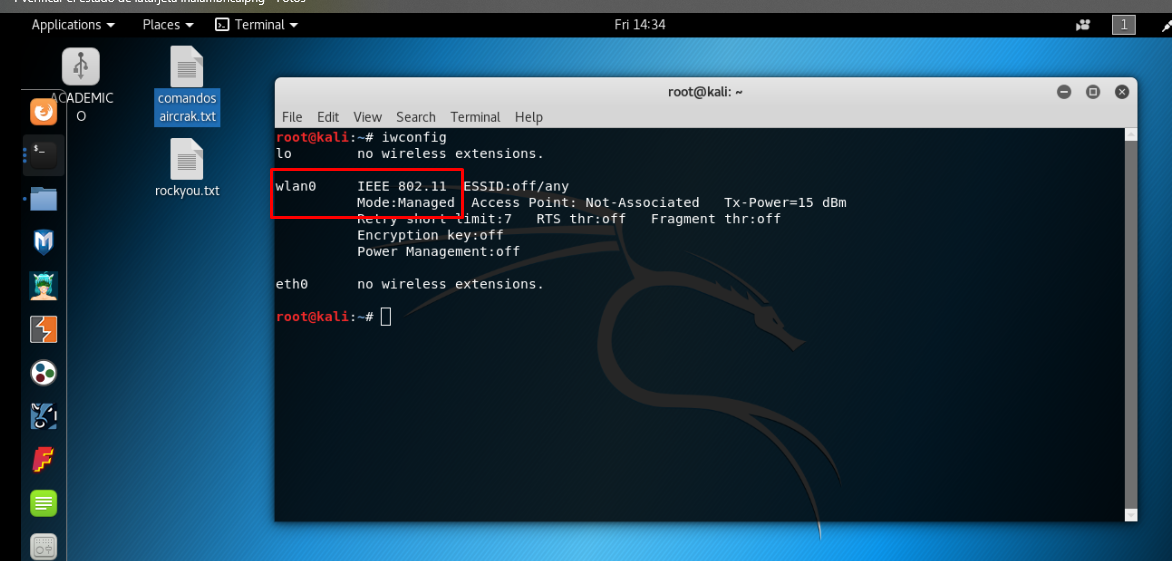
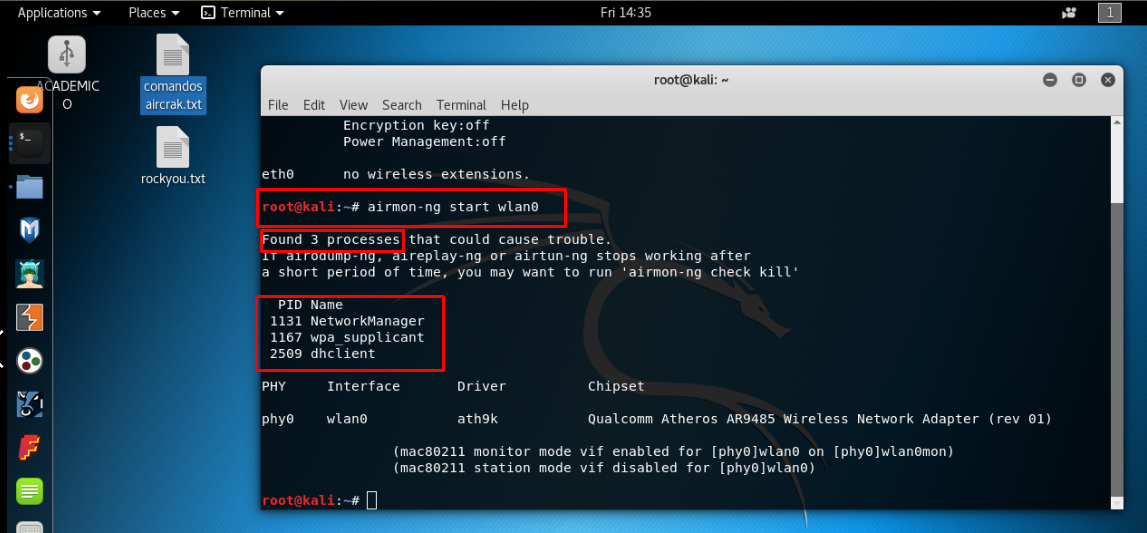
**Red: Wifi: WPA2**

