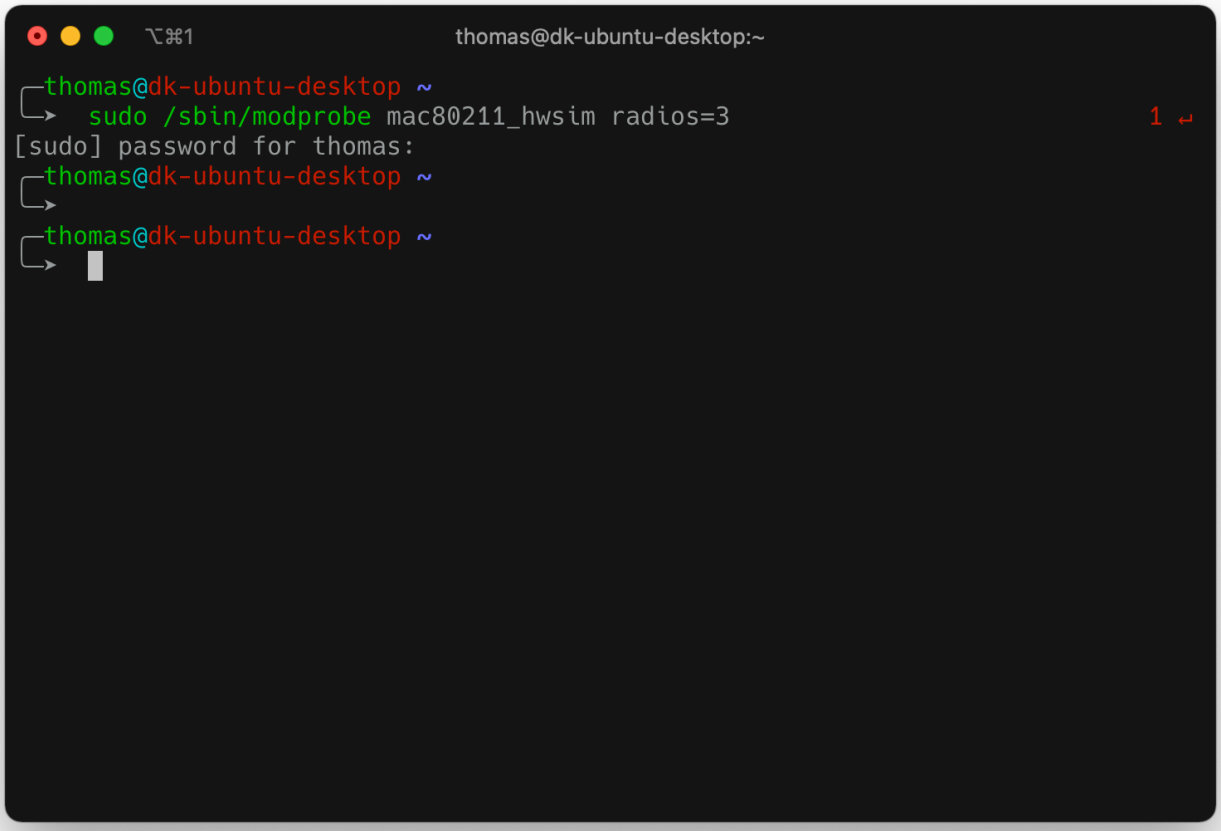
Thomas PEUGNET – Vincent LAGOGUÉ – David TEJEDA
M1 Réseaux et Sécurité – RS3

Cryptographie – Rendu TP03

Partie A

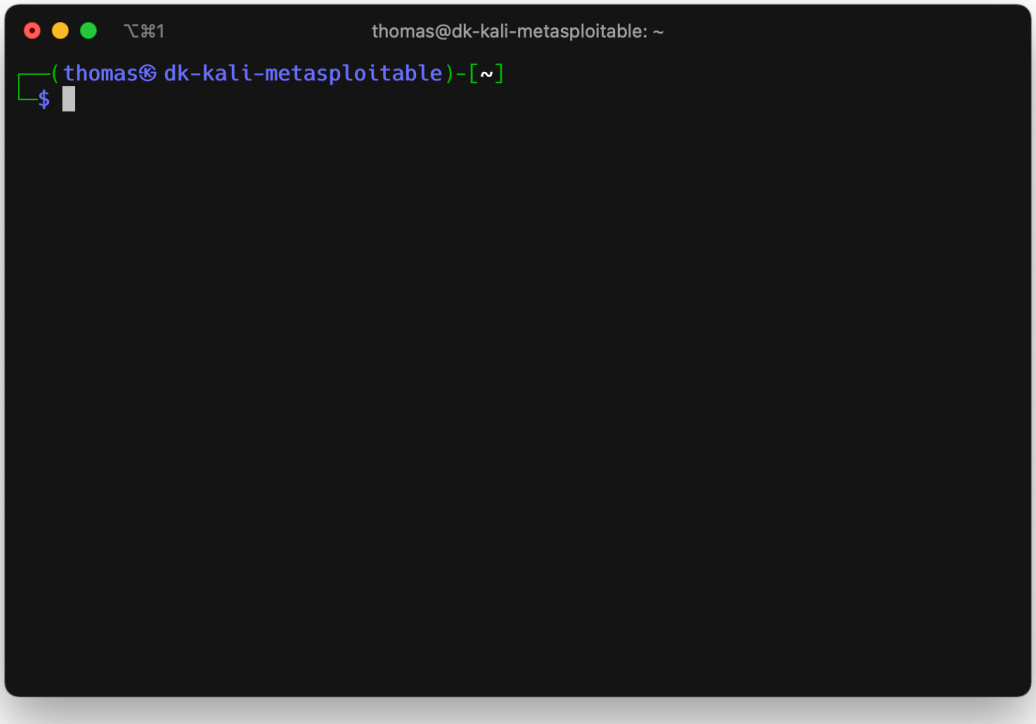
Question 1



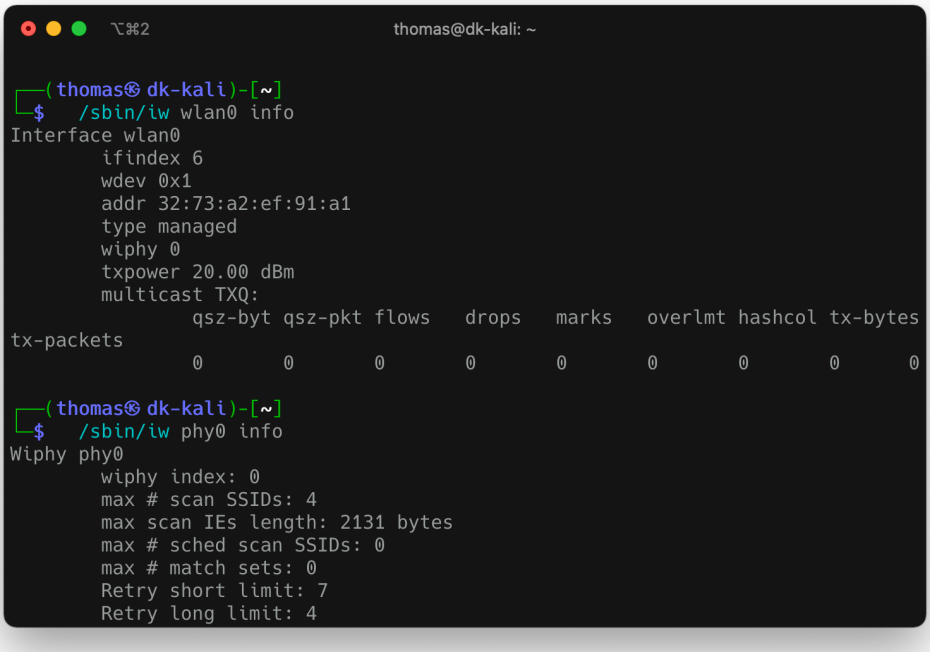
Le module a été correctement chargé.

Question 2

Problème rencontré : Ubuntu ne connaît pas la commande `/sbin/iw`. Nous effectuons donc un clone de notre VM sous Kali (debian based, contenant visiblement l'exécutable).



Une fois nos deux VMs mises à jour, nous avons le résultat suivant :



Nous pouvons noter que :

`Interface wlan0` : Nom de l'interface sans fil.

`ifindex 6` : Index d'interface, un numéro unique attribué à chaque interface réseau.

`wdev 0x1` : Identificateur de périphérique sans fil (wdev) pour cette interface.

`addr 32:73:a2:ef:91:a1` : Adresse MAC (Media Access Control) de l'interface wlan0.

