HACKUTT

WiFi

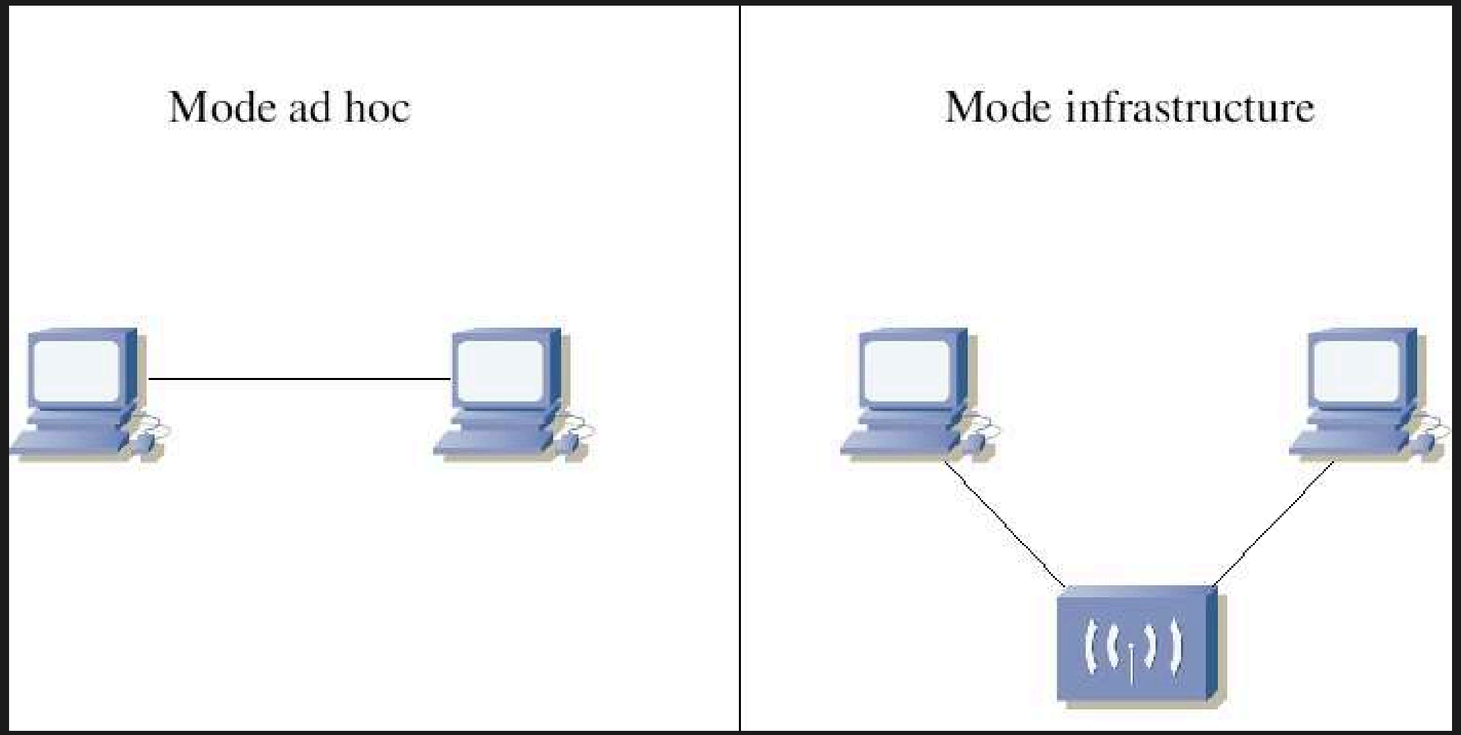
Arthur BIDET

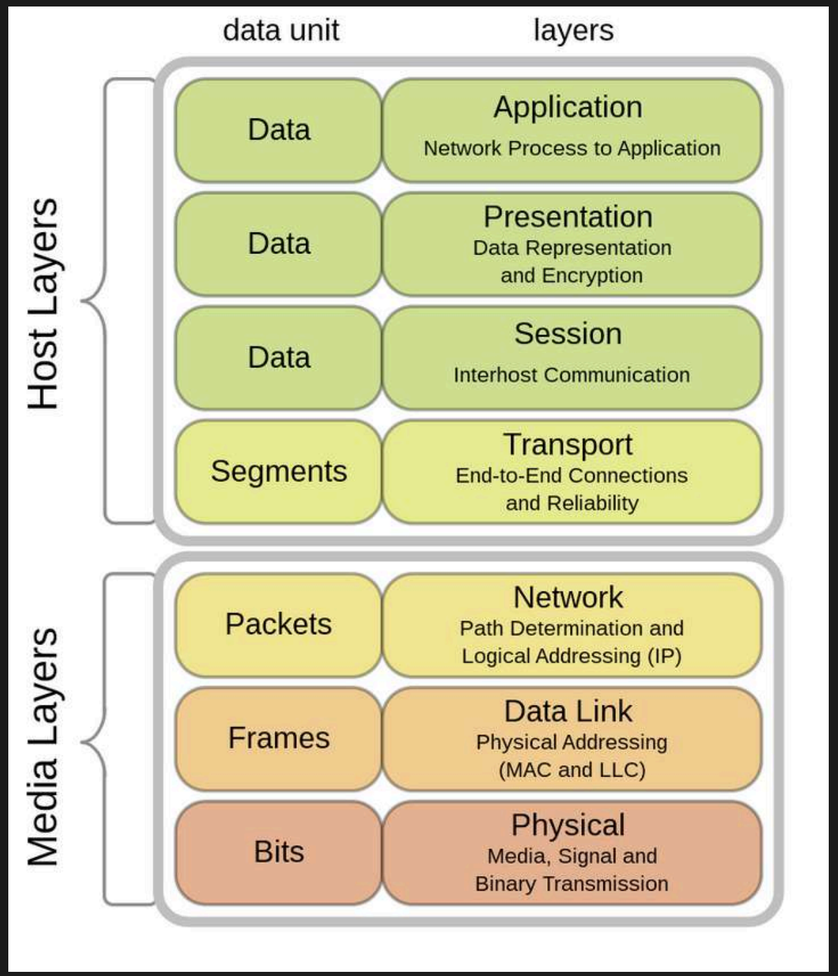
Lun. 8 Avril
2024

SOMMAIRE

