INSTALACIÓ (TL-WN722N ■ capture capture kali Linux airodump-ng airodump- -ng capture Troumpt -ng ngoest Trab_ forit who writers copaido wurter, coestoop, coizlicort droeloite teen andcabenge rossarest che paosesitete, cootare TL-WN722N 👺 🔗 🍯 🖪 🔟 🛊 📙 🗖 🚰

Ruben Apablaza Muñoz -OZonE-

Introducción

Esta pequeña guía muestra los pasos para configurar correctamente un adaptador TP-Link TL-WN722N (v2 -v3) en Kali Linux y colocar el mismo en modo monitor para poder realizar laboratorio de pruebas de sniffing.

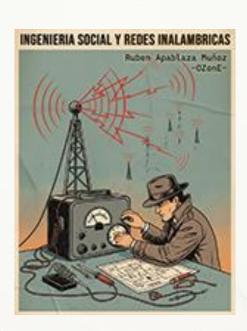
Cabe señalar que de todos los métodos existentes en internet ninguno me funcionaba al 100%. Si bien el nombre de la interfaz no cambia de wlan0 a wlanmon0, cuando se comprueba con el comando iwconfig, la tarjeta ya está en ese modo.

Espero que estos pasos te ayuden.

OBS. Este documento es la preparación para

"Seguridad Ofensiva - "Ingenieria social y Redes inalambricas".

OZONE



1. Preparar el sistema para la compilación

Antes de instalar el driver, necesitamos asegurarnos de que nuestro sistema tiene todas las herramientas y archivos necesarios para compilarlo.

• Actualizar el sistema e instalar dependencias: Abre una terminal y ejecuta el siguiente comando. Esto actualizará los repositorios e instalará las cabeceras del kernel, las herramientas de compilación (build-essential, git), la herramienta bc y dkms.

sudo apt update

sudo apt install -y linux-headers-\$(uname -r) build-essential git dkms bc

2. Eliminar y reinstalar el driver

Aunque ya teníamos el driver instalado (en Linux 2025 viene preinstalado, si no lo tienes no importa, simplemente sigues desde aquí), es mejor empezar de cero para evitar conflictos.

• Eliminar la instalación anterior: Si el directorio rtl8188eus ya existe, elimínalo para poder clonar el repositorio de nuevo.

rm -rf rtl8188eus

 Clonar el repositorio del driver: Descarga el driver compatible con el modo monitor.

git clone https://github.com/aircrack-ng/rtl8188eus.git

 Compilar e instalar el driver: Navega al directorio y usa make para compilar e instalar el driver.

cd rtl8188eus sudo make sudo make install

Si no hay errores, el driver se habrá instalado correctamente.

MUY IMPORTANTE

CADA VEZ QUE SE INICIE EL SISTEMA HAY QUE HACER LOS PASOS SIGUIENTES NUEVAMENTE!!!

3. Cargar el driver y activar el modo monitor

Una vez instalado el driver, debes cargarlo y configurar la interfaz en modo monitor manualmente.

Desactivar el driver genérico y cargar el nuevo: Esto asegura que el sistema use el driver que acabas de instalar.

sudo modprobe -r rtl8xxxu sudo modprobe 8188eu

Verificar que el driver está activo: Comprueba que el nuevo módulo del kernel está cargado.

Ismod | grep 8188eu

Deberías ver una salida que confirme que el módulo 8188eu está en uso.

EN ESTE PUNTO CONECTAR EL ADAPTADOR TP LINK

Activar el modo monitor manualmente: Evita airmon-ng y usa los comandos iw para un control más directo y fiable.

sudo airmon-ng check kill # Detiene procesos que pueden interferir sudo ip link set wlan0 down sudo iw dev wlan0 set type monitor

sudo ip link set wlan0 up

4. Escanear redes

Finalmente, con la interfaz en modo monitor, puedes usar airodump-ng para escanear las redes Wi-Fi cercanas.

Verificar el modo de la interfaz: Asegúrate de que wlan0 está en Mode:Monitor.

iwconfig

Ejecutar el escaneo: Utiliza airodump-ng en la interfaz wlan0.

sudo airodump-ng wlan0

Y con una interfaz identificada ya podemos realizar un escaneo dirigido y solicitar que envíe la salida a un archivo.

sudo airodump-ng --bssid 48:D3:43:XX:XX:XX -c 1 -w captura wlan0

HAY QUE HACER ESTOS PASOS CADA VEZ QUE INICIEMOS EL SISTEMA SI QUEREMOS UTILIZAR NUESTRO ADAPTADOR TPLINK.

ESTAMOS SIN INTERNET, POR QUE?

El problema que tienes es que al usar el comando **sudo airmon-ng check kill**, este detiene el proceso **NetworkManager**, que es el que gestiona todas tus conexiones de red (tanto cableadas como inalámbricas). Por lo tanto, al ejecutar ese comando se pierde la conexión a Internet.

Aquí está el procedimiento para solucionar esto y tener ambas cosas funcionando:

Ejecutar airmon-ng sin matar NetworkManager: En lugar de usar sudo airmon-ng check kill, que detiene el gestor de red, desactiva solo los procesos que afectan a la interfaz inalámbrica. Si ya usaste airmon-ng check kill, simplemente reinicia NetworkManager.

sudo systemctl start NetworkManager

Y con esto quedará ok la conexión cableada si tenías una.

DE TODAS FORMAS CADA VEZ QUE REINICIEMOS NUESTRA MAQUINA TENDREMOS NUEVAMENTE NUESTRA CONFIGURACION "NORMAL" Y SI NO ESTA CONECTADO EL ADAPTADOR WIFI SIMPLEMENTE NO HABRA PROBLEMA.

Configuración adicional en el router.

Otra configuración que hay que hacer para probar con este adaptador para capturar paquetes en nuestro laboratorio es ir a la configuración del router y en la configuración de red inalámbrica de **2.4ghz** la dejamos con la siguiente configuración y una contraseña sencilla para que nuestro diccionario **rockyou.txt** sea capaz de detectarla.



Y apagar la red inalámbrica de 5ghz