`type managed` : Mode de fonctionnement de l'interface, "Managed" signifiant qu'elle se connecte à un point d'accès sans fil en tant que client.

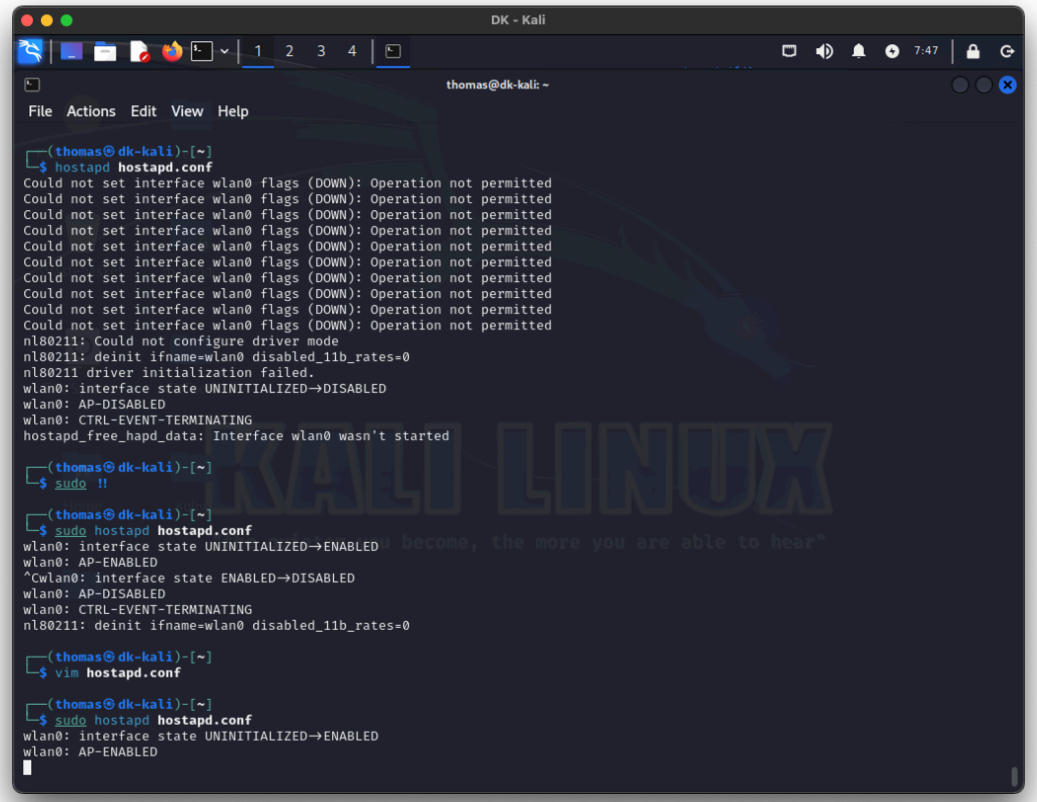
`wiphy 0` : Couche logicielle responsable des opérations sans fil, gérant cette interface.

`txpower 20.00 dBm` : Puissance de transmission de l'interface en décibels milliwatts (dBm), réglée à 20.00 dBm.

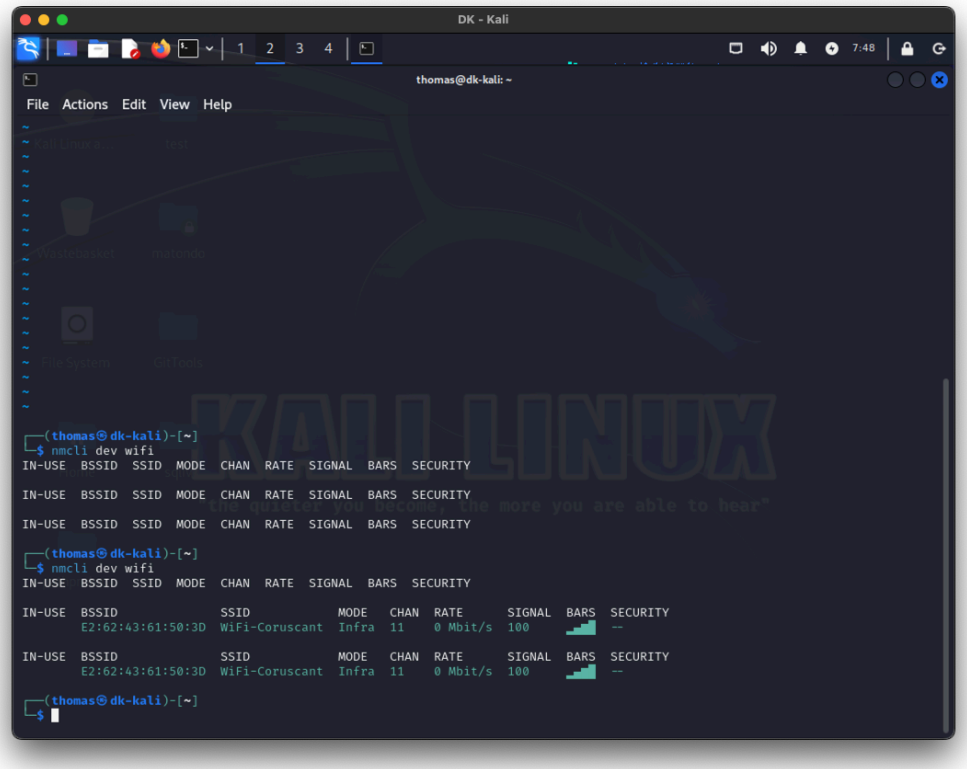
Note : Ces informations sont issues de la documentation de `/sbin/iw`.
Par ailleurs, la VM actuellement utilisée est sur un hyperviseur Proxmox. Le dongle Wifi installé n'est pas configuré en USB PassThrough. L'interface WLAN0 est donc actuellement en status `DOWN` (depuis la commande `ip addr`).

Question 3

Après avoir une configuration minimale sur un fichier nommé `hostapd.conf`, nous obtenons le résultat suivant :

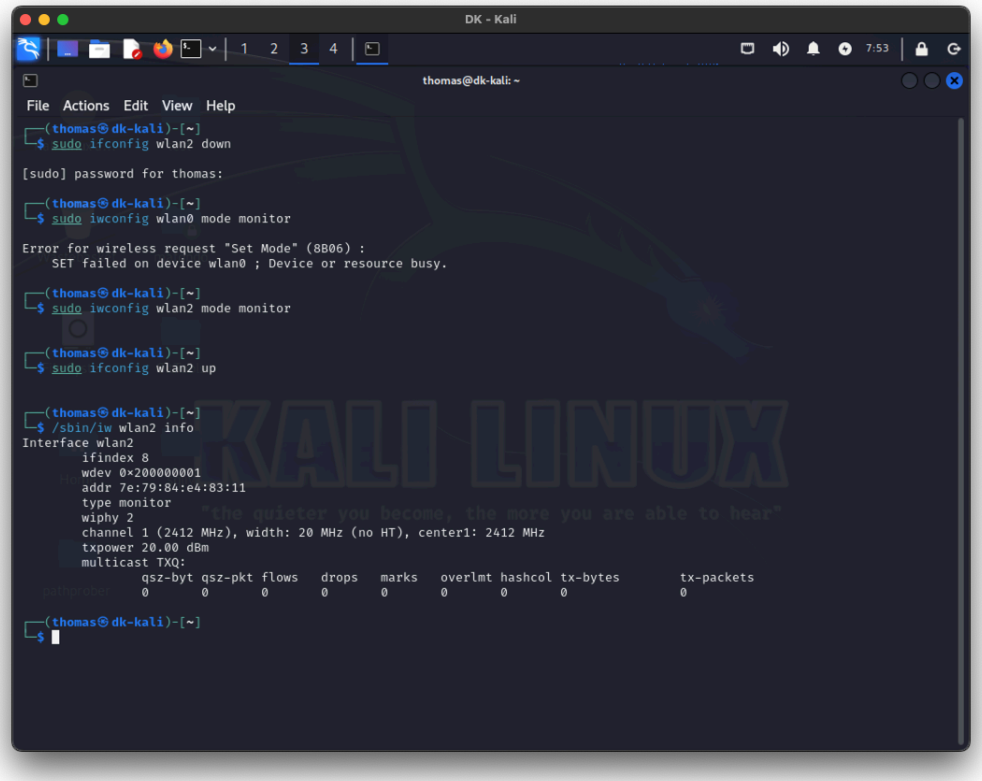


Le SSID de notre réseau apparaît bien.

