14 13. 2884

Luminița SCRIPCARIU
Ion BOGDAN
Ștefan Victor NICOLAESCU
Cristina Gabriela CHEORGHE
Liana NICOLAESCU

SECURITATEA REȚELELOR DE COMUNICAȚII

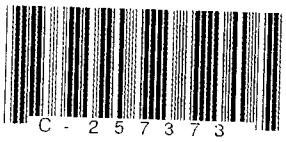


56

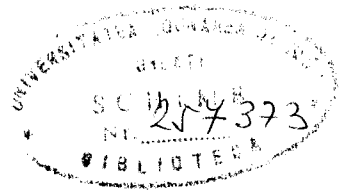
Casa de Editură
Venus
Iași 2008

III 19.988d1

Luminița SCRIPCARIU
Ion BOGDAN
Ștefan Victor NICOLAESCU
Cristina Gabriela CHEORGHE
Liana NICOLAESCU



SECURITATEA REȚELELOR DE COMUNICAȚII



Casa de Editură
Venus
Iași 2008

Luminița SCRIPCARIU, Ion BOGDAN, Ștefan Victor NICOLAESCU,
Cristina Gabriela CHEORGHE, Liana NICOLAESCU

SECURITATEA REȚELELOR DE COMUNICAȚII

Casa de Editură Venus, Iași, 2008

ISBN: 978-973-756-074-2

CUPRINS

CUVÂNT ÎNAINTE 5

Capitolul I INTRODUCERE 7
I.1 NOȚIUNI GENERALE DESPRE REȚELELE DE COMUNICAȚII 7
I.2 TIPURI DE REȚELE DE COMUNICAȚII 9
I.3 MODELAREA REȚELELOR DE CALCULATOARE 13
I.3.1 MODELUL DE REȚEA ISO/OSI 13
I.3.2 MODELUL TCP/IP 20
I.3.3 MODELUL CLIENT-SERVER 30
I.3.4 MODELUL PEER-TO-PEER 31
I.4 INTRODUCERE ÎN SECURITATEA REȚELELOR 33

Capitolul II PRINCIPII ALE SECURITĂȚII REȚELELOR 49
II.1 ASPECTE GENERALE 49
II.2 ANALIZA SECURITĂȚII REȚELEI 61
II.3 MODELE DE SECURITATE 63
II.4 SECURITATEA FIZICĂ 67
II.5 SECURITATEA LOGICĂ 69
II.5.1 SECURITATEA LOGICĂ A ACCESULUI 70
II.5.2 SECURITATEA LOGICĂ A SERVICIILOR 74
II.6 SECURITATEA INFORMAȚIILOR 77
II.6.1 CRIPTAREA CU CHEIE SECRETĂ 80
II.6.2 CRIPTAREA CU CHEIE PUBLICĂ 82
II.6.3 MANAGEMENTUL CHEILOR 84
II.7 INTEGRITATEA INFORMAȚIEI 86
II.7.1 TEHNICA HASH 87
II.7.2 SEMNĂTURA DIGITALĂ 91
II.7.3 CERTIFICATUL DIGITAL 94
II.7.4 MARCAREA 97
II.8 POLITICI DE SECURITATE 98

Capitolul III ATACURI ASUPRA REŢELELOR DE COMUNICAŢII 105
III.1 VULNERABILITĂŢI ALE REŢELELOR 105
III.2 TIPURI DE ATACURI 107
III.2.1 ATACURI LOCALE 108
III.2.2 ATACURI LA DISTANŢĂ 109
III.2.3 ATACURI PASIVE 113
III.2.4 ATACURI ACTIVE 114
III.3 ATACURI CRIPTOGRAFICE 120

Capitolul IV PROTOCOALE ŞI SERVERE DE SECURITATE. 125
IV.1 IPSEC 126
IV.1.1 PROTOCOLUL AH 132
IV.1.2 PROTOCOLUL ESP 133
IV.1.3 ASOCIAŢII DE SECURITATE 135
IV.1.4 APLICAŢII ALE IPSEC 136
IV.2 PROTOCOLUL KERBEROS 137
IV.3 PROTOCOLUL SESAME 140
IV.4 PROTOCOLUL RADIUS 144
IV.5 PROTOCOLUL DIAMETER 147
IV.6 PROTOCOLUL DE AUTENTIFICARE EXTINSĂ (EAP). 151

Capitolul V TEHNICI DE SECURITATE 155
V.1 INTRODUCERE 155
V.2 FIREWALL 158
V.3 SISTEME DE DETECŢIE A INTRUŞILOR 166
V.4 VPN REŢELE PRIVATE VIRTUALE 168

ABREVIERI 173

BIBIOGRAFIE 193