



H4ck Minds 2024

La ciberseguridad en telecomunicaciones aborda la protección de redes y sistemas de comunicación ante amenazas cibernéticas. Abordaremos los conceptos fundamentales y su relación con los drones y otras tecnologías inalámbricas, destacando los riesgos y las soluciones disponibles.

Las telecomunicaciones son la transmisión de información a través de medios físicos o inalámbricos. Estas incluyen redes de radio, televisión, satélites, WiFi y redes móviles. En el contexto de la ciberseguridad, es fundamental proteger estas comunicaciones contra accesos no autorizados y ataques maliciosos.

- Los protocolos son reglas que regulan la comunicación entre dispositivos. Los más comunes incluyen:
- **WiFi (IEEE 802.11):** Comunicación inalámbrica local.
- **Bluetooth:** Conexión de corto alcance.
- **ZigBee y LoRa:** IoT y redes de sensores.
- **5G y LTE:** Redes móviles avanzadas.
- Cada protocolo tiene vulnerabilidades específicas que deben considerarse.

Los drones dependen de las telecomunicaciones para operar. Utilizan WiFi, RF y GPS para su control, navegación y transmisión de datos. Comprender estas conexiones es clave para identificar puntos de entrada para ataques y protegerlos de posibles vulnerabilidades.

# ¿Por qué es Crucial la Ciberseguridad?

---

La ciberseguridad asegura que las telecomunicaciones sean confiables y estén protegidas de interferencias externas. Esto es especialmente relevante en aplicaciones críticas como drones, sistemas de IoT, y redes móviles donde las brechas de seguridad pueden tener graves consecuencias.



- Avances tecnológicos como 5G aumentan la superficie de ataque.
- Creciente dependencia de IoT y redes inalámbricas.
- Necesidad de equilibrar accesibilidad y seguridad.
- Dificultad para monitorear y asegurar entornos altamente dinámicos.
- El futuro de las telecomunicaciones depende de abordar estos retos de forma proactiva.



- Los ataques a telecomunicaciones se clasifican según su propósito:

## 1. Ataques de Interrupción:

1. **Denegación de Servicio (DoS):** Sobrecarga de la red para bloquearla.
2. **Jamming:** Interferencia en señales inalámbricas.

## 2. Ataques de Intercepción:

1. **Eavesdropping:** Espionaje de datos transmitidos.
2. **Sniffing:** Captura de paquetes para analizar información.

## 3. Ataques de Modificación:

1. **Man-in-the-Middle (MitM):** Alteración de comunicaciones en tiempo real.
2. **Spoofing:** Manipulación de identidad de dispositivos.

## 4. Ataques de Ingeniería Social:

1. Explotan la interacción humana para comprometer redes.





- Las telecomunicaciones sostienen sectores como energía, transporte, salud y defensa. Un ataque exitoso podría:
- Interrumpir servicios esenciales (energía o agua).
- Comprometer sistemas de transporte automatizados.
- Poner en riesgo información médica o militar.

La seguridad en telecomunicaciones es crucial para proteger estas infraestructuras.

- Para proteger redes de telecomunicaciones, se han establecido estándares y normativas:
- **ISO/IEC 27001:** Gestión de la seguridad de la información.
- **NIST SP 800-53:** Controles de seguridad en telecomunicaciones.
- **Regulaciones locales:** Leyes específicas en cada país.  
Estos estándares garantizan la implementación de buenas prácticas y medidas de protección.

- Las redes inalámbricas presentan desafíos únicos:
  - **Cifrado débil o nulo:** Redes abiertas o con WEP/WPA.
  - **Rangos de frecuencia saturados:** 2.4 GHz es muy utilizado.
  - **Movilidad de dispositivos:** Dificulta su monitoreo.
- El uso de protocolos robustos y monitoreo constante es esencial para reducir riesgos.