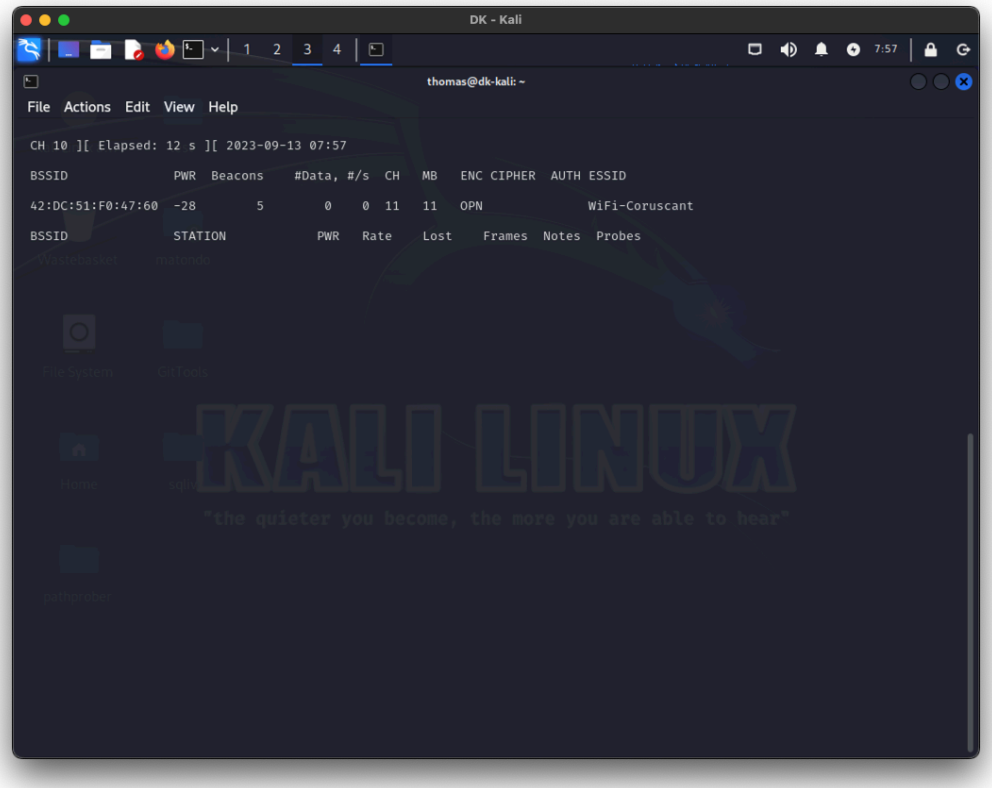


Question 4

Par l'intermédiaire de `iwconfig`, nous avons paramétré notre deuxième interface wifi en mode monitor. Statut vérifié par la commande `/sbin/iw wlan2 info`.

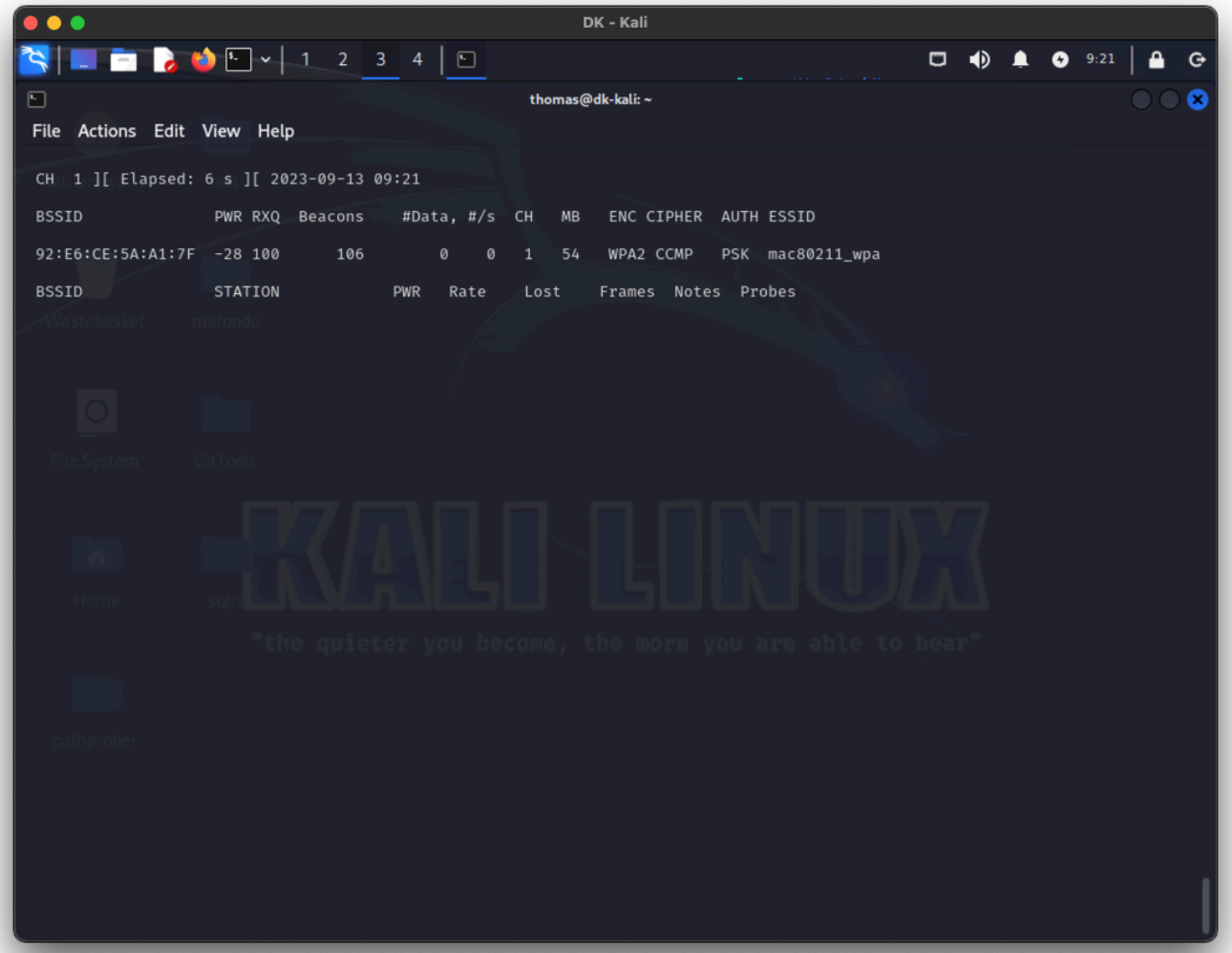


Après avoir lancé la commande `airodump-ng wlan2`, on obtient le résultat suivant, avec `WiFi-Coruscant` bien visible.



Question 5

Cette capture ci-dessus nous permet, dans un premier temps, de constater que notre réseau wifi n'est pas en WPA mais en Open. Nous changeons donc la configuration de hostapd.conf.



Voilà qui est mieux.

PWR : Cela représente la puissance du signal de chaque réseau Wi-Fi détecté. Plus le nombre est élevé, plus le signal est fort.

BEACONS : Il s'agit du nombre de balises de gestion (beacons) envoyées par le point d'accès. Les balises de gestion sont des paquets que les points d'accès envoient régulièrement pour annoncer leur présence et fournir des informations sur le réseau.

DATA : Cela représente le nombre de paquets de données qui ont été capturés depuis le point d'accès. Ces paquets contiennent généralement des données utiles transmises sur le réseau.

CH : Il s'agit du canal sur lequel le point d'accès fonctionne. Les réseaux sans fil peuvent utiliser différents canaux pour éviter les interférences.

MB : Cela indique la vitesse maximale de transmission des données prise en charge par le point d'accès, en mégabits par seconde (Mbps). Il peut s'agir de la vitesse de la norme Wi-Fi utilisée, comme 802.11n, 802.11ac, etc.

ENC : Cela indique si le réseau est chiffré ou non. Les valeurs courantes incluent "WEP" (Wired Equivalent Privacy), "WPA" (Wi-Fi Protected Access), "WPA2", etc.

