**Técnicas de pre-conexión, acceso en redes inalámbricas y descifrado por fuerza bruta**



Daniel Escaño Hernández CET Ciberseguridad

# 

# **1. Índice:**

[**1. Índice:**](#_4jq84lualx9d) **1**

[**2. Práctica 2-1**](#_ofiic1av8ddq) **2**

[**2.1 Capturar paquetes Wifi con Wireshark**](#_5d38uxjyswtl) **2**

[**2.2 Creación de AP falsos con Mana Toolkit**](#_lxlm2eujo30r) **5**

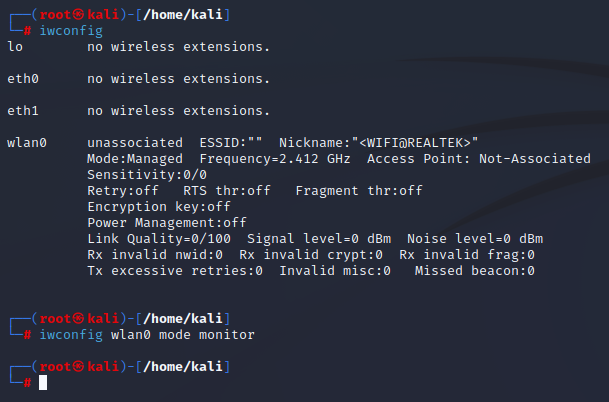
[**2.3 Ataques a dispositivos cifrados con WPS y WPA**](#_wljzpkdnorag) **9**

[**2.4 Wifislax**](#_uyfigniq1eq7) **11**

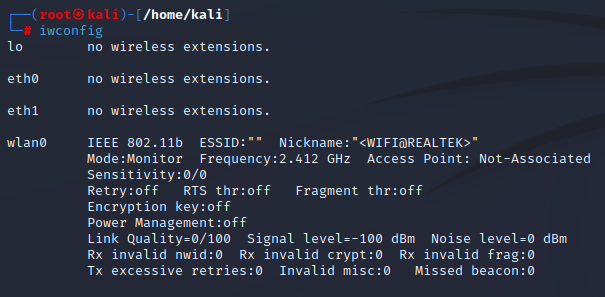
# **2. Práctica 2-1**

### **2.1 Capturar paquetes Wifi con Wireshark**

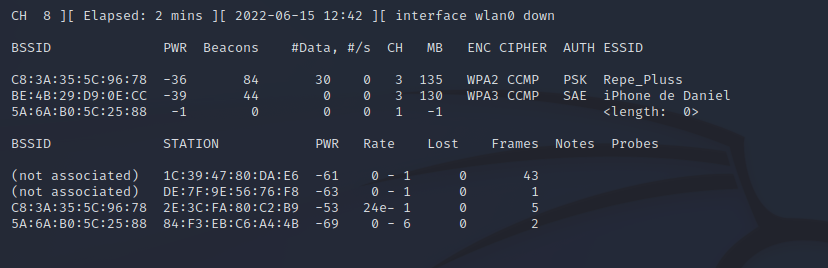
Comprobamos que detectamos la interfaz wlan, y la modificamos a modo monitor



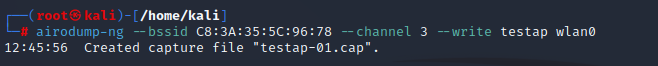
Comprobamos

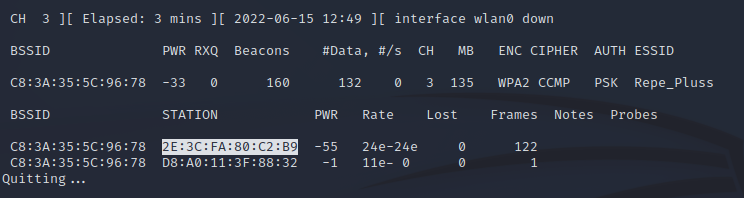


Con el la herramienta Airodump, realizaremos un rastreo de la red:



Procedemos a ejecutar airodump-ng fijando la red a auditar.

