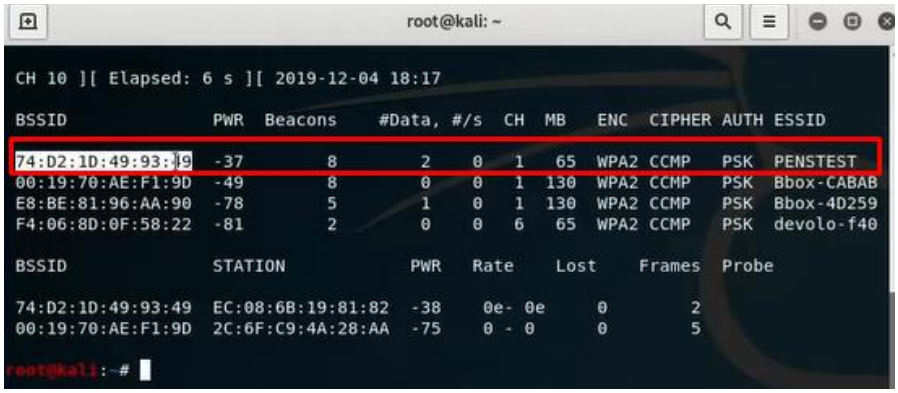
Airmon-ng check kill Pour kill tous les processus

Airmon-ng start walan0

Arodump-ng wlan0mon

Nous allons attaquer le wifi pentest



Avec la commande suivante on renseigne -c le chanel -b le bssid du point d'accès wifi

Il sera en écoute et avec la commande suivante nous allons donc déconnecter l'utilisateur avec l'adresse mac EC :08 :6B :19 :81 :82 pour l'obliger à se reconnecter et donc récupérer le handshake.

Au bout d'un certain temps lors de la reconnexion nous récupérons le handshake.

On lance ensuite le crack avec la commande suivante. On utilise le fichier rockyou.txt ce sera notre Word List elle est présente par default dans kali linux.

Al fin on trouve le mot de pas ou pas qui était dans la Word List vu que c'est une attaque par dictionnaire.