Contents

Preface xi

Introduction xiii

Chapter 1. Fundamentals of Network Security 1

1.1. Introduction. 1
1.1.1. The main objectives of securing a network. 2
1.1.2. Information security terminology 2
1.2. Types of network security 4
1.2.1. Physical security 4
1.2.2. Logical security 4
1.2.3. Administrative security 5
1.3. The main risks related to the logical security of the network. 5
1.3.1. Different kinds of network attacks 5
1.3.2. Network security measures 7
1.3.3. Vulnerability audit measures 8
1.4. Exercises to test learning 8

Chapter 2. Securing Network Devices 15

2.1. Types of network traffic 15
2.2. Securing the management plan 16
2.3. Securing passwords 16
2.4. Implementing connection restrictions 17
2.4.1. Configuring a login banner 17
2.4.2. Configuring connection parameters 17
2.5. Securing access through console lines, VTY and auxiliaries 18
2.5.1. Securing access through the console line
and deactivating the auxiliary line 18
2.5.2. Securing VTY access with ssh 18

2.6. Allocation of administrative roles. 19
2.6.1. Privilege levels of the IOS system 19
2.6.2. Configuring a privilege level 19
2.6.3. Setting a privilege level per user 20
2.6.4. Setting a privilege level for console, VTY, and auxiliary line access. 20
2.6.5. Securing access with the management of "views" and "super-views" 21
2.6.6. Securing configuration files and the IOS system 22
2.6.7. Using automated security features 23
2.7. Securing the control plane 24
2.7.1. Introduction 24
2.7.2. MD5 authentication 24
2.7.3. Configuring OSPF protocol authentication. 24
2.7.4. Configuring EIGRP protocol authentication 25
2.7.5. Configuring RIP authentication 26
2.8. Exercises for application 26

Chapter 3. Supervising a Computer Network 41

3.1. Introduction. 41
3.2. Implementing an NTP server 42
3.2.1. Introduction to the NTP 42
3.2.2. How the NTP works 42
3.2.3. NTP configuration 43
3.3. Implementing a Syslog server 44
3.3.1. Introduction to the Syslog 44
3.3.2. How Syslog works 45
3.3.3. Configuring a Syslog client 46
3.4. Implementing the Simple Network Management Protocol (SNMP) . . 46
3.4.1. Introducing the SNMP 46
3.4.2. How SNMP works 47
3.4.3. SNMP configuration 49
3.5. Exercises for application 50

Chapter 4. Securing Access Using AAA 67

4.1. Introduction. 67
4.2. AAA authentication 68
4.2.1. Local AAA authentication 68
4.2.2. AAA authentication based on a server 69
4.3. AAA authorizations 71
4.4. AAA traceability. 71
4.5. Exercises for application 72

Chapter 5. Using Firewalls 79

5.1. Introducing firewalls 80
5.2. Types of firewalls 80
5.3. Setting up a firewall 80
5.4. Different firewall strategies 81
5.5. ACL-based firewalls 81
5.5.1. Introduction 81
5.5.2. The location of ACLs 81
5.5.3. IPv4 ACLs 81
5.5.4. IPv6 ACLs 82
5.5.5. ACL recommendation 83
5.6. Zone-based firewalls 84
5.6.1. Introduction 84
5.6.2. Types of security zones in a network 84
5.6.3. Rules applied to interzone traffic 85
5.6.4. Terminology 86
5.6.5. Configuring a ZFW 86
5.7. Creating zones 86
5.8. Creating Class-Maps 86
5.9. Creating the Policy-Map to apply the Class-Maps 87
5.10. Defining the zone pairs 87
5.11. Applying the policy maps to the zone pairs 87
5.12. Assigning interfaces to zones 87
5.13. Exercises for application 88

Chapter 6. Putting in Place an Intrusion Prevention System (IPS) . 101

6.1. Introduction to a detector 102
6.2. The differences between an IDS and an IPS 102
6.3. Types of IPS 103
6.4. Cisco IP solutions 103
6.5. Modes of deploying IPS 103
6.6. Types of alarms 104
6.7. Detecting malicious traffic 104
6.7.1. Modes of detection 104
6.7.2. Signature-based detection 104
6.7.3. Other modes of detecting malicious traffic 105
6.8. Signature micro-engines 106
6.9. Severity levels of the signatures 107
6.10. Monitoring and managing alarms and alerts 108
6.11. List of actions to be taken during an attack 108
6.12. Configuration of an IOS IPS 109
6.13. Recommended practices 111
6.14. Exercises for application 112

Chapter 7. Securing a Local Network 125

7.1. Introduction 125
7.2. Types of attacks on Layer 2 126
7.2.1. MAC address flooding attacks 126
7.2.2. MAC spoofing attack 127
7.2.3. The DHCP starvation attack 127
7.2.4. VLAN hopping attacks 128
7.2.5. STP-based attacks 130
7.3. The best security practices for protecting Layer 2 131
7.4. Exercises for application 132

Chapter 8. Cryptography 143

8.1. Basic concepts in cryptography 143
8.1.1. Definition 143
8.1.2. Terminology 144
8.2. The different classifications of cryptology 144
8.2.1. Traditional cryptography 145
8.2.2. Modern cryptography 146
8.2.3. Symmetric and asymmetric encryption 147
8.3. Key management 149
8.3.1. Introduction 149
8.3.2. Diffie-Hellman key exchange 149
8.4. Hash functions 151
8.5. HMAC codes 151
8.6. Asymmetric cryptography 151
8.6.1. Introduction 151
8.6.2. How it works 152
8.6.3. Digital signatures 153
8.6.4. Public key infrastructure 155
8.7. Exercises for application 159

Chapter 9. IPsec VPNs 173

9.1. The IPsec protocol 173
9.1.1. Objectives of IPsec 173
9.1.2. Basic IPsec protocols 174
9.1.3. The IPsec framework 174
9.1.4. The IPsec security association 175
9.1.5. IPsec modes 175
9.2. IKE protocol 176
9.2.1. Introduction 176
9.2.2. Components of IKE 176
9.2.3. IKE phases 176

9.3. The site-to-site VPN configuration 178
9.3.1. Introduction 178
9.3.2. Configuration of IPsec VPN 179
9.4. Exercises for application 181

Chapter 10. Studying Advanced Firewalls 189

10.1. Cisco ASA firewalls 189
10.1.1. Introduction 189
10.1.2. ASA models 190
10.1.3. Modes for using ASA devices. 190
10.1.4. An overview of ASA 5505 191
10.1.5. ASA levels of security 192
10.1.6. Configuring an ASA with CLI 193
10.2. Exercises for application 198
10.3. Configuring Cisco elements with graphical tools 210
10.3.1. An overview of the CCP 210
10.3.2. An overview of the ASDM 210
10.3.3. Using CCP and ASDM. 210
10.4. The TMG 2010 firewall. 211
10.4.1. Introduction 211
10.4.2. Installation and configuration 211

References 243

Index 245