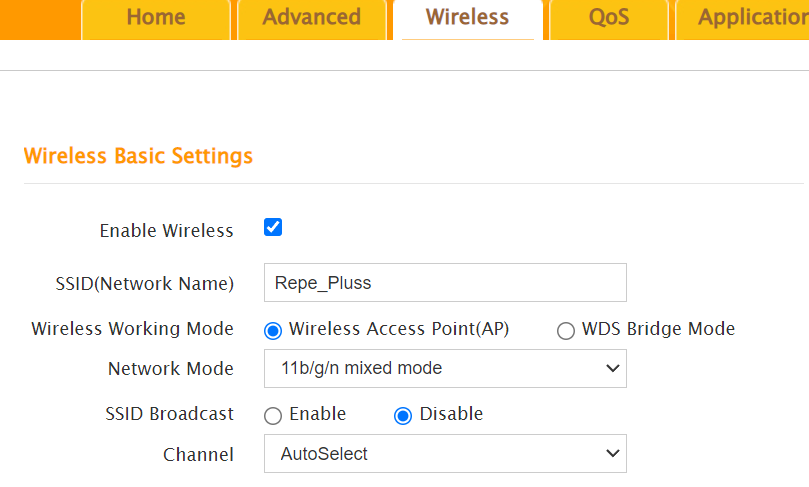


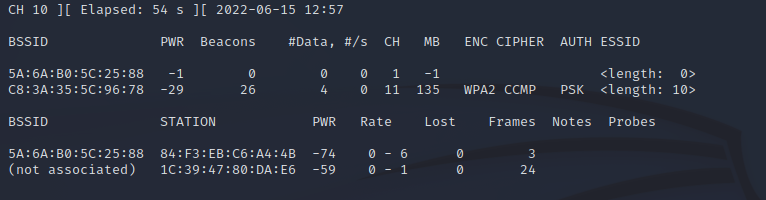




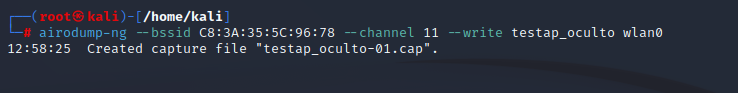
Descubrir redes ocultas. Una red wifi donde se ha ocultado el SSID y no sabemos cómo se llama es un método de protección básico no muy efectivo.

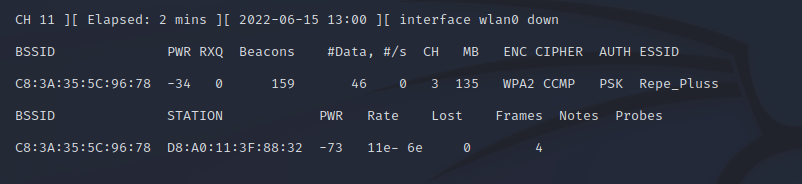
Vamos a hacer la prueba y entramos en la configuración de nuestro punto de acceso y buscamos la opción de OCULTAR SSID.