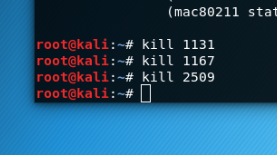
Se procede a verificar el modo de la tarjeta inalámbrica



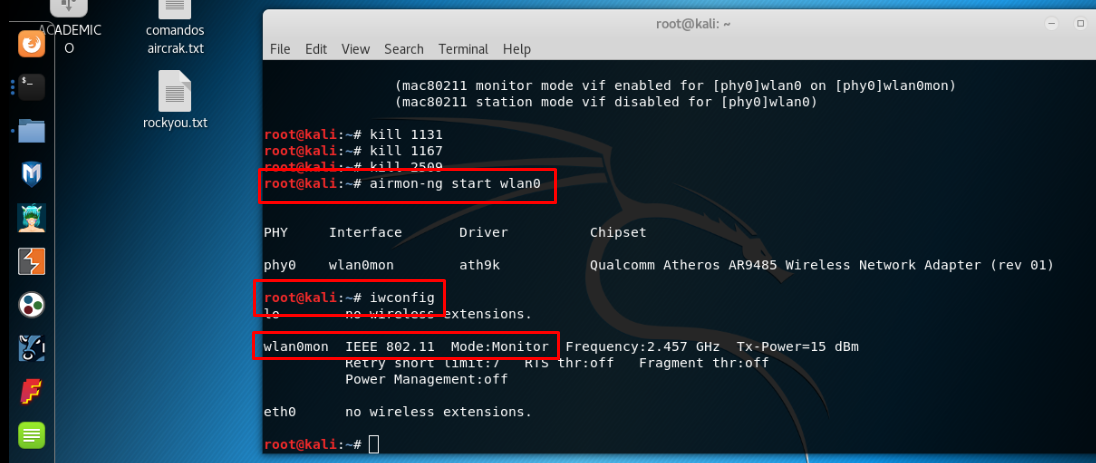
Dado el caso la tarjeta no este en modo monitor, se procede a pasar a dicho modo



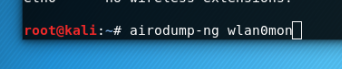
Si aparece procesos que pueden tener algún conflicto, entonces se procede a matarlos



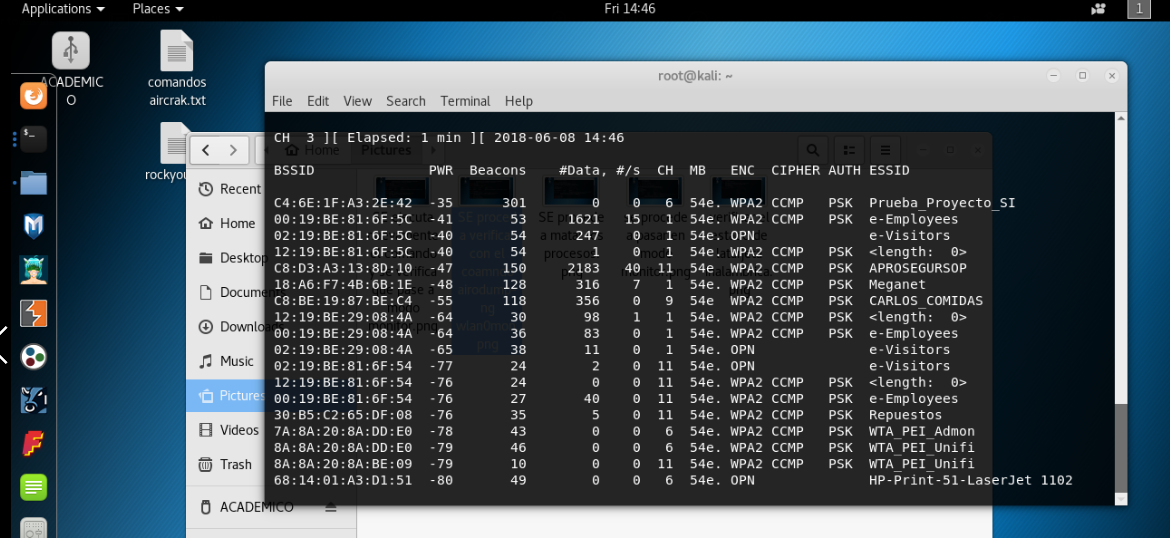
Se procede a habilitar el modo monitor de la tarjeta inalámbrica