LE WIFI ? C'EST QUOI ?

> Norme (802.11) qui concerne les couches 1 et 2 du modèle OSI

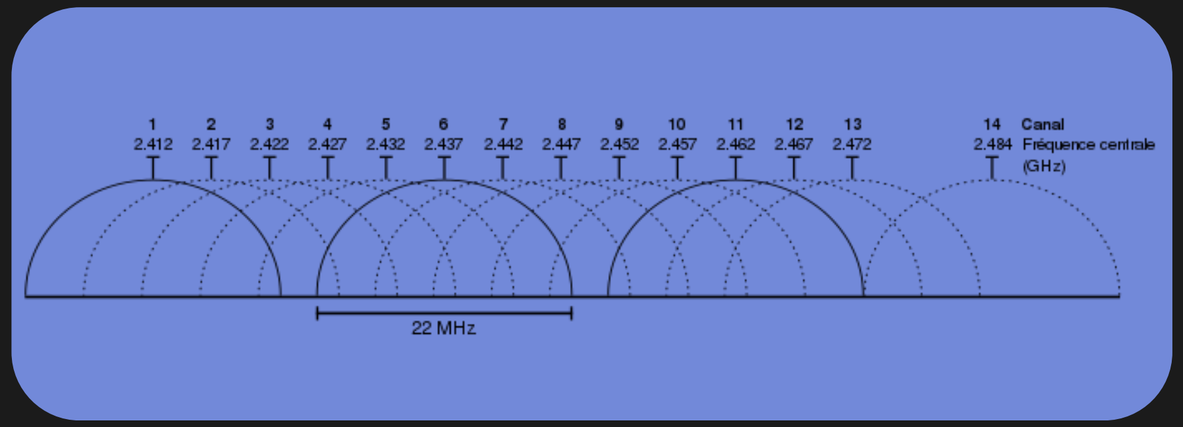




LE WIFI ? C'EST QUOI ?

