Informe 3 – Segundo Parcial

Yadier Stiven Mayoral Palomeque

Facultad de Ingeniería, Universidad Tecnológica del Chocó Diego Luis Córdoba

2720409: Seguridad y Auditoria de Redes

Docente: Rafael Sandoval Morales

Quibdó, Chocó

Septiembre 2025

Tabla de Contenido

Pag.

Introducción 4

Objetivos 5

Objetivo General 5

Objetivos Específicos 5

Entorno 6

Desarrollo 6

Conexión del Adaptador a la Máquina 6

Preparación del Entorno 7

Descarga del Controlador Realtek RTL8188EUS 9

Desactivación de controladores en conflicto 9

Habilitación del Modo Monitor 10

Prueba de Detección de Redes e Inyección de Paquetes 11

Prueba de Detección de Redes 11

Prueba de Inyección de Paquetes 12

Conclusión 13

Referencias 14

Tabla de Ilustraciones

Pag.

Ilustración 1 Configuración de adaptador 6

Ilustración 2 Verificación de modelo adaptador 7

Ilustración 3 Actualización de dependencias 7

Ilustración 4 Instalación de herramientas 8

Ilustración 5 Clonación de repositorio 9

Ilustración 6 Compilación de código 9

Ilustración 7 Bloqueo de controladores 10

Ilustración 8 Verificación del modo 10

Ilustración 9 Cambio a modo monitor 11

Ilustración 10 Detección de redes 11

Ilustración 11 Prueba de Inyección de paquetes 12

Introducción

En este informe se documenta el proceso de instalación de los drivers pertinentes de la antena **TP-LINK TL-WN722N VERSION 4** en Kali Linux, con el objetivo de hacer uso de esta en su modo monitor para hacer auditorias de redes inalámbricas y demás.

Objetivos

Objetivo General

Documentar y ejecutar el proceso de instalación de los controladores para la antena **TP-LINK TL-WN722N versión 4** en **Kali Linux**, con el fin de habilitar el modo monitor.

Objetivos Específicos

Identificar y confirmar el chipset de la antena mediante comandos de sistema (lsusb, dmesg) para determinar el controlador apropiado.

Instalar las dependencias y herramientas necesarias para compilar e integrar drivers (git, build-essential, dkms, linux-headers, etc.).

Descargar, compilar e instalar el driver compatible (con soporte DKMS cuando esté disponible) para el chipset Realtek presente en la versión 4.

Configurar el sistema para evitar conflictos de módulos (blacklist de drivers nativos) y cargar el módulo correcto en el kernel.

Poner la interfaz inalámbrica en modo monitor y comprobar su reconocimiento con herramientas como iwconfig, airmon-ng y ip.

Entorno

Se trabajó en un entorno controlado conformado por una máquina virtual Kali Linux ejecutada en VirtualBox, en la cual se instaló y configuró la antena TP-LINK TL-WN722N versión 4.

Las herramientas empleadas incluyeron: lsusb, dmesg, git, make, gcc/g++, dkms, iwconfig, airmon-ng, airodump-ng, aireplay-ng y utilidades estándar de Linux para la gestión de redes y compilación de drivers.

