

Contents

Introduction

xix

Lesson 1	Understanding Security Layers	1
	Introducing Core Security Principles	3
	Understanding Confidentiality	4
	Understanding Integrity	4
	Understanding Availability	5
	Understanding the Principle of Least Privilege	7
	Understanding Separation of Duties	9
	Understanding an Attack Surface	10
	Performing an Attack Surface Analysis	10
	Understanding Social Engineering	12
	Linking Cost with Security	13
	Understanding Physical Security as the First Line of Defense	14
	Understanding Site Security	14
	Understanding Computer Security	19
	Performing Threat Modeling	23
	Skill Summary	25
	Knowledge Assessment	27
	Multiple Choice	27
	Fill in the Blank	29
	Matching and Identification	29
	Build List	30
	Business Case Scenarios	30
	Scenario 1-1: Designing a Physical Security Solution	30
	Scenario 1-2: Securing a Mobile Device	30
	Scenario 1-3: Understanding Confidentiality, Integrity, and Availability	30
	Scenario 1-4: Managing Social Engineering	30
Lesson 2	Understanding Authentication, Authorization, and Accounting	33
	Starting Security with Authentication	35
	Configuring Multifactor Authentication	36
	Authentication Based on What a User Owns or Possesses	38
	Authentication Based on a User's Physical Traits	38
	Introducing RADIUS and TACACS+	39
	Running Programs as an Administrator	40
	Introducing Directory Services with Active Directory	41
	Understanding Domain Controllers	42

Understanding NTLM	43
Understanding Kerberos	44
Using Organizational Units	44
Understanding Objects	46
Using Groups	49
Understanding Web Server Authentication	52
Comparing Rights and Permissions	52
Understanding NTFS	54
Using NTFS Permissions	54
Understanding Effective NTFS Permissions	56
Understanding Inheritance	60
Copying and Moving Files	62
Using Folder and File Owners	62
Sharing Drives and Folders	64
Share a Folder	64
Understanding Special Shares and Administrative Shares	66
Introducing the Registry	67
Access Registry Permissions	70
Using Encryption to Protect Data	70
Types of Encryption	71
Introducing Public Key Infrastructure (PKI)	72
Encrypting Email	78
Encrypting Files with EFS	79
Encrypting Disks in Windows	82
Understanding IPsec	87
Encrypting with VPN Technology	89
Introducing Smart Cards	92
Set Up a Virtual TPM Smart Card Environment	93
Create a Certificate Template	93
Create a TPM Virtual Smart Card	94
Enroll for the Certificate on the TPM Virtual Smart Card	94
Configuring Biometrics, Windows Hello, and Microsoft Passport	95
Set Up Windows Hello Facial Recognition	96
Set Up Windows Hello Fingerprint Reader	96
Using Auditing to Complete the Security Picture	97
Audit Files and Folders	100
Skill Summary	101
Knowledge Assessment	105
Multiple Choice	105
Fill in the Blank	107

	Business Case Scenarios	108
	Scenario 2-1: Understanding Biometrics	108
	Scenario 2-2: Limiting Auditing	108
	Scenario 2-3: Assigning NTFS Permissions	108
	Scenario 2-4: Using EFS	108
Lesson 3	Understanding Security Policies	111
	Using Password Policies to Enhance Security	113
	Using Password Complexity to Make a Stronger Password	113
	Using Account Lockout to Prevent Hacking	114
	Examining Password Length	115
	Using Password History to Enforce Security	115
	Setting Time Between Password Changes	116
	Using Password Group Policies to Enforce Password Security	118
	Configuring and Applying Password Settings Objects	119
	Establishing Password Procedures	121
	Understanding Common Attack Methods	122
	Protecting Domain User Account Passwords	125
	Install Hyper-V and Isolated User Mode on Windows 10	126
	Enable Device Guard and Credential Guard	126
	Skill Summary	127
	Knowledge Assessment	129
	Multiple Choice	129
	Fill in the Blank	131
	Business Case Scenarios	131
	Scenario 3-1: Understanding Long Passwords	131
	Scenario 3-2: Using Keys and Passwords	132
	Scenario 3-3: Managing User Accounts	132
	Scenario 3-4: Configuring a Local Security Policy	132
Lesson 4	Understanding Network Security	133
	Using Dedicated Firewalls to Protect a Network	135
	Understanding the OSI Model	136
	Types of Hardware Firewalls and Their Characteristics	140
	Understanding When to Use a Hardware Firewall Instead of a Software Firewall	143
	Understanding Stateful Inspection and Stateless Inspection	145
	Using Isolation to Protect the Network	146
	Understanding VLANs	146
	Understanding Routing	148