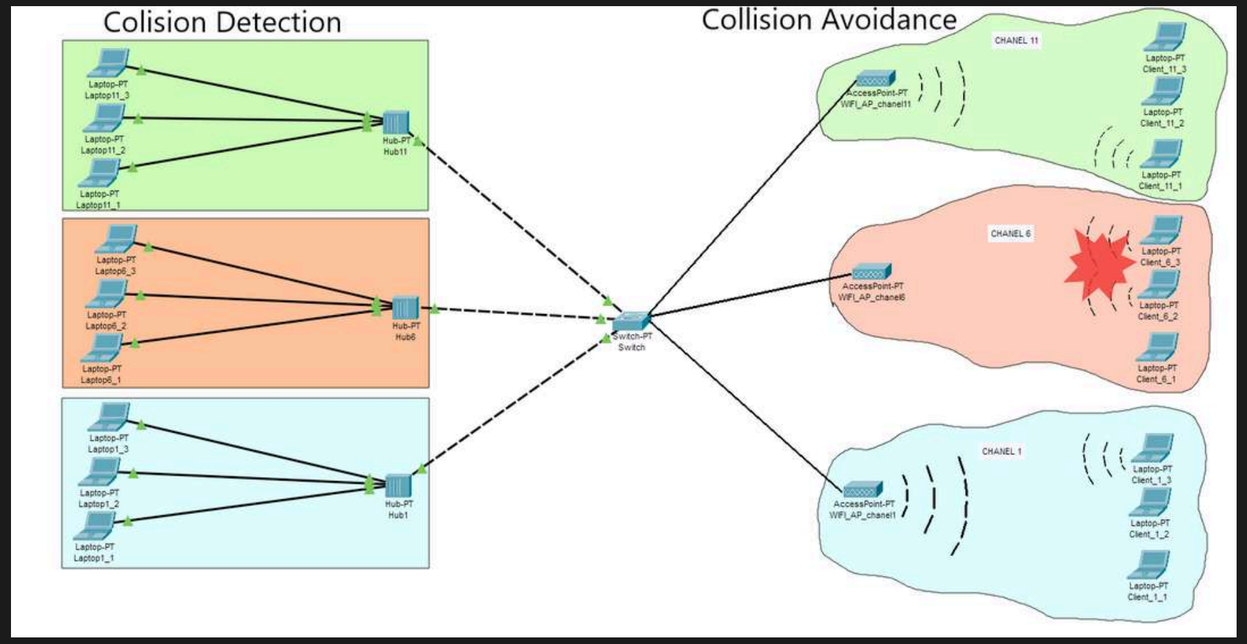
OFDM

> Technique de modulation où un signal est divisé en plusieurs sous-porteuses orthogonales.
> Les canaux représentent des bandes de fréquences sur lesquelles les appareils communiquent



CSMA/CA

> La méthode d'accès est CSMA/CA, il peut donc y avoir plusieurs clients sur le même canal. De même, il peut aussi y avoir plusieurs AP sur le même canal.



OBJECTIFS

Pourquoi ?

- Vol de données (mots de passe, information sensibles, ...)
- Contrôle (accès au réseau privé, ...)
- Multitude de motivations possibles

Les types d'attaques

- Les attaques de mots de passe
- Rogue Access Point (AP)
- Les attaques Man-in-the-Middle
- *Brouillage*
- *DoS*