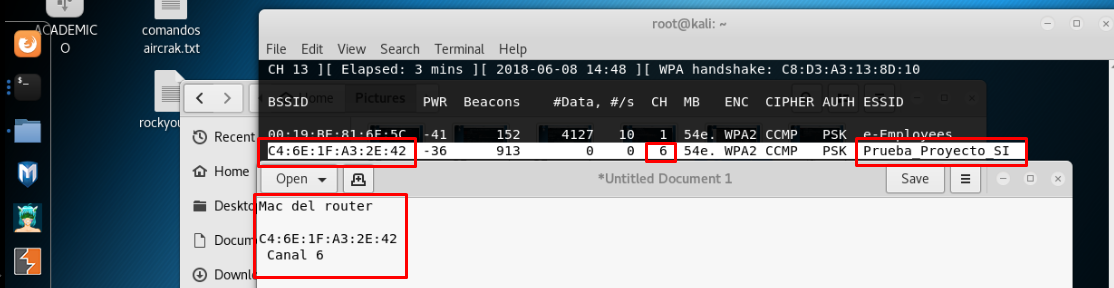
Se procede a ejecutar el comando para visualizar las redes cercanas



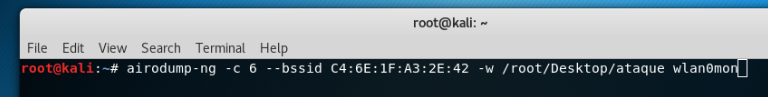
Se detecta varias redes, entre esas la red que se desea atacar



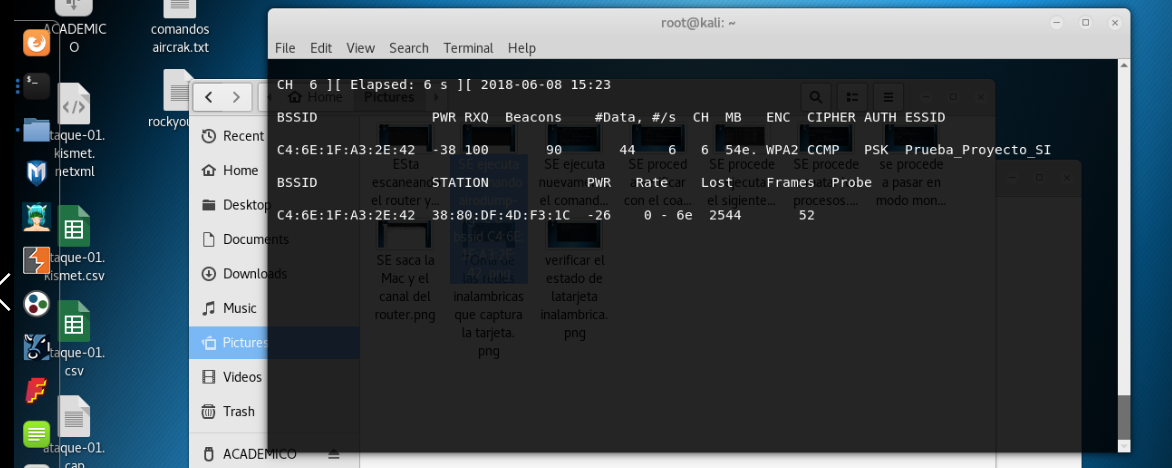
Se procede a tomar los datos del canal y la MAC del router victima