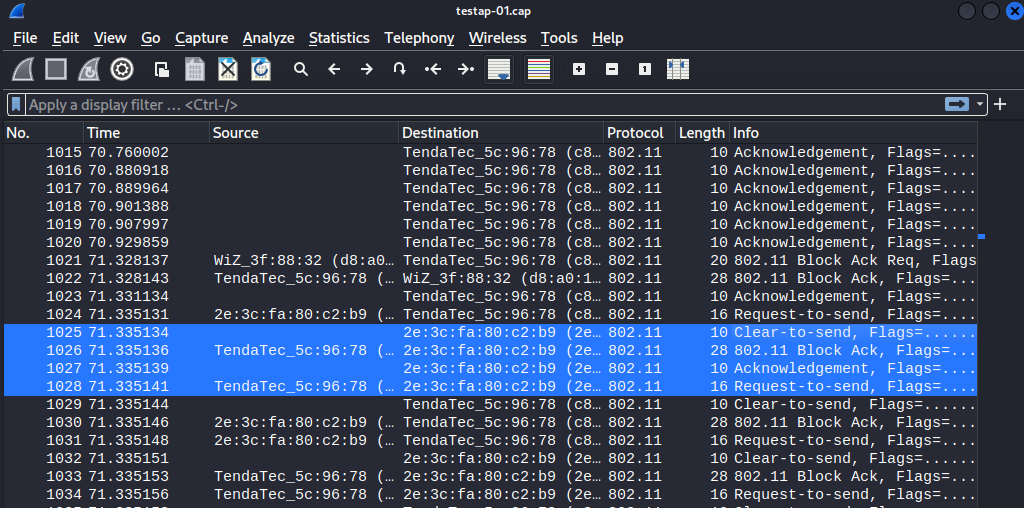


Comprobamos que nuestra red no emite el nombre y nos ponemos a escuchar la red con el comando adaptado al objetivo



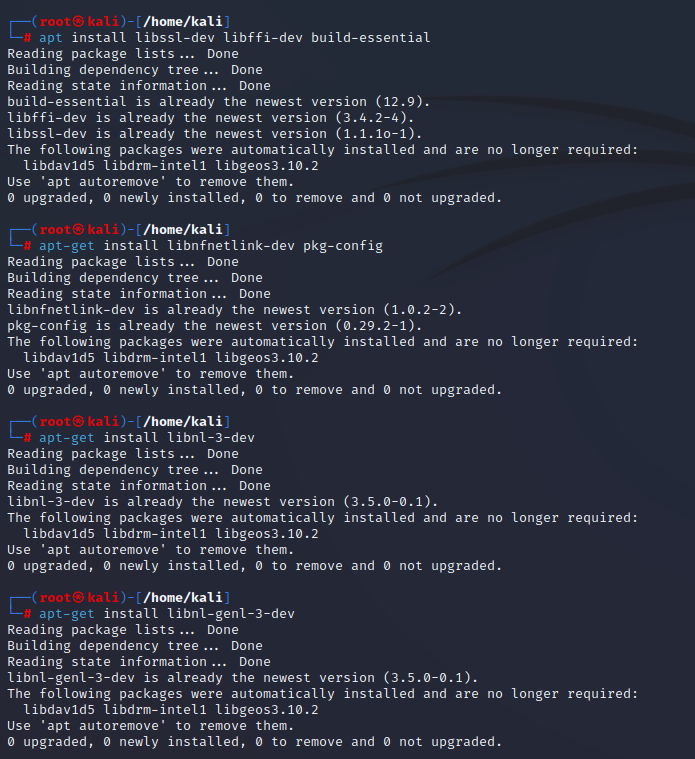


Después de rastrear los paquetes, usar Wireshark, para analizar los paquetes y ver qué información se recopiló de los archivos generados. Si la red específica usa el cifrado WPA2 o la WPA3 que tenemos con el punto de acceso móvil, todos los paquetes están cifrados

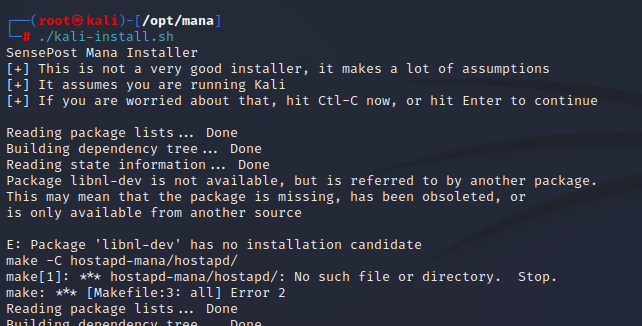


### **2.2 Creación de AP falsos con Mana Toolkit**

En primer lugar instalamos las siguientes dependencias



Antes de continuar, se debe instalar la aplicación primero antes de intentar editar algo en el directorio. Lo instalamos ejecutando el script de instalación