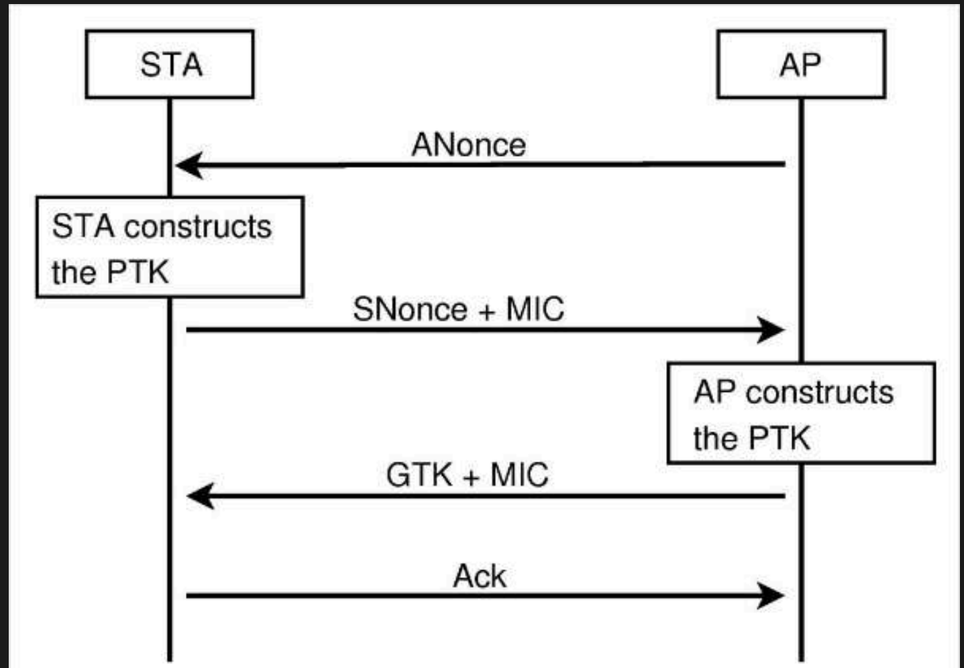
PARTIE 1 : WPA2
SON FONCTIONNEMENT

EAP

Un protocole de communication réseau : il est constitué d'un échange de trames dans un format spécifique à EAP pour réaliser l'authentification d'un partenaire

EAPOL

Une extention de EAP définie par IEEE 802 (WiFi)



The 4-way handshake WPA/WPA2 encryption protocol

After a couple of days that i am trying to understand the principles in the 4- way handshake between the client and the AP, i think i got...

Medium / Dec 13, 2021

DISCLAIMER POUR LES SCRIPTKIDDIES

- Les attaques doivent se faire sur des environnement contrôlés (votre réseau), comprenez vos actions
- Les attaques passives étant généralement indétectables, c’est votre devoir de filtrer les réseaux
- Un antécédent de cyberattaque ? dites au revoir aux employeurs

PARTIE 1 : WPA2
ATTAQUE SUR EAPOL

En sniffant le réseau, on peut capturer une communication WiFi entre des appareils. Si on capture un handshake EAPOL, on peut ensuite tenter de retrouver le mot de passe.

Pour cela, on utilisera des outils performants :

- hashcat (bruteforce des mots de passe)
- aircrack-ng (capture, configuration, attaque passive/active)
- hcxdumptool (capture, attaque passive)

Pour les versions récentes de hashcat, il est conseillé d'utiliser hcxdumptool :

https://www.notion.so/Wifi-d3eb7668fd2942d2bd1e7e7344053220?pvs=4#ec064df6c7024838b3d1fe96c690f0bb

PARTIE 1 : WPA2
ATTAQUE SUR PMKID

Cette attaque a été découverte accidentellement alors qu'elle cherchait de nouveaux moyens d'attaquer la nouvelle norme de sécurité WPA3.

Avantages

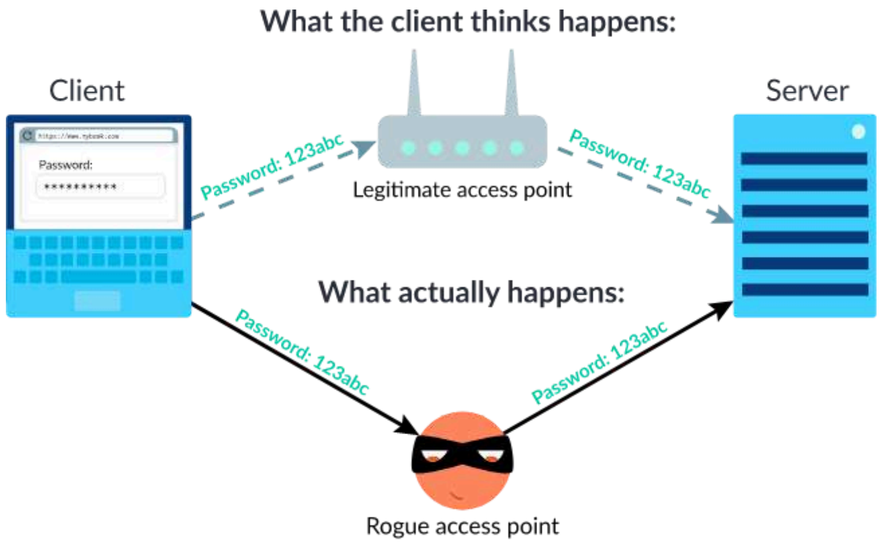
- Ne nécessite pas de 4-way handshake
- Ne nécessite pas de client connecté à l'AP