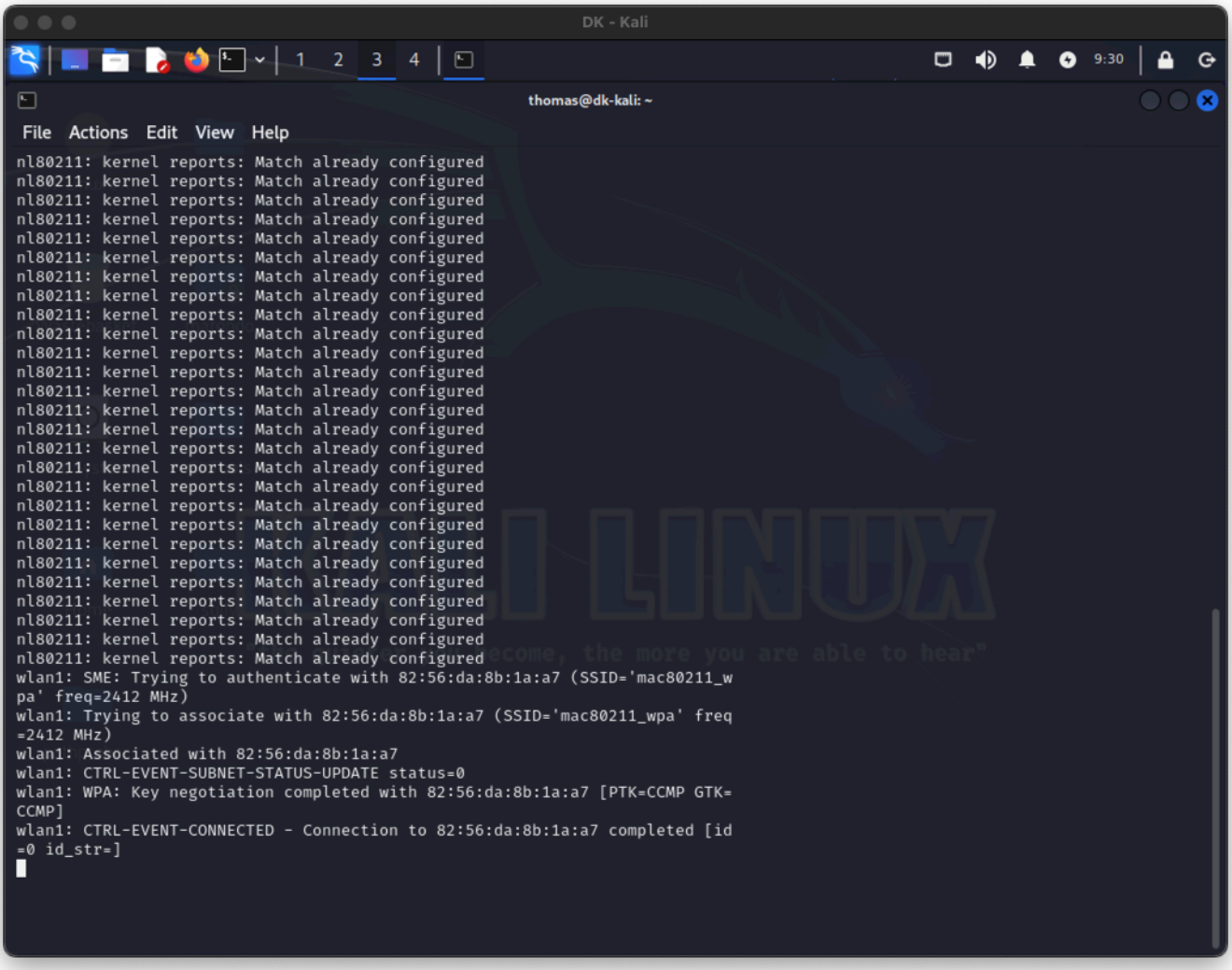
CIPHER : Cela spécifie l'algorithme de chiffrement utilisé pour sécuriser les communications sur le réseau, tel que "TKIP", "CCMP", etc.

AUTH : Cela indique le type d'authentification utilisé pour se connecter au réseau, tel que "PSK" (Pre-Shared Key) pour un mot de passe partagé ou "EAP" (Extensible Authentication Protocol) pour une authentification plus complexe.

ESSID : Il s'agit du nom du réseau sans fil (SSID) tel qu'il est diffusé. C'est le nom que vous voyez lorsque vous recherchez des réseaux Wi-Fi disponibles.

Question 6

On a bien le 4 ways handshake.



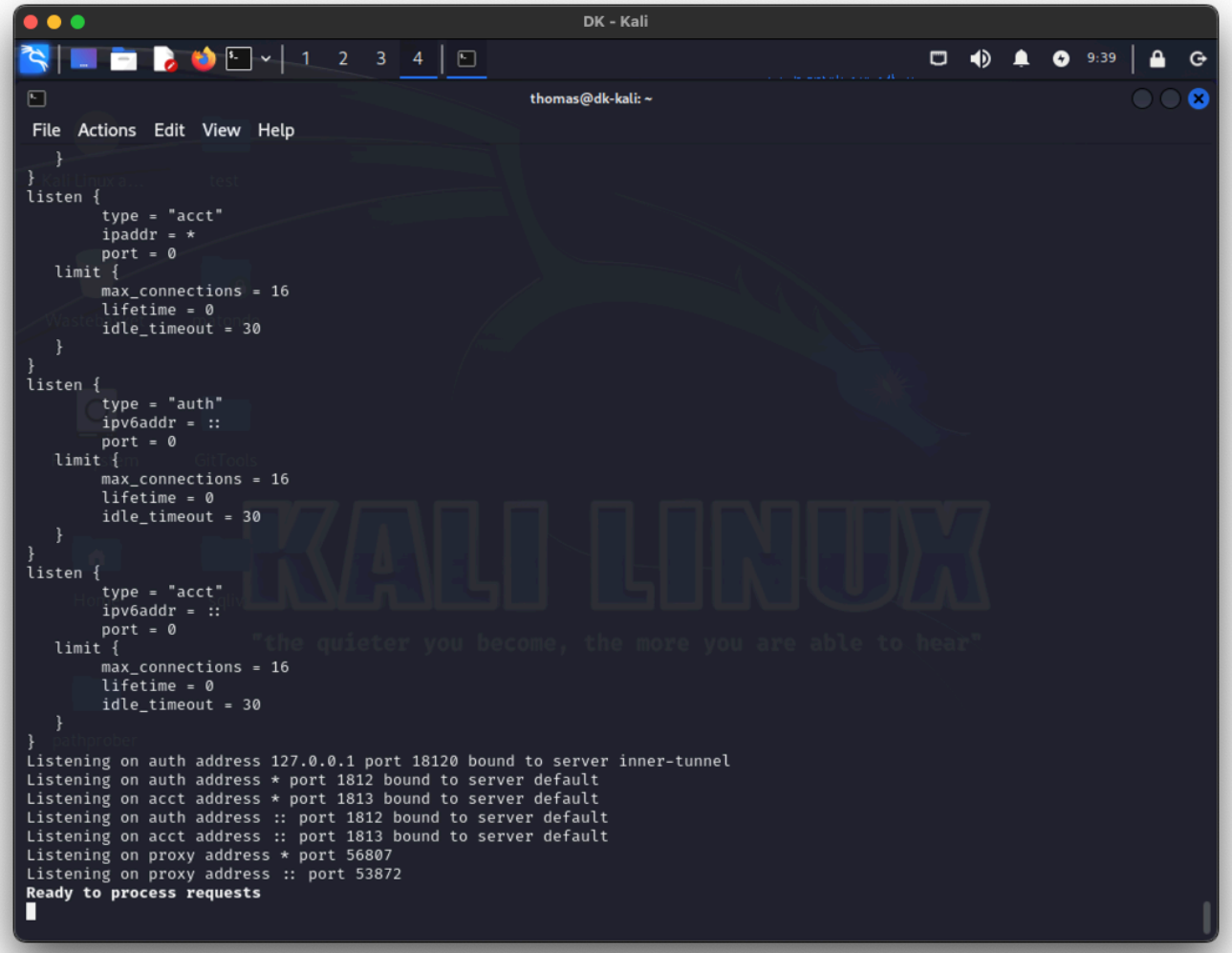
Question 7

Question 8

Partie B

Question 1

On a bien “Ready to process requests”.



Le serveur écoute sur le port `18120`. L’utilisateur qui lance le serveur est `freerad`. On peut confirmer cette observation en utilisant la commande `ps`. Il est actuellement en correctement en fonction.