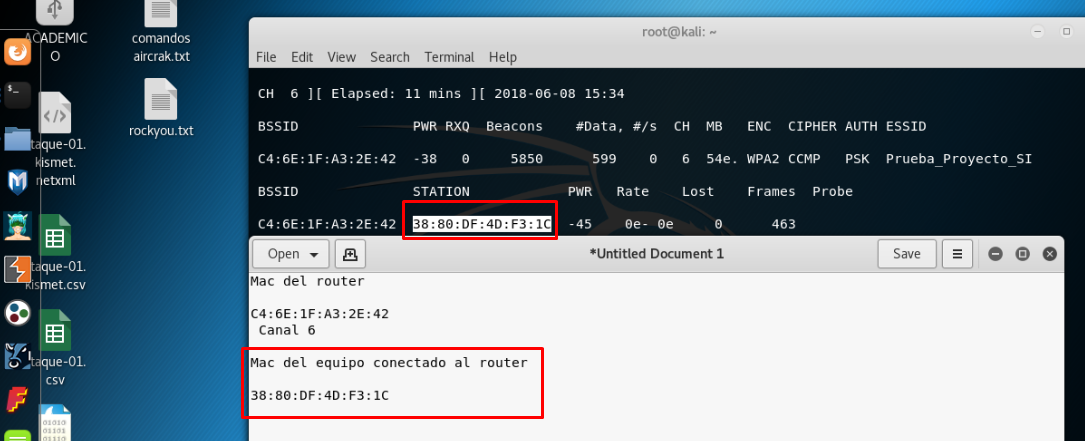
Después de obtener esta información, se ejecuta el siguiente comando especificando MAC y canal de la víctima, donde se crea un archivo, donde estará alojado el handshake



Se ejecuta el comando y se observa que hay un dispositivo conectado a la red



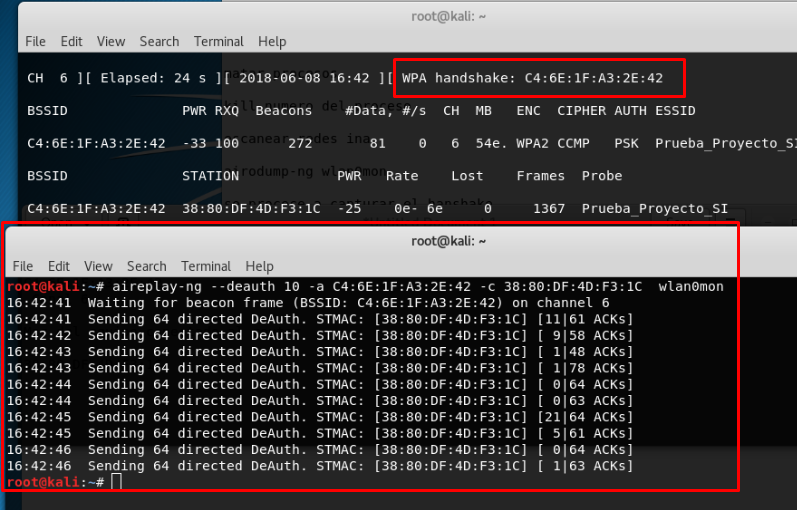
Se toma la MAC del dispositivo que esta conectado al router



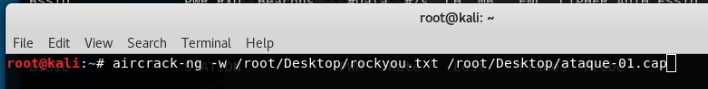
Mientras en la línea de comandos anterior sigue tomando datos de la red, se abre una nueva línea de comandos y se copia lo siguiente



El cual realizara una solicitud 10 veces al router, y cuando termine arrojara el handshake



Después de realizar lo anterior, abriremos otra terminal, y ejecutaremos el siguiente comando, el cual se utilizará aircrack-ng, especificando el diccionario a utilizar y el archivo donde se guardó el handshake.



El cual detecto la contraseña muy rápido, solo comparo 2860 contraseñas, y logro encontrarla, el cual quiere decir que la contraseña que configuramos en el router es insegura.

