

Brief Contents

1	Understanding Security Layers	1
2	Authentication, Authorization, and Accounting	19
3	Understanding Security Policies	69
4	Understanding Network Security	87
5	Protecting the Server and Client	133
	Appendix A	163
	Index	165

Lesson 1: Understanding Security Layers 1

Objective Domain Matrix 1

Key Terms 1

Introducing Security 2

Understanding Confidentiality 2

Understanding Integrity 3

Understanding Availability 3

Defining Threats and Risk Management 3

Understanding the Principle of Least

Privilege 5

Understanding Attack Surface 6

Understanding Social Engineering 7

Linking Cost with Security 8

Looking at Physical Security as the First Line of Defense 8

Understanding Site Security 9

Understanding Computer Security 12

Skill Summary 15

Knowledge Assessment 16

Workplace Ready 18

Lesson 2: Authentication, Authorization, and Accounting 19

Objective Domain Matrix 19

Key Terms 19

Starting Security with Authentication 20

Authenticating with What You Know 21

Authenticating with What You Own or Possess 22

Authenticating with What You Are 22

Introducing RADIUS and TACACS+ 23

Using Run As 24

Introducing Directory Services with Active Directory 25

Looking at Domain Controllers 25

Introducing NTLM 26

Introducing Kerberos 26

Using Organizational Units 27

Looking at Objects 28

Using Groups 31

Looking at Web Server Authentication 33

Comparing Rights and Permissions 34

Looking at NTFS 35

Using NTFS Permissions 35

Looking at Effective NTFS Permissions 36

Copying and Moving Files 39

Using Folder and File Owners 39

Sharing Drives and Folders 40

Looking at Special and Administrative

Shares 42

Introducing the Registry 42

Using Encryption to Protect Data 44

Examining Types of Encryption 45

Introducing Public Key Infrastructure 47

Encrypting Email 51

Encrypting Files with EFS 51

Encrypting Disks in Windows 54

Introducing IPSec 57

Encrypting with VPN Technology 58

Using Auditing to Complete the Security Picture 60

Skill Summary 64

Knowledge Assessment 65

Workplace Ready 68

Lesson 3: Understanding Security Policies 69

Objective Domain Matrix 69

Key Terms 69

Using Password Policies to Enhance Security 69

Using Password Complexity to Make a Stronger Password 70

Using Account Lockout to Prevent Hacking 71

Looking at Password Length 71

Using Password History to Enforce Security 71

- Setting the Time between Password Changes 72
- Using Password Group Policies to Enforce Security 77
- Understanding Common Attack Methods 80

Skill Summary 82**Knowledge Assessment 83****Workplace Ready 86**

Lesson 4: Understanding Network Security 87

Objective Domain Matrix 87**Key Terms 87****Using Dedicated Firewalls to Protect a Network 88**

- Examining Hardware Firewalls and Their Characteristics 92
- Using Hardware Firewalls versus Software Firewalls 95
- Using Stateful versus Stateless Inspection 96

Controlling Access with Network Access Protection (NAP) 97

- Understanding the Purpose of NAP 97
- Looking at How NAP Works 98
- Examining the Requirements for NAP 100

Using Isolation to Protect the Network 101

- Understanding Virtual LANs 101
- Understanding Routing 102
- Looking at Intrusion Detection and Intrusion Prevention Systems 107
- Looking at Honeypots 108
- Looking at DMZs 109
- Understanding Network Address Translation (NAT) 111
- Understanding Virtual Private Networks (VPNs) 112
- Understanding Internet Protocol Security (IPsec) 113
- Using Other VPN Protocols 114
- Looking at Server and Domain Isolation 116

Protecting Data with Protocol Security 117

- Understanding Tunneling 118
- Using DNS Security Extensions (DNSSEC) 118
- Looking at Protocol Spoofing 119
- Utilizing Network Sniffing 120
- Understanding Common NETWORK Attack Methods 121

Securing Wireless Network 123

- Using Service Set Identifier (SSID) 124
- Understanding Keys 125
- Utilizing MAC Filters 126
- Considering Pros and Cons of Specific Security Types 126

Skill Summary 127**Knowledge Assessment 128****Workplace Ready 132**

Lesson 5: Protecting the Server and Client 133

Objective Domain Matrix 133**Key Terms 133****Protecting the Client Computer 134**

- Protecting Your Computer from Malware 134
- Utilizing Windows Updates 138
- Utilizing User Account Control 140
- Using Windows Firewall 143
- Using Offline Files 146
- Locking Down a Client Computer 147

Protecting Your Email 147

- Dealing with Spam 148
- Relaying Email 149

Securing Internet Explorer 149

- Looking at Cookies and Privacy Settings 149
- Examining Content Zones 152
- Phishing and Pharming 154

Protecting Your Server 155

- Placing the Server 155
- Hardening the Server 155
- Using Secure Dynamic DNS 157

Skill Summary 157**Knowledge Assessment 158****Workplace Ready 161**

Appendix A 163

Index 165