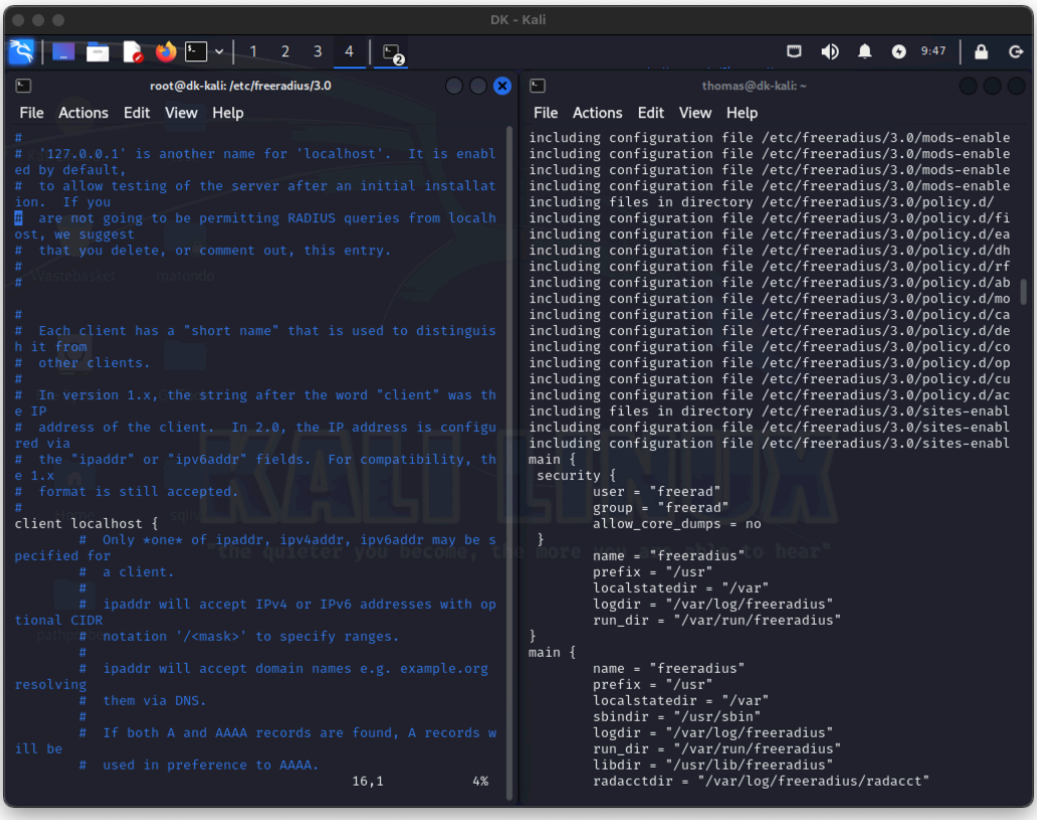
Question 2

C'est dans ce fichier que l'on déclare les différents clients (switchs par exemple) qui vont pouvoir requêter le serveur freeradius.

Le paramètre `testing123` est le mot de passe par défaut du serveur freeradius permettant de s'authentifier.

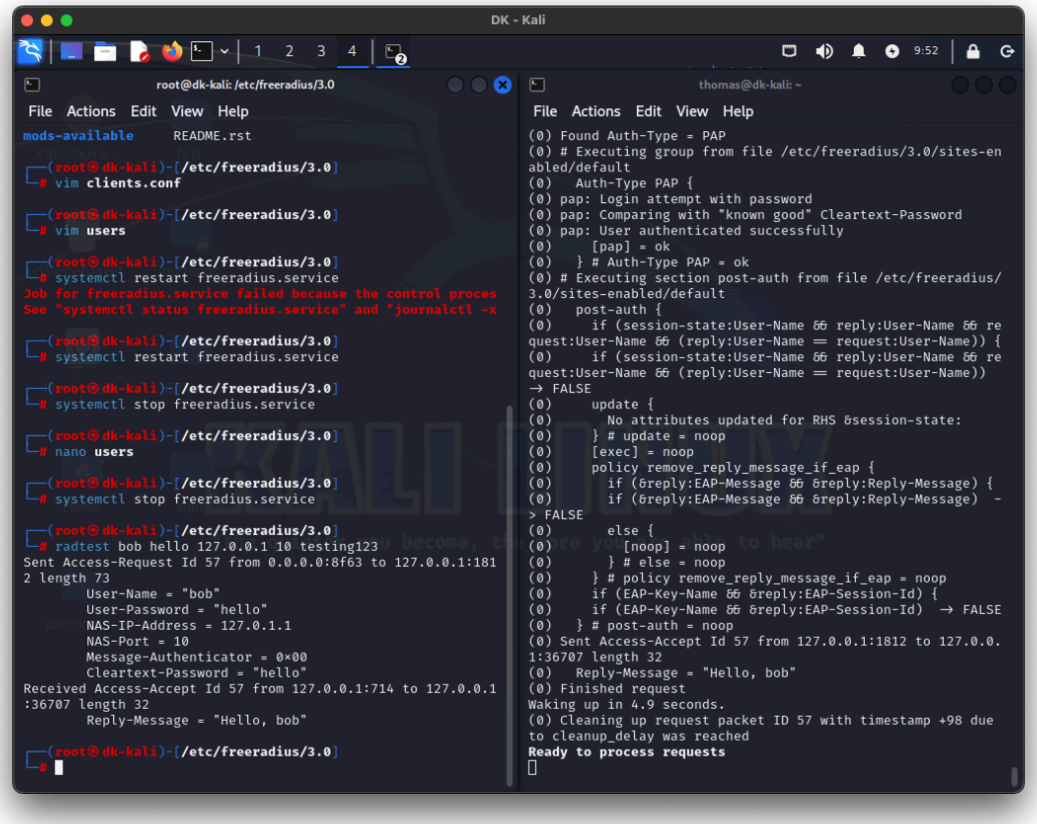
Les différents clients s'authentifient au serveur par l'intermédiaire d'un objet `client{}` créé dans le fichier `clients.conf`. Cet objet contient le nom du client, son secret et son IP. Si son IP n'est pas définie, la connexion sera refusée.

Le client `localhost` existe bel et bien.

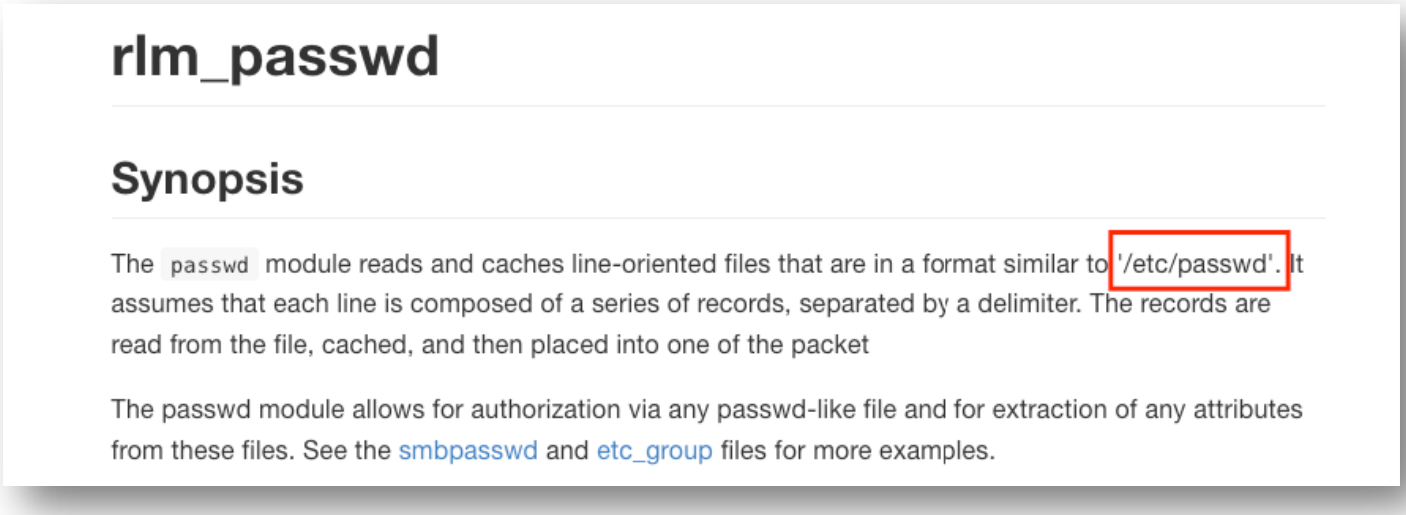


Question 3

On vient de se connecter avec l'utilisateur `bob` avec le serveur `freeradius` en mode debug.



