15

RISK MANAGEMENT AND DATA PRIVACY 453

Managing Risk 454

Defining Risk 455

Risk Types 456

Risk Analysis 457

Risk Management 461

Data Privacy 466

User Concerns 467

Data Breach Consequences 468

Data Types 468

Protecting Data 468

Data Destruction 470

SUMMARY 470

KEY TERMS 472

REVIEW QUESTIONS 473

CASE PROJECTS 476

APPENDICES A

COMPTIA SECURITY+ SY0-601 CERTIFICATION EXAM OBJECTIVES 479

APPENDICES B

TWO RIGHTS & A WRONG: ANSWERS 505

GLOSSARY 515

INDEX 543