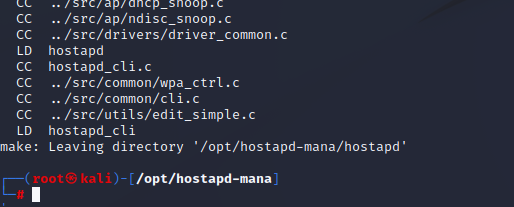


Lo siguiente será instalar hostapd-mana:

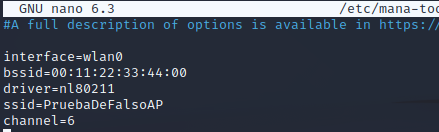
git done <https://github.com/sensepost/hostapd-mana>

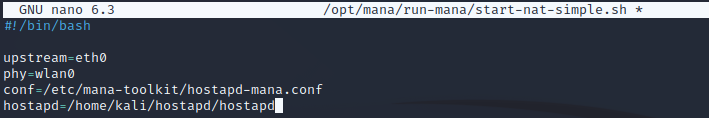
cd hostapd-mana

make -C hostapd

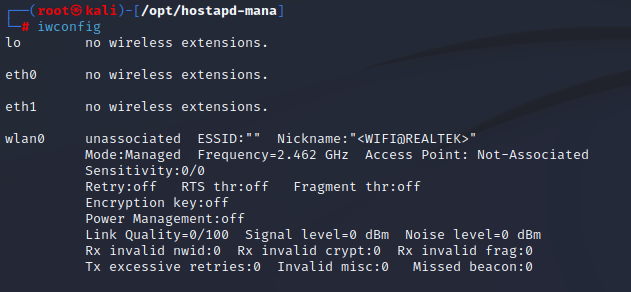


Modificamos los archivos de configuración y comprobamos

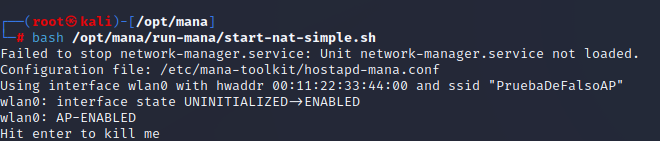




Es importante tener la interfaz de red en modo Manager:



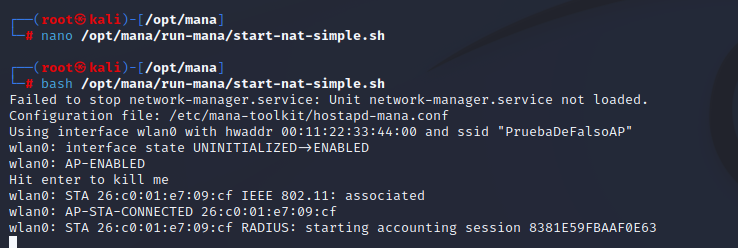
Una vez hecho, ejecutamos mana.



Podemos observar ahora nuestro falso punto de acceso creado, nos conectamos:

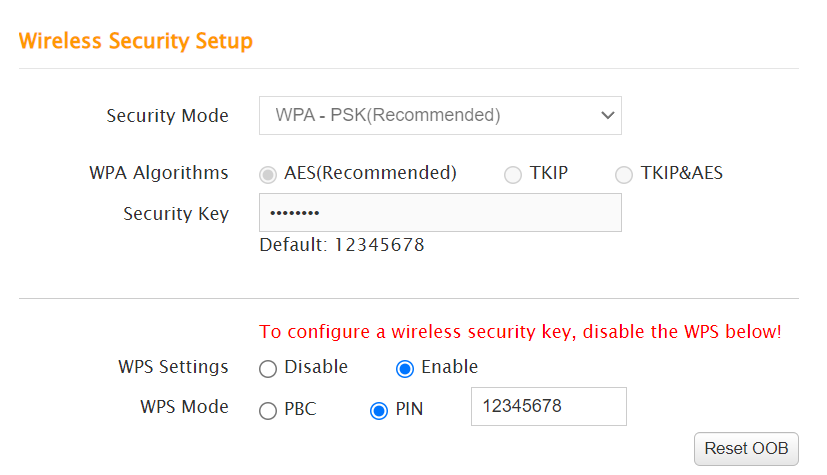


Vemos que al conectarnos, nos aparece la MAC del dispositivo:

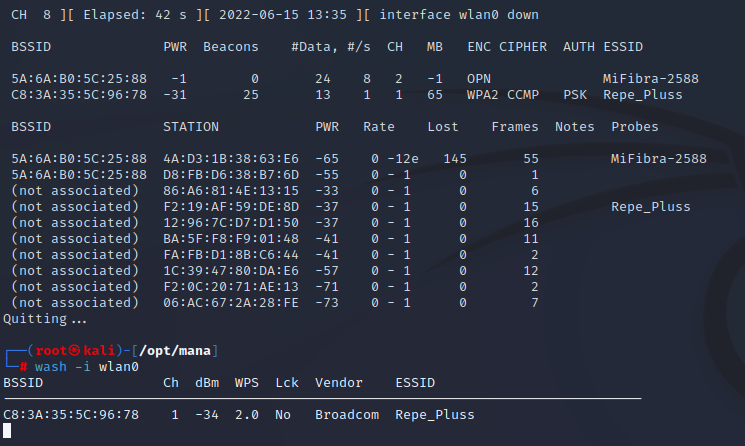


### **2.3 Ataques a dispositivos cifrados con WPS y WPA**

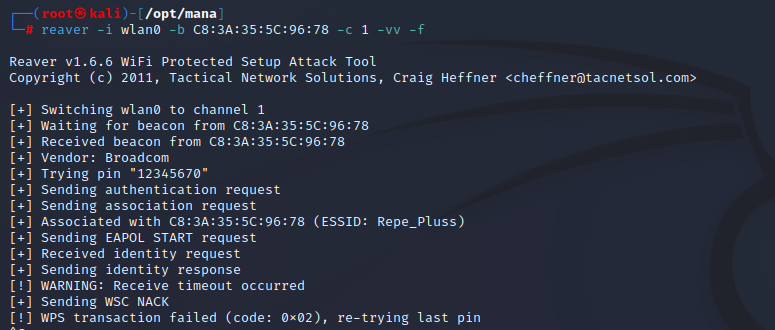
Comenzaremos este apartado entrando a la configuración del router y seleccionando la opción PIN:

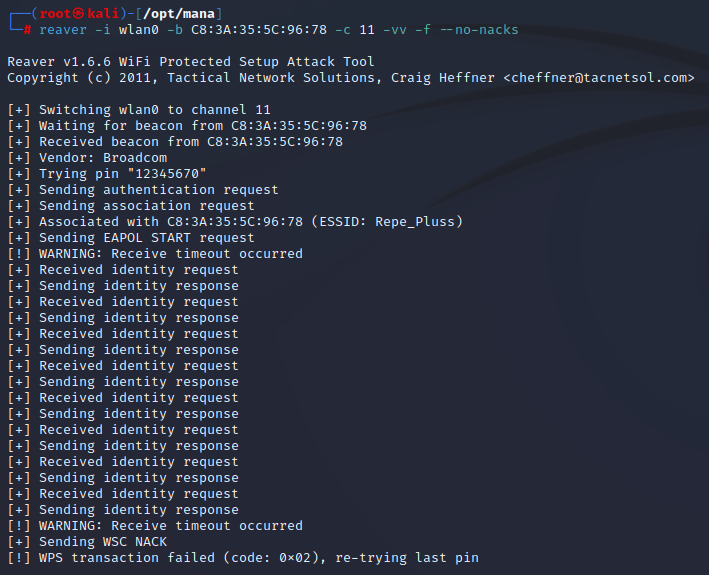


Establecemos el modo monitor y usamos el comando wash -i wlan0.