Desarrollo

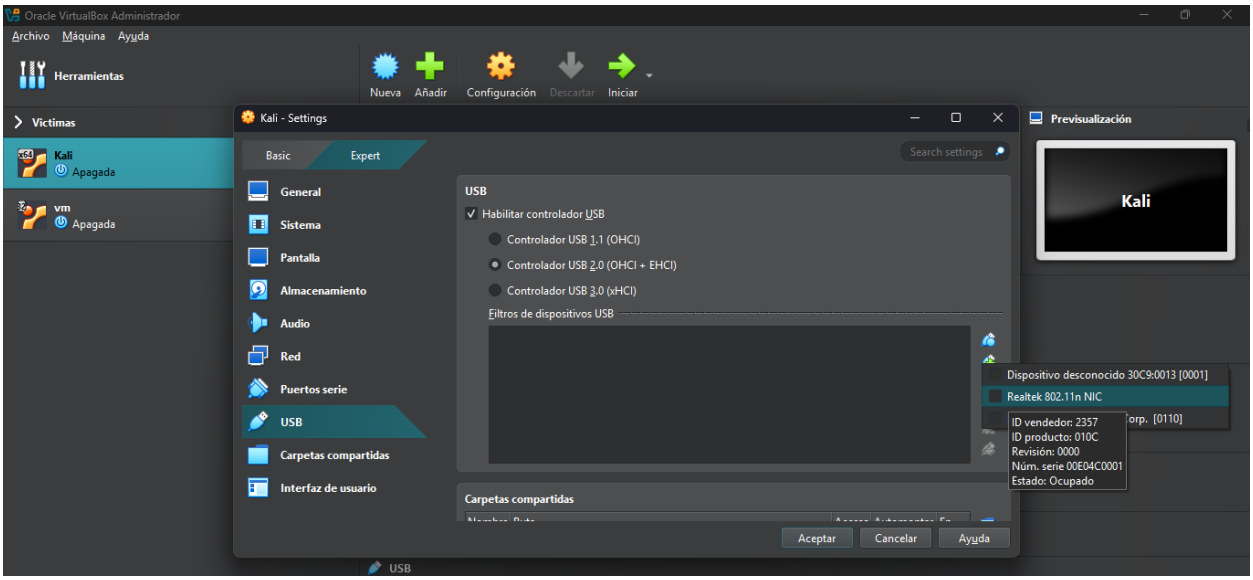
A continuación, se documenta el procedimiento seguido para identificar el chipset, descargar e instalar el controlador adecuado, preparar el sistema y poner la interfaz inalámbrica en **modo monitor**.

Conexión del Adaptador a la Máquina

Conectar físicamente la antena TP-LINK TL-WN722N v4 al dispositivo.

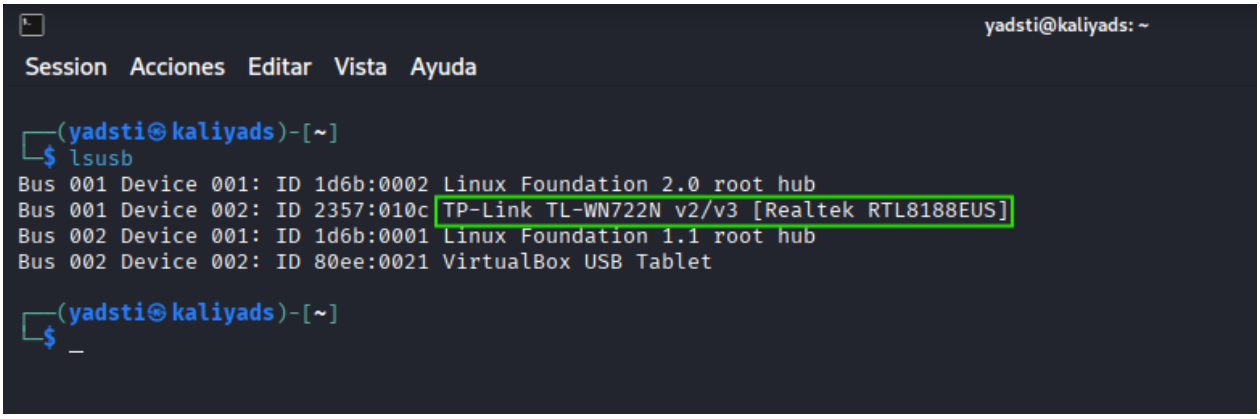
En VirtualBox: Dispositivos → USB seleccionar el adaptador USB para que sea "conectado" a la VM Kali.

Ilustración 1 Configuración de adaptador



Luego se enciende la máquina virtual, se abre una terminal y se comprueba que si haya reconocido el dispositivo USB, con el comando lsusb, como se evidencia en la siguiente ilustración y dentro de un recuadro verde se ve que el Bus 001 Device 002 tiene un adaptador TP-Link TL-WN722N v2/v3 Realtek RTL8188EUS.