Méthode :
> Calculer des PMK candidats par bruteforce
> Calculer le PMKID correspondant et le comparer avec celui capturé

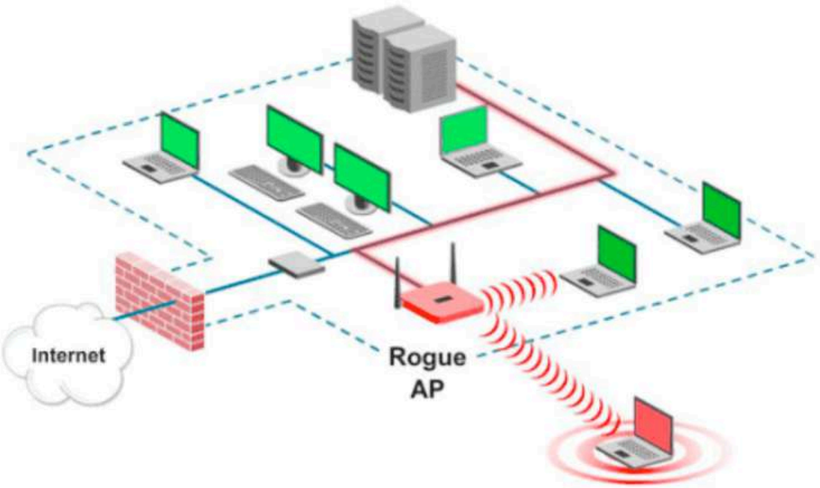
PMKID = HMAC-SHA1-128(PMK, "PMK Name" | MAC_AP | MAC_STA)
https://www.notion.so/Wifi-d3eb7668fd2942d2bd1e7e7344053220?pvs=4#7d86d440c5674b2180a220e0a540a570