D'après la documentation, il est possible d'utiliser un fichier avec un module ayant une syntaxe similaire à celle de `/etc/passwd`. Il ne semble donc pas possible d'utiliser directement le fichier en tant que tel.



rlm_passwd

Synopsis

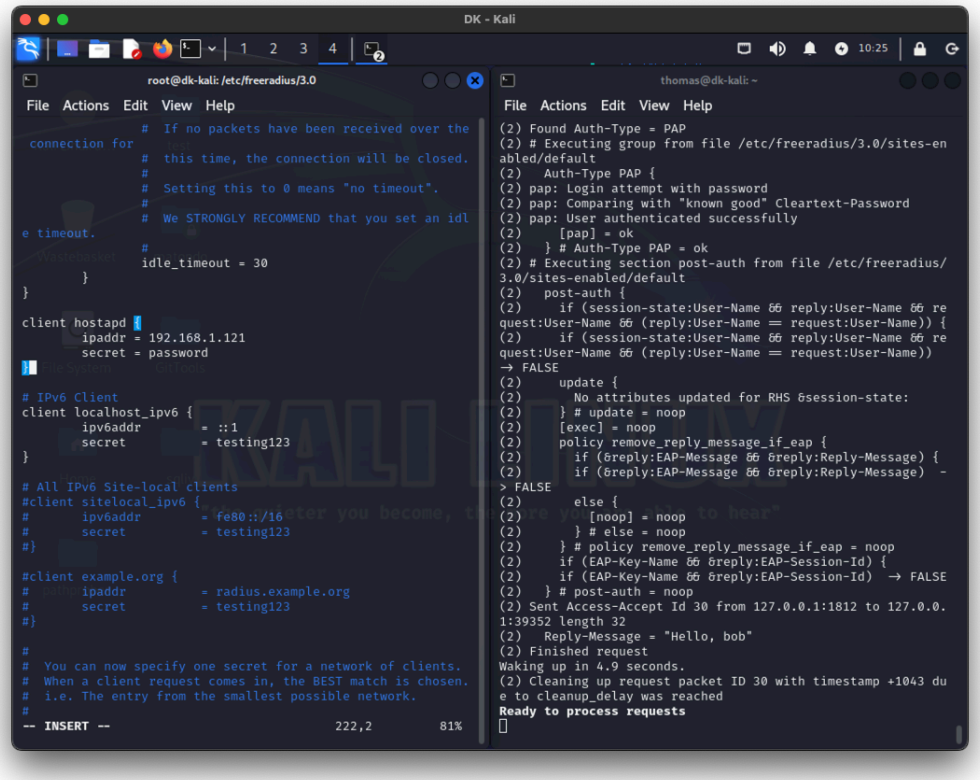
The `passwd` module reads and caches line-oriented files that are in a format similar to '/etc/passwd'. It assumes that each line is composed of a series of records, separated by a delimiter. The records are read from the file, cached, and then placed into one of the packet

The passwd module allows for authorization via any passwd-like file and for extraction of any attributes from these files. See the smbpasswd and etc_group files for more examples.

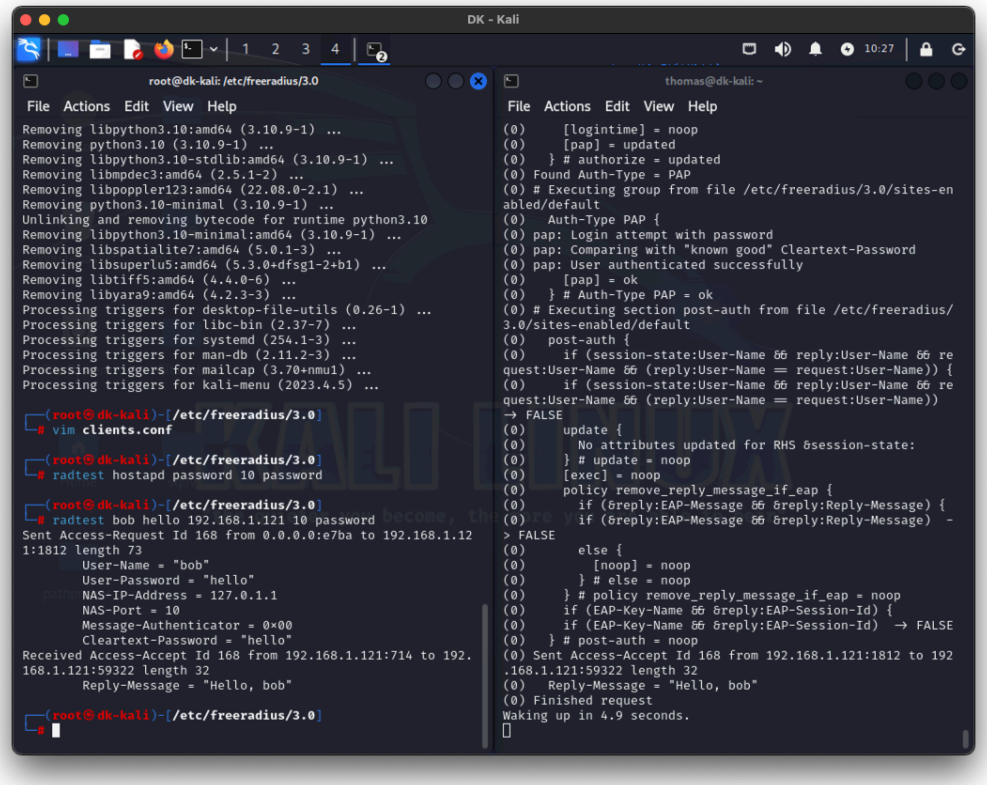
Question 4

Ajoutons un nouveau client, permettant de se connecter depuis ce dernier au lieu de localhost.

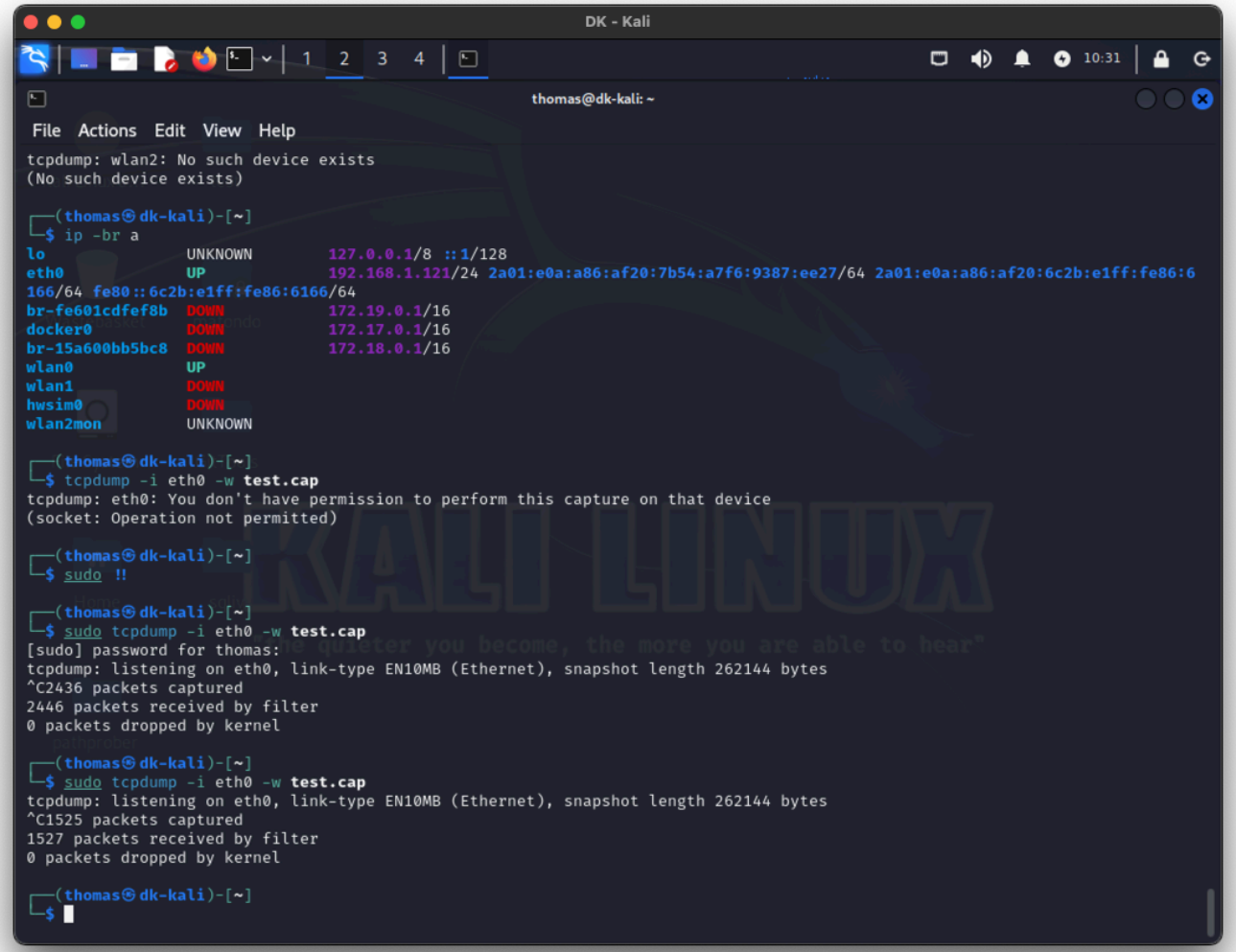
Notre nouveau client ci-dessous.



