

République Algérienne Démocratique et Populaire
Ministère de l'Enseignement Supérieur et la Recherche
Scientifique
Centre de Recherche sur l'Information Scientifique et
Technique



Mémoire de fin d'étude pour l'obtention du diplôme
de Post-Graduation Spécialisée en Sécurité Informatique

Thème

La sécurité dans les réseaux Wi-Fi

• *Elaboré par:*

- YALAOUI Moussa.
- TAHRAOUI Mohamed Reda.

• *Encadré par:*

- Mr. Dr DERHAB Abdelouahid.

• *Devant le jury:*

Dr. TANDJAOUI Djamel

Président

Mr. KHELADI Lyes

Membre

Mr. BABAHOUYA Abdelaziz

Membre

-Janvier 2009 -

Remerciements

Nous remercions tout d'abord ALLAH, le tout puissant, pour nous avoir donné la santé et le courage pour finir ce modeste travail.

Nous remercions Mr. Dr Abdelouahid DERHAB, qui a encadré ce travail avec enthousiasme, et a su nous conseiller efficacement tout en nous accordant la liberté et la confiance d'agir.

Nous remercions aussi les membres de jury qui nous ont honorés par leur participation à l'évaluation de ce modeste travail.

Sans oublier de remercier tout le staff du CERIST (enseignements et responsables) en particulier le personnel du bureau formation.

Nous remercions chaudement nos familles et nos camarades.

Table de matière

Introduction générale	1
Chapitre 1 : Les réseaux sans fil Wi-Fi	3
Introduction	3
1- Une vue générale sur les réseaux	4
2- Une étude des différentes technologies sans fil	5
2.1 Les réseaux sans fil de type WPAN	6
2.2 Les réseaux sans fil de type WLAN (norme IEEE 802.11)	7
2.3 Les réseaux sans fil de type WMAN (norme IEEE 802.16)	8
2.4 Les réseaux sans fil de type WWAN	8
3- Une introduction aux réseaux sans fil WI-FI	9
3-1 Historique	9
3-2 Présentation du Wi-Fi	9
3.2.1 La norme 802.11	10
3.2.2 Les canaux de transmission de Wi-Fi	11
3-3 Utilisation du Wi-Fi	11
3-4 Architecture et fonctionnement du Wi-Fi	12
3.4.1 Fonctionnement du Wi-Fi	12
3-5 Les avantages du Wi-Fi	13
3-6 Les différentes normes de Wifi	14
3-7 La portées et le débits des différentes normes de IEEE 802.11	15
802.11a	16
802.11b	16
802.11g	17
4- Localisation et connexion a un réseau sans fil	17
4-1 Localisation d'un réseau Wi-Fi	17
4.1.1 Les signaux demande/réponses	17
4.1.2 La sonde	18
4-2 Connexion à un réseau sans fil	18
Conclusion	19
Chapitre 2 : La sécurité des réseaux IEEE 802.11b	20
Introduction	20
1. L'insécurité des réseaux sans fil	21
1.1. Réseau ouvert, réseau non sécurisé	21
1.2. Mécanismes de sécurité du 802.11b	21
1.2.1. Le SSID	21
1.2.2. Le WEP	22
1.2.3. Autres mécanismes de sécurisation non standardisés	24
1.2.3.1 Filtrage par MAC adresse	24
1.2.3.2 Base d'utilisateurs	25

1.3 Vulnérabilités lors de l'implémentation	25
2. Conclusion	25
Chapitre 3 : Les réseaux Wi-Fi : Attaques et contre mesures	26
Introduction	26
1- Evaluation générale des risques	27
1.1) Disponibilité	27
1.2) Intégrité	28
1.2.1 Intrusion	28
1.2.2 Usurpations d'identité	29
1.3) Confidentialité	30
1.4) Qualités des preuves techniques	31
2- Scan d'un réseau sans fil	31
2.1 Le scan actif	31
2.2 Le scan Passif	31
3. Les attaques	32
3.1 La dé-authentification	32
3.2 Cassage du filtrage MAC	33
3.3 Cassage de clé WEP	33
3.4 Une attaque Dictionnaire contre le WEP	35
3.5 Une attaque Statistique contre le WEP	35
3.6 L'attaque par injection: ChopChop	36
3.7 Fragmentation attaque	37
3.8 Décryptage d'un paquet chiffré avec le WEP sans connaître la clé	37
3.9 ROGUE APS	39
3.10 Déni de service RTS / CTS attaques	39
3.11 FakeAP	39
3.12 Attaque par intermédiaire (Man-in-the-Middle)	39
3.13 Le War-driving	39
4. Les contre-mesures	40
4.1 Des contre-mesures pour éviter la Dé-authentification	40
4.2 Des contre-mesures pour éviter le filtrage MAC	40
4.3 Se défendre contre les attaques visant le WEP	40
4.3.1 Le Cryptage WPA ou Wifi Protected Access	41
4.3.2 Le WPA2 / 802.11i	41
4.3.3 Les architectures WPA2	42
4.4 Se défendre contre les APs malhonnêtes	42
4.4.1 Le protocole EAP	42
5- Conclusion	43

Chapitre 4 : Des configurations sécurisé pour un réseau Wi-Fi	44
Introduction	44
1-La sécurité des Stations clientes	44
1.1 Les objectifs de sécurité d'une station cliente	45
1.1.1 Sécurité de l'accès au client	45
1.1.2 La sécurité des communications	45
1.1.2.1 SSL	46
1.1.2.2 SSH	48
1.2 Les journaux d'événement	48
1.3 Les mises à jour de sécurité	49
2- La sécurité du client sous Windows	49
2.1 Installation du client Windows	49
2.2 La protection du système d'exploitation	49
2.3 Protection antivirus	49
2.4 Pare-feu	50
2.5 ARP statique	50
2.6 Les journaux d'événement	50
3- La sécurité d'une station Linux	50
3.1 Installation du client Linux	50
3.2 La configuration du noyau	50
3.3 Configuration de la sécurité du noyau	51
3.4 Configuration de la carte	51
3.5 La protection du système d'exploitation	51
4- La sécurité des points d'accès	51
4.1 La mise en place d'un point d'accès	52
4.2 Généralités sur la sécurité des points d'accès	52
4.2.1 Le filtrage d'adresses MAC	52
4.2.2 Gestion des interfaces	53
4.2.3 Le journal d'événement de l'AP	53
4.2.4 La surveillance SNMP	53
4.2.5 Les méthodes d'authentification	54
4.2.4 Les trap hôte	54
5- La sécurité des passerelles	55
5.1 Le pare-feu	55
5.2 Architecture des Passerelles	55
5.3 L'installation sécurisée d'une passerelle	57
5.4 La création des Règles du pare-feu	57
5.5 Les journal d'audit	57
6- La pratique des solutions VPN sur les réseaux Wi-Fi	58
6.1 Quelques définitions	58
6.1.1 Différentiation de modes d'accès	58
6.1.2 Les éléments à prendre en compte	59
6.2 Démarche de mise en oeuvre de VPN	60
7. Conclusion	60

Conclusion générale
Annexe

62
64

BIBLIOTHEQUE DU CERIST