Ilustración 2 Verificación de modelo adaptador

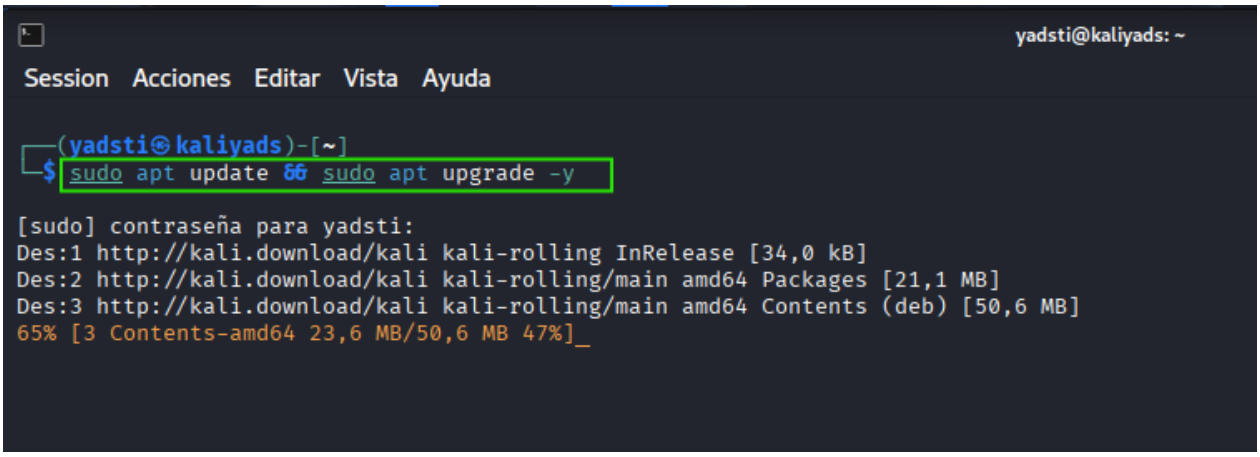


Preparación del Entorno

Una vez se confirma que Kali si reconoce el dispositivo, se procede con la preparación del entorno (actualización de dependencias e instalación de herramientas).

Lo primero es la actualización de las dependencias de Kali usando el comando **sudo apt updtae && sudo apt upgrade -y**.

Ilustración 3 Actualización de dependencias



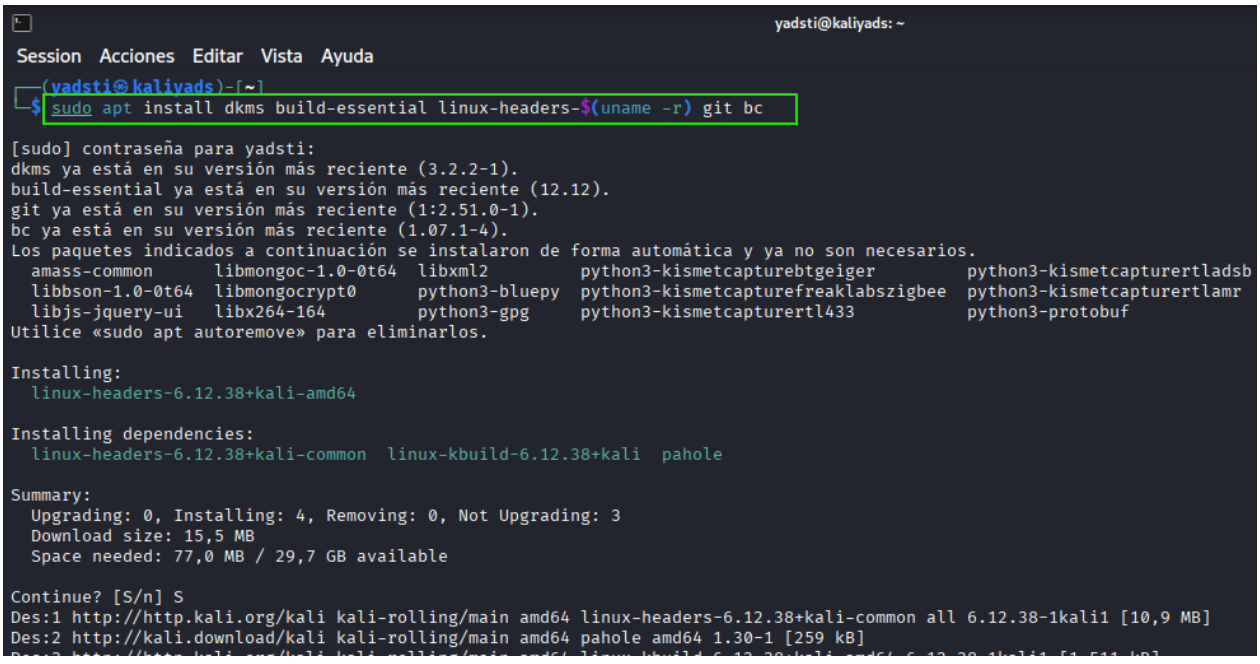
Luego se instalan las herramientas de compilación haciendo uso del siguiente comando:

