

# ExamLabs

**Security Fundamentals**

**Study Guide**

**Exam 98-367**

<b>1</b>	Understanding Security Layers	1
<b>2</b>	Understanding Authentication, Authorization, and Accounting	25
<b>3</b>	Understanding Security Policies	82
<b>4</b>	Understanding Network Security	99
<b>5</b>	Protecting the Server and Client	141

	Index	197
--	-------	-----

## Lesson 1: Understanding Security Layers 1

---

**Lesson Skill Matrix** 1

**Key Terms** 1

**Introducing Core Security Principles** 2

- Understanding Confidentiality 2
- Understanding Integrity 3
- Understanding Availability 3
- Understanding the Principle of Least Privilege 5
- Understanding Separation of Duties 6
- Understanding an Attack Surface 7
- Performing an Attack Surface Analysis 8
- Understanding Social Engineering 9
- Linking Cost with Security 10

**Understanding Physical Security as the First Line of Defense** 10

- Understanding Site Security 11
- Understanding Computer Security 14

**Performing Threat Modeling** 18

**Skill Summary** 20

**Knowledge Assessment** 21

**Business Case Scenarios** 23

**Workplace Ready** 24

## Lesson 2: Understanding Authentication, Authorization, and Accounting 25

---

**Lesson Skill Matrix** 25

**Key Terms** 25

**Starting Security with Authentication** 26

- Authentication Based on What a User Knows 27
- Authentication Based on What a User Owns or Possesses 28
- Authentication Based on a User's Physical Traits 28
- Introducing RADIUS and TACACS+ 29
- Running Programs as an Administrator 30

**Introducing Directory Services with Active Directory** 31

- Understanding Domain Controllers 31
- Understanding NTLM 32

- Understanding Kerberos 32
- Using Organizational Units 33
- Understanding Objects 34
- Using Groups 37
- Understanding Web Server Authentication 39

**Comparing Rights and Permissions** 40

**Understanding NTFS** 41

- Using NTFS Permissions 41
- Understanding Effective NTFS Permissions 42
- Copying and Moving Files 46
- Using Folder and File Owners 46

**Sharing Drives and Folders** 47

- Understanding Special Shares and Administrative Shares 49

**Introducing the Registry** 49

**Using Encryption to Protect Data** 51

- Types of Encryption 52
- Introducing Public Key Infrastructure (PKI) 54
- Encrypting Email 58
- Encrypting Files with EFS 59
- Encrypting Disks in Windows 61

**Understanding IPsec** 64

- Encrypting with VPN Technology 66

**Introducing Smart Cards** 69

**Configuring Biometrics, Windows Hello, and Microsoft Passport** 71

**Using Auditing to Complete the Security Picture** 73

**Skill Summary** 76

**Knowledge Assessment** 78

**Business Case Scenarios** 80

**Workplace Ready** 81

## Lesson 3: Understanding Security Policies 82

---

**Lesson Skill Matrix** 82

**Key Terms** 82

**Using Password Policies to Enhance Security** 83

- Using Password Complexity to Make a Stronger Password 83
- Using Account Lockout to Prevent Hacking 84
- Examining Password Length 85
- Using Password History to Enforce Security 85
- Setting Time Between Password Changes 85

Using Password Group Policies to Enforce Password Security	87
Configuring and Applying Password Settings Objects	88
Establishing Password Procedures	89
Understanding Common Attack Methods	89

## Protecting Domain User Account Passwords 92

### Skill Summary 94

### Knowledge Assessment 95

### Business Case Scenarios 97

### Workplace Ready 98

## Lesson 4: Understanding Network Security 99

### Lesson Skill Matrix 99

### Key Terms 99

### Using Dedicated Firewalls to Protect a Network 100

Understanding the OSI Model	101
Types of Hardware Firewalls and Their Characteristics	104
Understanding When to Use a Hardware Firewall Instead of a Software Firewall	107
Understanding Stateful Inspection and Stateless Inspection	108

### Using Isolation to Protect the Network 109

Understanding VLANs	109
Understanding Routing	110
Understanding Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS)	115
Understanding Honeypots	116
Understanding DMZ	117
Understanding NAT	119
Understanding VPN	121
Understanding Other VPN Protocols	122
Understanding Server and Domain Isolation	123

### Protecting Data with Protocol Security 125

Understanding Tunneling	125
Understanding DNS Security Extensions (DNSSEC)	126
Understanding Protocol Spoofing	127
Understanding Network Sniffing	127
Understanding Common Attack Methods	128

### Understanding Denial-of-Service (DoS) Attacks 131

### Securing the Wireless Network 132

Understanding Service Set Identifier (SSID)	133
Understanding Keys	133
Understanding MAC Filters	135
Understanding the Advantages and Disadvantages of Specific Security Types	135

### Skill Summary 136

### Knowledge Assessment 137

### Business Case Scenarios 139

### Workplace Ready 140

## Lesson 5: Protecting the Server and Client 141

### Lesson Skill Matrix 141

### Key Terms 141

### Protecting the Client Computer 142

Protecting Your Computer from Malware	142
Configuring Windows Updates	147
Understanding User Account Control (UAC)	151
Using Windows Firewall	153
Using Offline Files	156
Locking Down a Client Computer	157

### Managing Client Security Using Windows Defender 158

### Protecting Your Email 162

Managing Spam	162
Relaying Email	163

### Securing Internet Explorer 163

Understanding Cookies and Privacy Settings	163
Using Content Zones	166
Understanding Phishing and Pharming	168
Understanding Secure Sockets Layer (SSL) and Certificates	169

### Configuring Microsoft Edge 170

### Protecting Your Server 171

Separating Services	171
Using a Read-Only Domain Controller (RODC)	172
Hardening Servers	172
Understanding Secure Dynamic DNS	173

### Using Security Baselines 174

Using Security Templates	174
Using Security Compliance Manager	177

### Locking Down Devices to Run Only Trusted Applications 179

### Managing Windows Store Apps 184

Configuring the Windows Store	184
Implementing Windows Store Apps	185
Implementing Windows Store for Business	187

### Skill Summary 189

### Knowledge Assessment 191

### Business Case Scenarios 194

### Workplace Ready 195

### Index 197