Understanding Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS)	154
Understanding Honeypots	155
Understanding DMZ	156
Understanding NAT	159
Understanding VPN	160
Understanding Other VPN Protocols	162
Understanding Server and Domain Isolation	164
Protecting Data with Protocol Security	165
Understanding Tunneling	166
Understanding DNS Security Extensions (DNSSEC)	167
Understanding Protocol Spoofing	168
Understanding Network Sniffing	168
Understanding Common Attack Methods	170
Understanding Denial-of-Service (DoS) Attacks	173
Securing the Wireless Network	175
Understanding Service Set Identifier (SSID)	176
Understanding Keys	176
Understanding MAC Filters	178
Understanding the Advantages and Disadvantages of Specific Security Types	178
Skill Summary	179
Knowledge Assessment	182
Multiple Choice	182
Fill in the Blank	184
Business Case Scenarios	185
Scenario 4-1: Using Windows Firewall	185
Scenario 4-2: Using a Routing Table	185
Scenario 4-3: Using Ports	185
Scenario 4-4: Accessing and Configuring Wireless Settings	185

Lesson 5	Protecting the Server and Client	187
	Protecting the Client Computer	189
	Protecting Your Computer from Malware	189
	Configuring Windows Updates	196
	Understanding User Account Control (UAC)	200
	Using Windows Firewall	203
	Using Offline Files	207
	Locking Down a Client Computer	207
	Managing Client Security Using Windows Defender	208
	Remove a Quarantined Item	210
	Schedule a Windows Defender Scan	212

Protecting Your Email	213
Managing Spam	214
Email Spoofing	215
Relaying Email	216
Securing Internet Explorer	216
Understanding Cookies and Privacy Settings	216
Using Content Zones	219
Understanding Phishing and Pharming	222
Understanding Secure Sockets Layer (SSL) and Certificates	223
Configuring Microsoft Edge	223
Protecting Your Server	225
Separating Services	225
Using a Read-Only Domain Controller (RODC)	226
Hardening Servers	226
Understanding Secure Dynamic DNS	227
Using Security Baselines	227
Using Security Templates	228
Using Security Compliance Manager	232
Locking Down Devices to Run Only Trusted Applications	235
Access AppLocker	236
Create and Test an AppLocker Rule	238
Export the Local Policy	240
Import the Local Policy	240
Managing Windows Store Apps	241
Configuring the Windows Store	242
Implementing Windows Store Apps	244
Implementing Windows Store for Business	246
Skill Summary	248
Knowledge Assessment	251
Multiple Choice	251
Fill in the Blank	254
Business Case Scenarios	255
Scenario 5-1: Enforcing Physical Security	255
Scenario 5-2: Programming Backdoors	255
Scenario 5-3: Configuring a Windows Defender Quarantine	255
Scenario 5-4: Protecting Your Resources	255
Scenario 5-5: Reviewing Windows Updates	255
Appendix	
Answer Key	257
Lesson 1: Understanding Security Layers	258
Answers to Knowledge Assessment	258
Answers to Business Case Scenarios	259

Lesson 2: Understanding Authentication, Authorization, and Accounting	260
Answers to Knowledge Assessment	260
Answers to Business Case Scenarios	261
Lesson 3: Understanding Security Policies	263
Answers to Knowledge Assessment	263
Answers to Business Case Scenarios	264
Lesson 4: Understanding Network Security	266
Answers to Knowledge Assessment	266
Answers to Business Case Scenarios	267
Lesson 5: Protecting the Server and Client	270
Answers to Knowledge Assessment	270
Answers to Business Case Scenarios	271
<i>Index</i>	273