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

Este comando se desglosa de la siguiente forma:

- dkms: Administra los módulos del kernel.
- build-essential: Incluye herramientas de compilación como y .gccmake
- linux-headers-$(uname -r): Instala los encabezados que coinciden con la versión actual del kernel.
- git: Se utiliza para clonar repositorios, esencial para descargar el código fuente del controlador.
- bc: Un lenguaje de calculadora, a veces necesario durante la compilación del controlador para operaciones matemáticas.

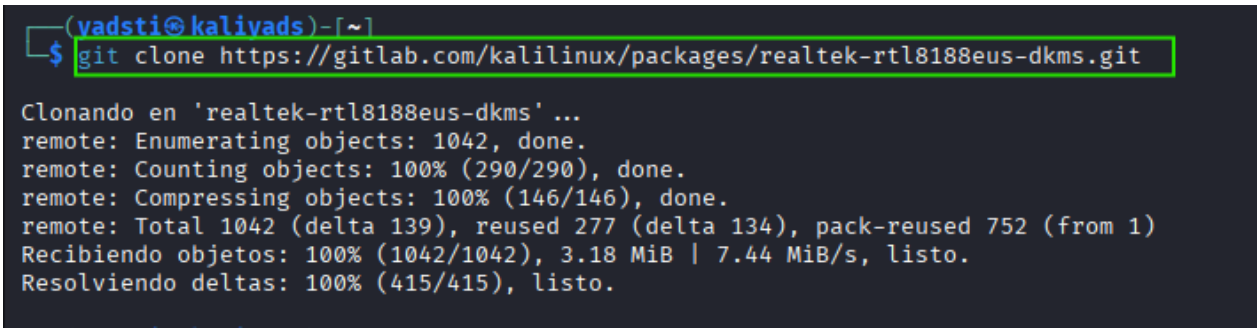
Ilustración 4 Instalación de herramientas



Descarga del Controlador Realtek RTL8188EUS

Esta es la parte importante, se procede a clonar el repositorio que contiene el controlador, el cual es proporcionado por Kali Linux desde su repositorio oficial.

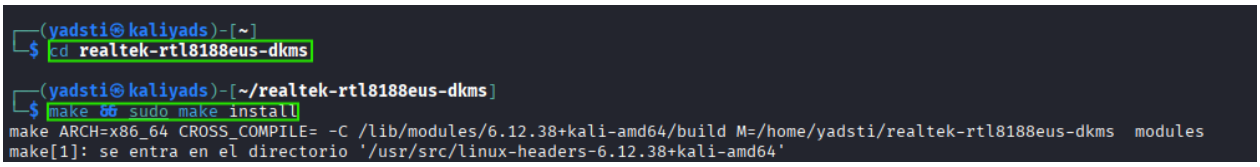
Ilustración 5 Clonación de repositorio



Una vez clonado el repositorio, el siguiente paso es compilar el controlador desde el código fuente.

Se navega hasta el directorio clonado y se ejecuta el siguiente comando para compilar el controlador:

Ilustración 6 Compilación de código



Desactivación de controladores en conflicto

Una vez el controlador esta instalado, se procede a bloquear los controladores que lo precedían con el fin de evitar fututos conflictos.

