

Table des matières

Introduction	1
Chapitre 1. Mise en évidence de la sécurité	5
1.1. Introduction	5
1.2. Raisons d’être de la sécurité	6
1.2.1. Raisons techniques	6
1.2.2. Raisons sociales	8
1.3. Attaques de sécurité.	9
1.3.1. Classification passive/active des attaques.	10
1.3.2. Classification directe/indirecte des attaques	12
1.3.3. Exemples d’attaques	14
1.3.4. Quelques statistiques	16
1.4. Objectifs de la sécurité	17
1.4.1. Mise en place d’une culture	18
1.4.2. Mise en place des solutions techniques	18
1.5. Domaines de la sécurité	18
1.5.1. Sécurité énergétique	19
1.5.2. Sécurité organisationnelle et physique.	19
1.5.3. Sécurité logique	21
1.6. Normalisation de la sécurité.	23
1.6.1. Problématique et présentation générale	23
1.6.2. Norme ISO 7498-2	23

1.7. Services de sécurité	29
1.7.1. Authentification	30
1.7.2. Confidentialité	31
1.7.3. Intégrité	32
1.7.4. Non-répudiation	32
1.7.5. Traçabilité et contrôle d'accès	32
1.7.6. Disponibilité de service	32
1.8. Mécanismes de sécurité	32
1.8.1. Chiffrement	33
1.8.2. Contrôle d'intégrité	34
1.8.3. Contrôle d'accès	34
1.8.4. Signature numérique	35
1.8.5. Notarisation	35
1.9. Bonnes pratiques	35
1.10. Conclusion	36

Chapitre 2. Failles de sécurité 39

2.1. Introduction	39
2.2. Failles au niveau de TCP/IP	40
2.2.1. Arpanet, ancêtre d'Internet	40
2.2.2. Internet et problèmes de sécurité	40
2.2.3. Internet et facilité d'analyse	41
2.3. Failles dues aux <i>malwares</i> et outils d'intrusions	42
2.3.1. Virus	43
2.3.2. Ver (<i>worm</i>)	46
2.3.3. Spam	47
2.3.4. Bombe logique	48
2.3.5. Cheval de Troie	48
2.3.6. Espiociel (<i>spyware</i>)	50
2.3.7. <i>Keylogger</i>	51
2.3.8. <i>Adware</i>	51
2.3.9. Autres <i>malwares</i>	52
2.3.10. Comparaison entre quelques outils d'intrusion	52
2.4. Conclusion	53

Chapitre 3. Techniques et outils d'authentification	55
3.1. Introduction	55
3.2. Concepts théoriques de l'authentification	56
3.2.1. Identification	56
3.2.2. Authentification	57
3.3. Différents types d'authentification	57
3.3.1. Authentification à un service local	57
3.3.2. Authentification à travers le réseau	58
3.4. Service AAA	62
3.4.1. AAA en local	63
3.4.2. AAA sur serveur	65
3.5. Conclusion	70
Chapitre 4. Techniques de contrôle d'accès, ACL et <i>firewall</i>	71
4.1. Introduction	71
4.2. Liste de contrôle d'accès	72
4.2.1. Classifications des ACL	72
4.2.2. Configuration des ACL sous Cisco	74
4.2.3. Configuration des ACL sous Huawei	80
4.3. <i>Firewall</i>	85
4.3.1. Fonctionnalité de filtrage	86
4.3.2. Fonctionnalités de traçage et NAT	88
4.3.3. Architecture d'un <i>firewall</i>	89
4.3.4. Fonctionnement d'un <i>firewall</i>	91
4.3.5. Classifications des <i>firewalls</i>	92
4.3.6. <i>Firewall</i> à états	94
4.3.7. <i>Firewall</i> basé sur les zones	95
4.3.8. Exemples de <i>firewall</i>	98
4.4. Notion de DMZ	100
4.4.1. Définition et utilité	100
4.4.2. Topologies de mise en œuvre	101
4.5. Conclusion	104

Chapitre 5. Techniques et outils de détection d'intrusions . . .	105
5.1. Introduction	105
5.2. Antivirus	105
5.2.1. Fonctionnalités d'un antivirus	106
5.2.2. Méthodes de détection de virus	106
5.2.3. Manipulations possibles pour un antivirus	107
5.2.4. Composants d'un antivirus	107
5.2.5. Comparaison entre antivirus et <i>firewall</i>	108
5.3. Systèmes de détection d'intrusions	109
5.3.1. Fonctionnalités d'un IDS	109
5.3.2. Composants et fonctionnement d'un IDS	109
5.3.3. Classifications des IDS	111
5.3.4. Exemples d'IDS/IPS	114
5.4. Conclusion	115
Chapitre 6. Techniques et outils de chiffrement, IPSec et VPN	117
6.1. Introduction	117
6.2. Techniques de chiffrement	118
6.2.1. Principes de base du chiffrement	119
6.2.2. Cryptanalyse	120
6.2.3. Évolution de la cryptographie	121
6.2.4. Notion de certificat	126
6.2.5. Comparaison entre les techniques de chiffrement.	127
6.3. IPSec	128
6.3.1. AH	128
6.3.2. ESP	129
6.3.3. Différents modes IPSec	129
6.3.4. Différentes implémentations de l'IPSec	130
6.3.5. Différentes encapsulations IPSec	131
6.3.6. Protocole IKE	134
6.4. VPN	135
6.4.1. Problématique et raisons d'être	135
6.4.2. Principe du VPN	135
6.4.3. Différents types de VPN	136

6.4.4. Différents protocoles de tunnelisation	137
6.4.5. Configuration VPN IPSec <i>Site-to-Site</i>	137
6.5. Conclusion	140

Chapitre 7. Nouvelles tendances de sécurité pour SDN et IoT

143

7.1. Introduction	143
7.2. Sécurité du réseau SDN	144
7.2.1. Description générale du réseau SDN	144
7.2.2. Architecture du réseau SDN	145
7.2.3. Composants du réseau SDN	146
7.2.4. Problématiques de sécurité d'un réseau SDN	148
7.2.5. Solutions de sécurité d'un réseau SDN	149
7.3. Sécurité IoT/IoE	152
7.3.1. Réseaux de capteurs	152
7.3.2. Problématique de sécurité en IoT	153
7.3.3. <i>Blockchain</i> , solution de sécurité pour IoT	156
7.4. Conclusion	157

Chapitre 8. Management de la sécurité

159

8.1. Introduction	159
8.2. Audit sécurité	160
8.2.1. Objectifs	160
8.2.2. Diagramme d'action d'audit	161
8.2.3. Audit organisationnel et physique	162
8.2.4. Audit technique	163
8.2.5. Test intrusif	165
8.2.6. Méthodologies d'audit	165
8.3. Mise en évidence d'une politique de sécurité	167
8.3.1. Test et évaluation de sécurité	167
8.3.2. Développement d'une politique de sécurité	172
8.3.3. Composants d'une politique de sécurité	174
8.4. Normes, directives et procédures	175

8.4.1. Norme ISO 27000	176
8.4.2. Norme ISO/FDIS 31000	176
8.4.3. Norme ISO/IEC 38500	177
8.5. Conclusion	177
Liste des acronymes	179
Bibliographie.	181
Index	183