PARTIE 2 : ROGUE AP MOTIVATIONS

MAN IN THE MIDDLE



POINT D'ENTRÉE



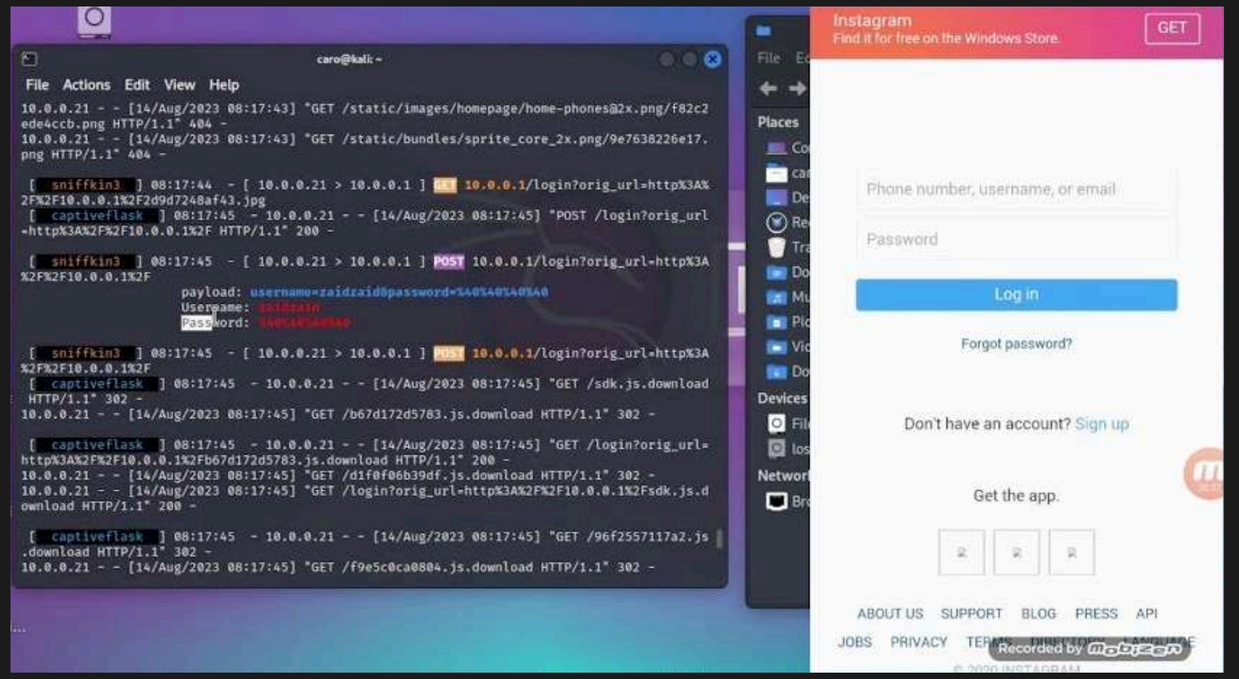
PARTIE 2 : ROGUE AP MITM-MÉTHODE

Principe

- Proposer un point d’accès WiFi avec un adaptateur réseau
- Transmettre les requettes vers un point d’accès internet
- Intercepter les pacquets

Les types d’attaques

- Interception des données
- Interception + social engeneering



PARTIE 2 : ROGUE AP WIFIPUMPKIN3

Dans cet exemple, nous allons utiliser Wifipumpkin3, un “Powerful framework for rogue access point attack”.

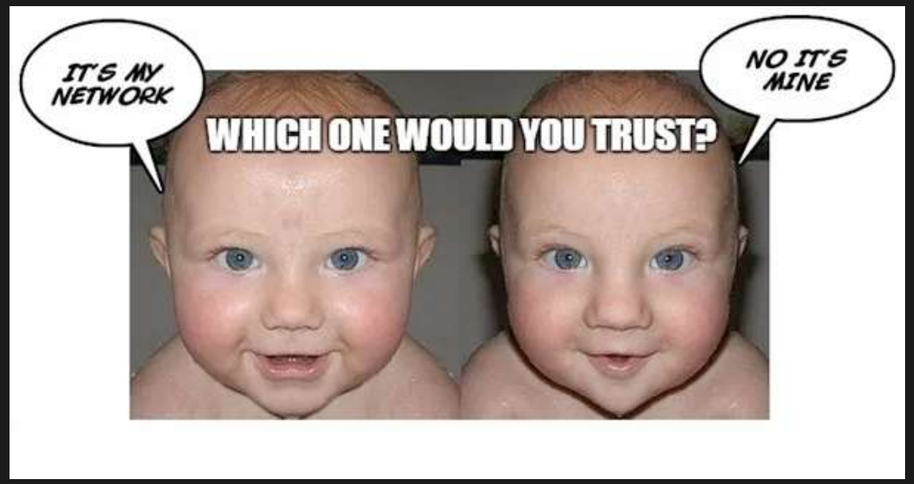
Un guide pour l’installation complet est disponible sur le Notion : https://www.notion.so/Wifi-d3eb7668fd2942d2bd1e7e7344053220?pvs=4#78ba5eba597a42d685841863d8e00fba