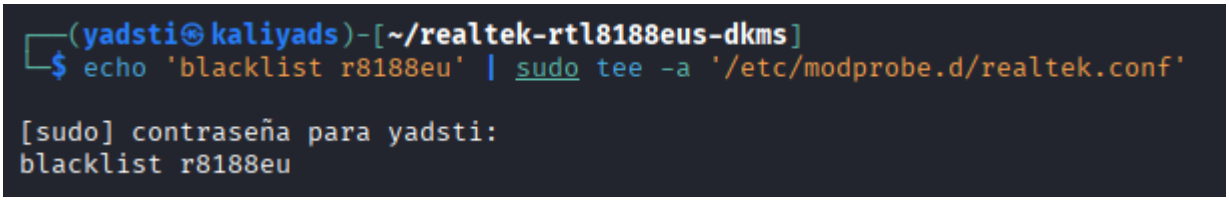
Esto se hace con el siguiente comando:

echo 'blacklist r8188eu' | sudo tee -a '/etc/modprobe.d/realtek.conf'

Este comando se desglosa:

- **echo 'blacklist r8188eu'**: Crea una línea de texto para bloquear el controlador.r8188eu
- **| sudo tee -a '/etc/modprobe.d/realtek.conf'**: Anexa ese texto al archivo con privilegios de superusuario, lo que garantiza que el controlador esté en la lista negra./etc/modprobe.d/realtek.conf

Ilustración 7 Bloqueo de controladores



Una vez hecho esto se reinicia la máquina virtual para continuar con el proceso.

Habilitación del Modo Monitor

Luego de reiniciar la maquina se abre una terminal nuevamente y se utiliza el siguiente comando: **iwconfig**, con el fin de revisar en qué modo está trabajando la antena.

Ilustración 8 Verificación del modo

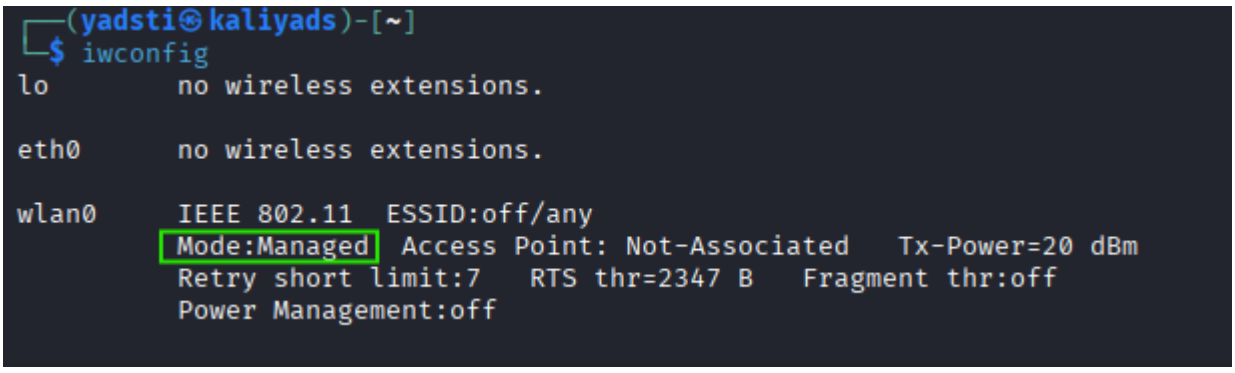
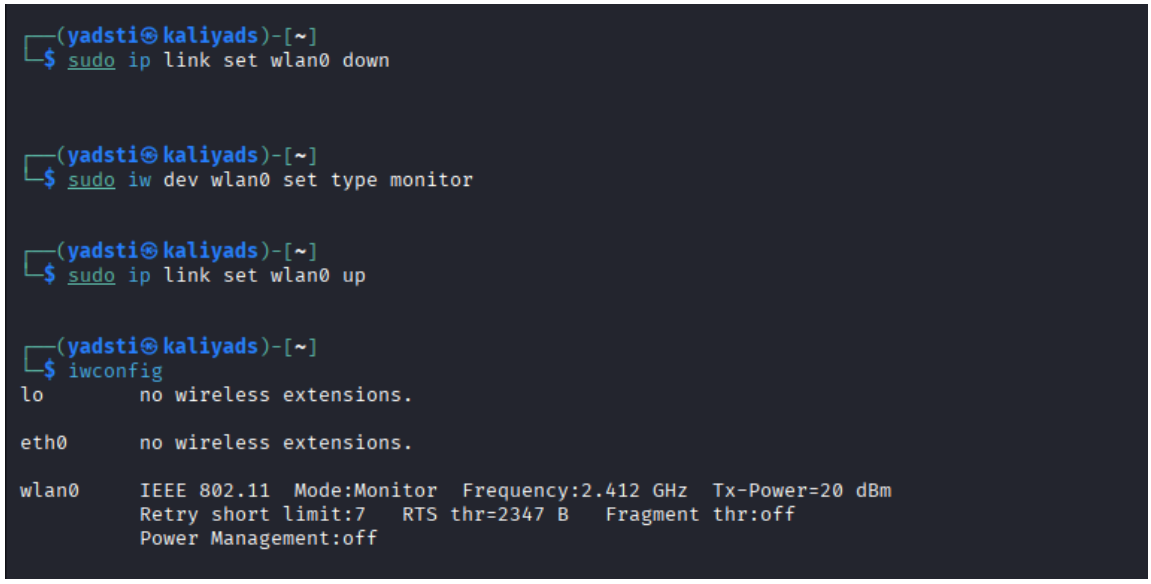