Le résultat, succès.



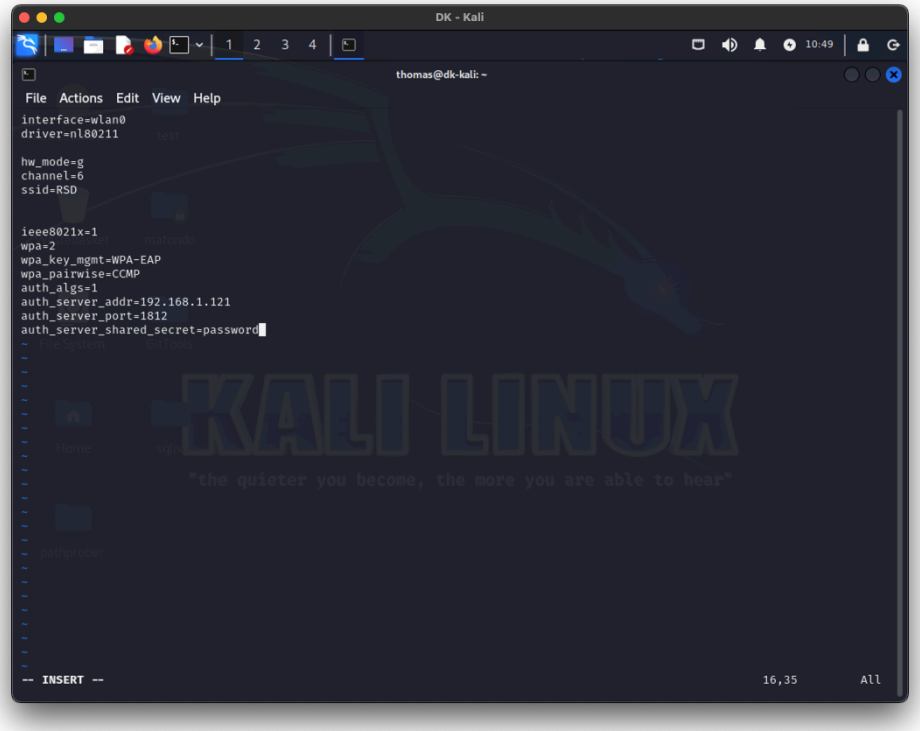
La capture, avec la commande tcpdump ci-dessous :



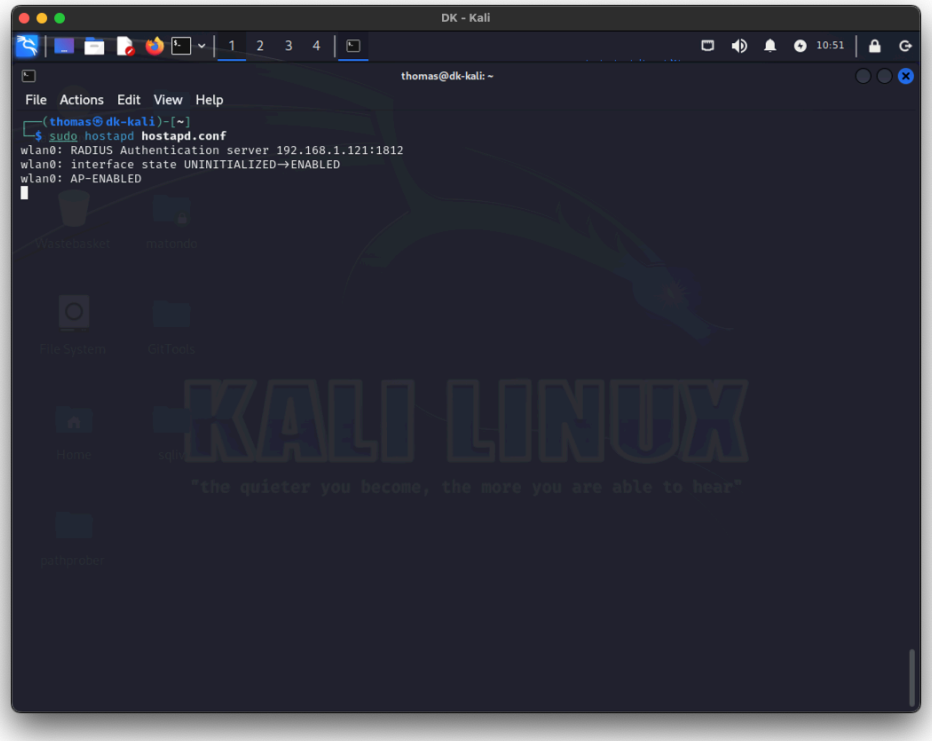
Partie C

Question 1

Noter que le client hostapd a déjà été créé dans les étapes précédentes, en ayant précisé son IP.
Les connexions ne seront donc pas bloquées.

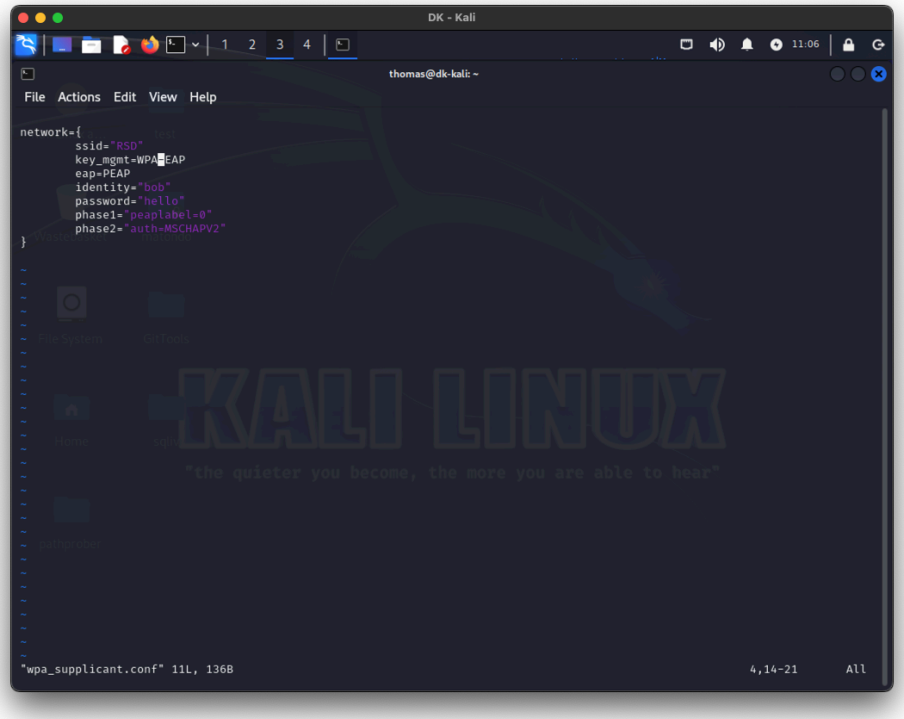


On peut constater qu'il y a bien un serveur d'authentification qui est sur l'ip `192.168.1.121`.