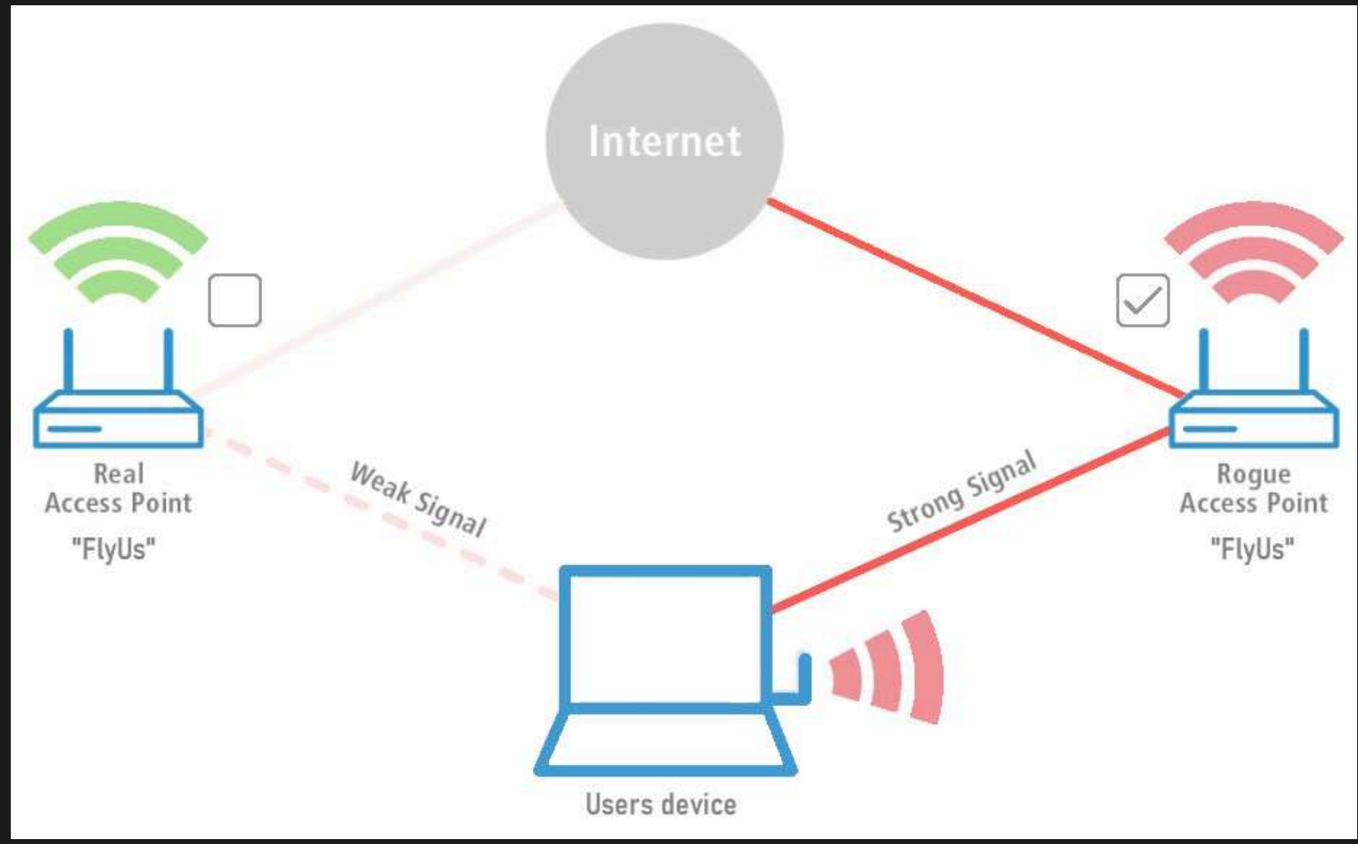
Cet outil automatise

- La création du point d’accès
- La configuration du proxy
- La translation d’adresse (NAT)
- La création du site de phishing

PARTIE 3 : EVIL TWIN AP PRINCIPES

An Evil Twin is a copy of a legitimate AP. It tries to hook clients to connect to the fake network to steal information, it is a kind of Rogue AP too.





PARTIE 3 : EVIL TWIN AP
PRINCIPES

Pourquoi ?

- Faire télécharger un virus à la victime
- Pour usurper la connexion de la victime et récolter des informations d'identification de médias sociaux, avec redirection DNS
- Pour rediriger toutes les personnes accédant à votre réseau vers une page de minage de crypto-monnaie
- **Pour l'inciter à vous donner le mot de passe wpa2 de son point d'accès**

PARTIE 3 : EVIL TWIN AP ATTAQUE

Méthode 1

- Utiliser un outil (Airgeddon)

Méthode 2

- Tout faire à la main 😎

Rappels

- mkdir nouveau_dossier #créer un dossier
- cd dossier #change directory
- sudo apt-get install package #installer un package
- ./executable.bin #executer un executable
- vi fichier.txt ; nano fichier.txt ; gedit fichier.txt #editer un fichier

https://www.notion.so/Wifi-d3eb7668fd2942d2bd1e7e7344053220?pvs=4#5da32383af34463db0efa8ab4f2baec5

THE END

Merci d'être venu !

RETROUVEZ TOUTE LA PARTIE TECHNIQUE SUR MON NOTION : HTTPS://WWW.NOTION.SO/WIFI-D3EB7668FD2942D2BD1E7E7344053220?PVS=4