Ilustración 9 Cambio a modo monitor



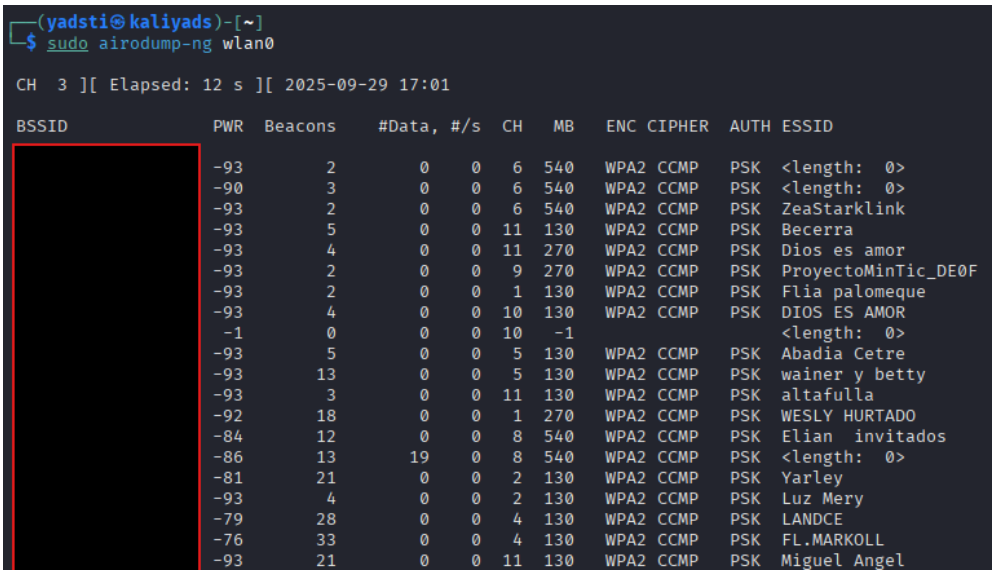
Prueba de Detección de Redes e Inyección de Paquetes

Luego de que se verifica que efectivamente la antena ya se encuentra en modo monitor se procede a hacer una prueba de detección de redes y otra de inyección.