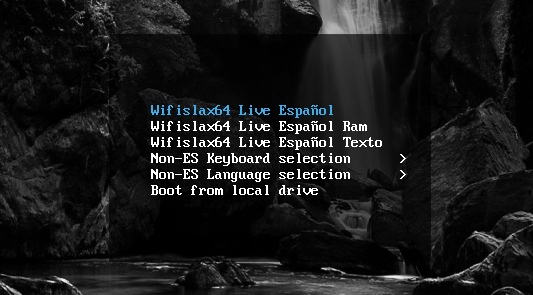
[Me aparecen errores al realizar los diferentes tipos de ataques]

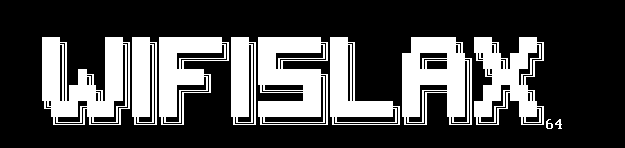




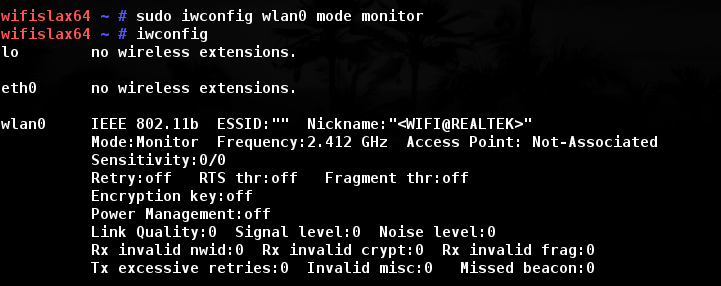
### **2.4 Wifislax**

Instalamos en una máquina virtual nueva, con la iso proporcionada Wifislax:





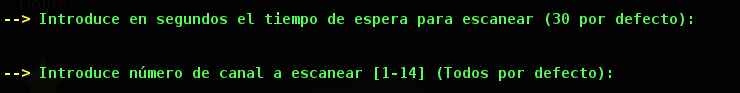
Configuramos la interfaz wlan0 en modo monitor:



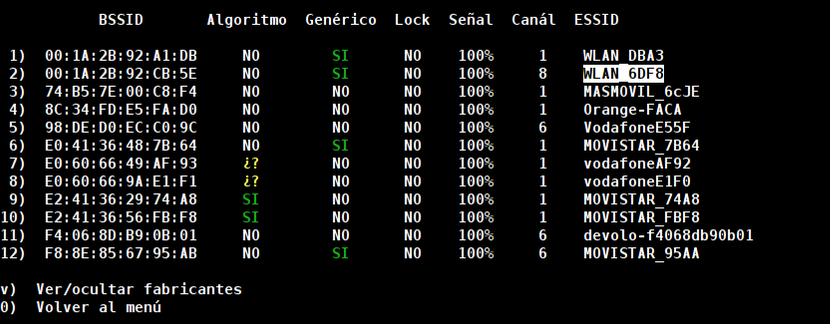
Probaremos las siguientes herramientas: WPSPinGenerator, una herramienta para la búsqueda de objetivos con WPS activado.



Introducimos los parámetros requeridos y comprobamos los resultados.







Otra herramienta es Linset, esta herramienta es capaz de agregar un falso punto de acceso y desconectar a los clientes de la red a la que estamos suplantando para que a la hora de que los usuarios intenten conectarse de nuevo a la red se les redirja a un falso portal.