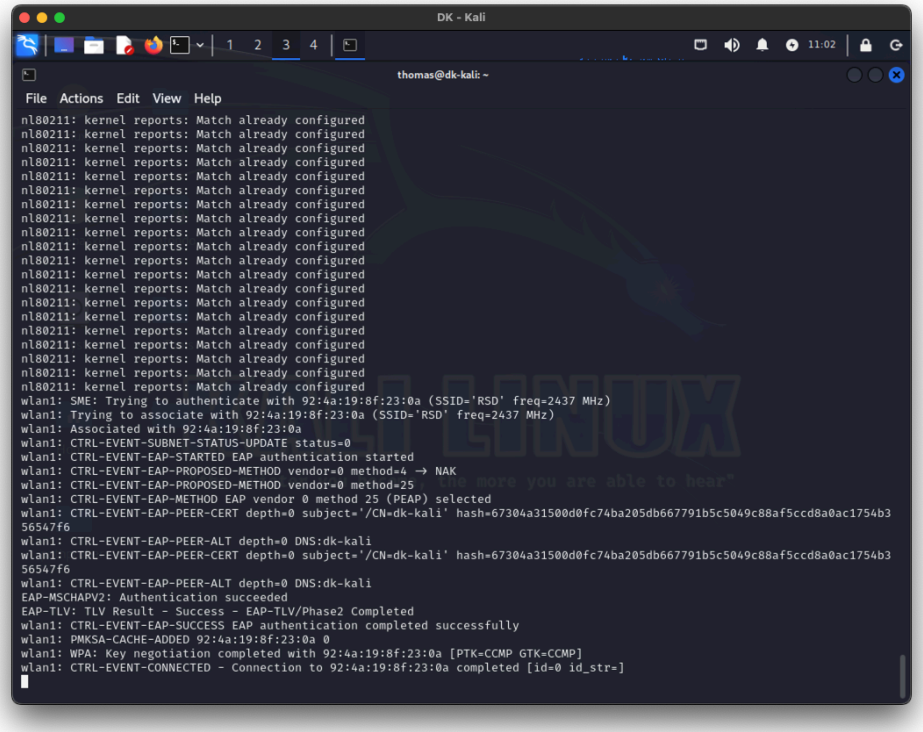


Question 2

Configuration du fichier `wpa2_supplicant.conf` ci-dessous.



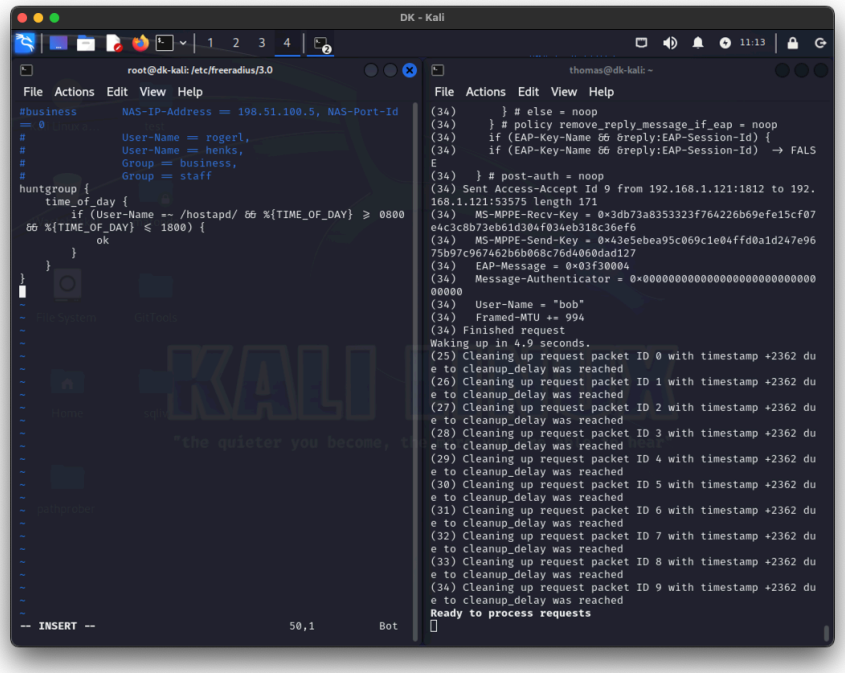
Après avoir démarré `hostapd`, on exécute `wpa_supplicant`, la connexion fonctionne !



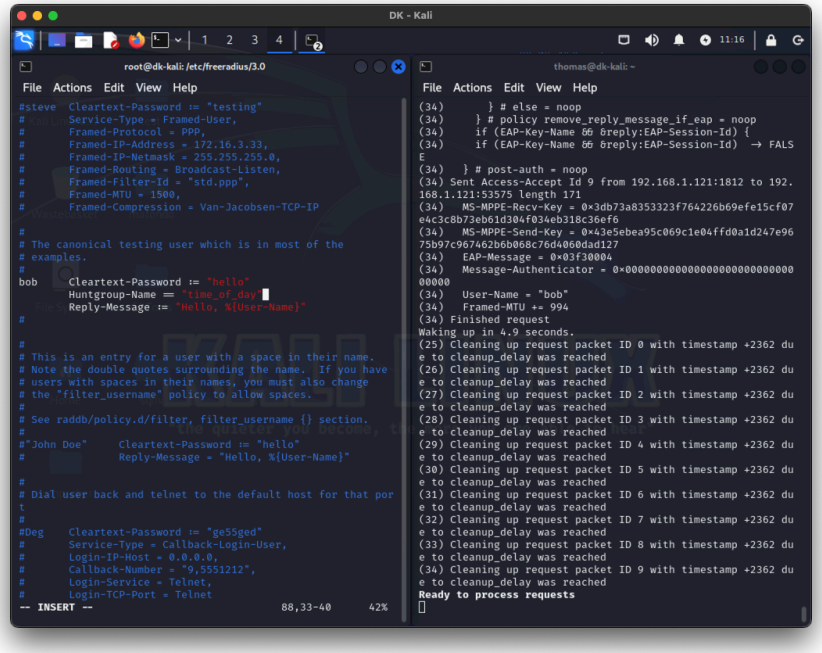
Question 3

Le terme AAA signifie Authentication, Authorization, Accounting.
Voici les fichiers de configurations, ci-dessous, pour n'autoriser les connexions que pendant certaines heures (8h à 18h).

HuntGroup `time_of_day` :

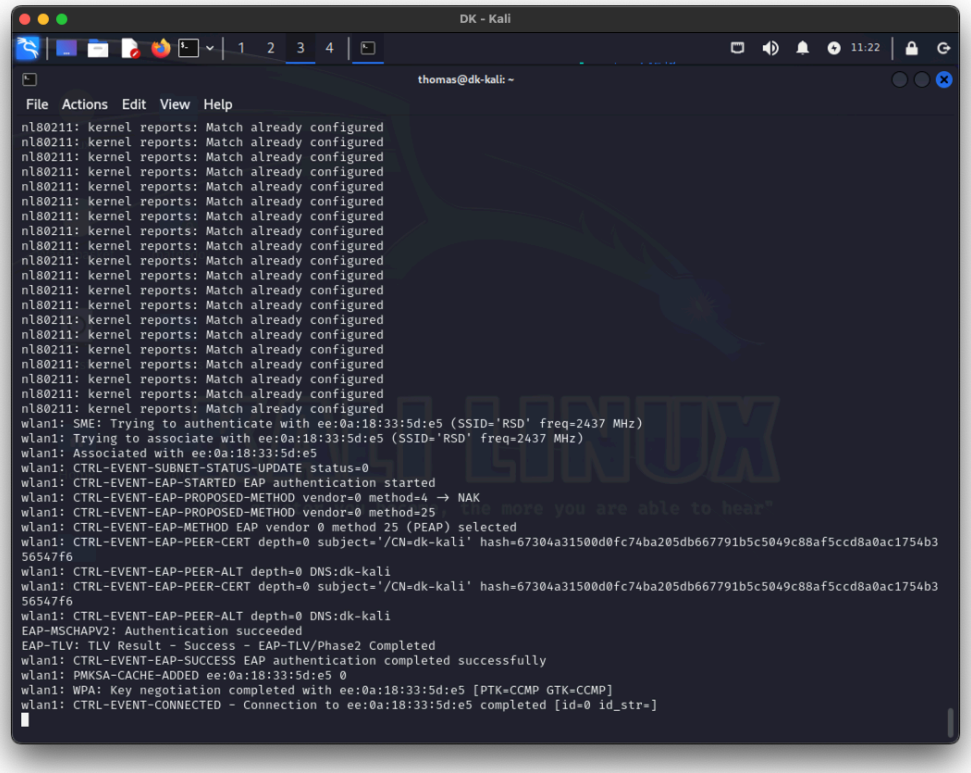


Fichier `users` : on spécifie le group auquel appartient l'utilisateur `bob`.



Question 4

Après avoir modifié la version de `wpa=3` dans le fichier `hostapd.conf`, on tente à nouveau de se connecter, la connexion semble prendre sensiblement plus de temps.



Question 5

WPA3 est une meilleure sécurité Wi-Fi que WPA2. Il rend plus difficile pour les pirates de deviner les mots de passe, offre un cryptage plus fort et protège mieux les réseaux sans fil. De plus, il fonctionne bien avec les appareils plus anciens en les gardant sécurisés.