Prueba de Detección de Redes

Para hacer la prueba de detección se utiliza el comando **airodump-ng wlan0**

Ilustración 10 Detección de redes

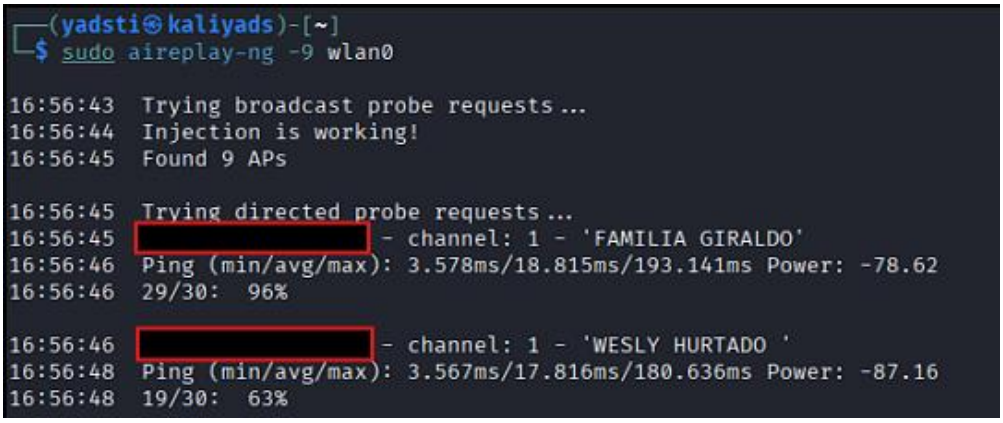


La figura muestra la salida de **airodump-ng** obtenida con la interfaz inalámbrica en modo monitor. En la tabla se listan los puntos de acceso detectados, con sus respectivas direcciones MAC (BSSID), potencia de señal (PWR), número de beacons, volumen de tráfico (#Data), canal (CH), tasa máxima anunciada (MB) y configuración de seguridad (ENC, CIPHER, AUTH). Se observan múltiples redes protegidas con **WPA2-CCMP (PSK)**, lo que indica uso de contraseña precompartida; además aparecen redes con ESSID oculto (<length: 0>). Las intensidades de señal varían, valores próximos a -90 dBm corresponden a AP con señal débil, lo que influye en la viabilidad de capturas e inyección. Esta información permite seleccionar objetivos para pruebas controladas.

Prueba de Inyección de Paquetes

Se realizó una prueba de inyección con **aireplay-ng -9** para verificar la capacidad de inyección del adaptador en modo monitor. El comando confirmó que la inyección funciona (Injection is working!) y detectó múltiples APs. Para cada AP se registraron BSSID, canal, ESSID, potencia (Power), tiempos de respuesta y porcentaje de respuesta a probes dirigidos (ej. 29/30: 96% indica 29 respuestas de 30 paquetes). Los APs con mayor porcentaje de respuesta y mejor potencia son los candidatos más adecuados para posteriores pruebas controladas (captura de handshakes, tests de deautenticación).

Ilustración 11 Prueba de Inyección de paquetes



Conclusión

La instalación de los drivers correspondientes a la antena TP-LINK TL-WN722N versión 4 en Kali Linux permitió habilitar correctamente el dispositivo para su uso. Una vez instalados y configurados, se verificó que el adaptador pudo ser puesto en **modo monitor**, lo que facilita la captura y análisis del tráfico inalámbrico.

Este proceso demostró la importancia de contar con controladores adecuados para garantizar la compatibilidad del hardware con el sistema operativo, así como la correcta ejecución de funciones avanzadas como el monitoreo de redes. En conclusión, la práctica fue exitosa, ya que se logró el objetivo de activar el modo monitor en la antena, validando su funcionamiento dentro del entorno de pruebas.

Referencias

Sandoval Morales, R. (2025). *Seguridad y Auditoria de Redes. Quibdó*

netcat | Kali Linux Tools. (n.d.). Kali Linux. https://www.kali.org/tools/netcat/

Davidochobits. (2021, November 4). *Uso del comando Ncat (nc) en Linux con ejemplos - ochobitshacenunbyte*. Ochobitshacenunbyte. https://www.ochobitshacenunbyte.com/2021/11/04/uso-del-comando-ncat-nc-en-linux-con-ejemplos/

Ejemplos de comandos WC: contar el número de líneas, palabras y caracteres. (n.d.). https://es.linux-console.net/?p=20171

Kumar, A. (2024, September 28). *How I used monitor mode on TP-Link WN722N for fun*. It's FOSS. https://itsfoss.com/monitor-mode-fun/?utm_source=chatgpt.com