- La tecnología avanza rápidamente:
  - **5G y Beyond:** Mayor velocidad y menor latencia, pero más puntos vulnerables.
  - **Redes Privadas 5G:** Soluciones específicas para empresas.
  - **Convergencia de IoT y telecomunicaciones:** Más dispositivos conectados, más riesgos.
  - **Post-Quantum Cryptography:** En preparación para amenazas futuras de computación cuántica.
- 

- Para garantizar la seguridad de las telecomunicaciones:
    - 1.Segmentación de Redes:** Separar redes críticas de redes públicas.
    - 2.Cifrado Avanzado:** Uso de WPA3 y VPNs.
    - 3.Monitoreo Continuo:** Identificar anomalías con herramientas como IDS/IPS.
    - 4.Simulaciones de Ataques:** Identificar vulnerabilidades antes que los atacantes.
- 

- La IA se utiliza para:
  - **Análisis predictivo:** Identificación de patrones sospechosos.
  - **Detección de anomalías:** Monitoreo automatizado de redes.
  - **Automatización de respuestas:** Bloqueo de amenazas en tiempo real.
- La IA complementa las estrategias tradicionales, mejorando la eficiencia y capacidad de respuesta.

1. Mirai Botnet (2016): Uso de dispositivos IoT para ataques DDoS masivos.
  2. Ataques GPS Spoofing: Interrupción de navegación en drones y buques.
  3. Operación Aurora: Hackeo dirigido a redes corporativas vía telecomunicaciones.
- Estos casos subrayan la importancia de la seguridad en telecomunicaciones.



- Los drones, también llamados UAV (Vehículos Aéreos No Tripulados), son dispositivos capaces de volar sin intervención directa de un piloto a bordo. Originalmente usados en aplicaciones militares, ahora son esenciales en áreas como logística, agricultura, seguridad y entretenimiento.
  - **Primera generación:** Uso militar.
  - **Actualidad:** Incorporación masiva en sectores comerciales y recreativos.
- 

Un dron típico consta de:

- 1. Controlador de Vuelo:** El "cerebro" que procesa las órdenes y controla los motores.
- 2. Motores y Hélices:** Proporcionan el empuje necesario para volar.
- 3. Batería:** Fuente de energía para todos los componentes.
- 4. Sensores:** Giroscopios, acelerómetros, GPS y cámaras para navegación y estabilidad.
- 5. Sistemas de Comunicación:** WiFi, RF o Bluetooth para interactuar con el controlador.

- Los drones se clasifican según su diseño y propósito:

**1.Multirrotores:** Comunes en fotografía y vigilancia.

**2.De ala fija:** Alta autonomía, usados en agricultura y mapeo.

**3.Híbridos:** Combina multirrotores y ala fija.

**4.Submarinos y terrestres:** Diseñados para operaciones específicas fuera del aire.

- Un dron consta de múltiples componentes que trabajan en conjunto:
  - 1. Controlador de Vuelo (Flight Controller):** Administra la navegación y responde a comandos del piloto.
  - 2. Motores y Hélices:** Generan el empuje y controlan la estabilidad.
  - 3. Baterías:** Alimentan los sistemas electrónicos y motores.
  - 4. Sensores:**
    - 1. Giroscopios y Acelerómetros:** Para estabilización.
    - 2. GPS:** Navegación y rutas autónomas.
    - 3. Cámaras:** Reconocimiento de objetos y mapeo.
  - 5. Módulos de Comunicación:** Transmiten datos y reciben instrucciones.

1. **WiFi:** Transmite video en tiempo real y permite control remoto.
  2. **Radiofrecuencia (RF):** Control mediante controladores remotos dedicados.
  3. **Bluetooth:** Conexiones de corto alcance para configuraciones rápidas.
  4. **GPS:** Permite operaciones autónomas basadas en coordenadas.
  5. **LTE/5G:** Para aplicaciones comerciales avanzadas con cobertura extendida.
- **Nota:** Cada sistema presenta ventajas, pero también posibles vectores de ataque.


- Los drones pueden operar en diversos modos según el nivel de autonomía y control:
  - 1.Manual:** Control total del piloto, requiere experiencia.
  - 2.Asistido:** Sensores y GPS ayudan al operador.
  - 3.Autónomo:** Ruta predefinida sin intervención humana.
  - 4.Retorno Automático (RTH):** Regresa automáticamente a un punto de inicio en caso de pérdida de conexión.


1. Redes no Seguras: Uso de WiFi sin cifrado o con contraseñas débiles.
2. Ataques GPS: Spoofing o interferencia (jamming).
3. Firmware Obsoleto: Exposición a exploits conocidos.
4. Intercepción de Datos: Robos de video o telemetría.
5. Acceso Físico: Manipulación directa del hardware.




1. Espionaje: Robos de datos críticos durante vuelos.
2. Interferencia Operativa: Derribo o control forzado del dron.
3. Daños a Infraestructura: Uso malicioso como herramienta para sabotajes.
4. Privacidad: Intrusión en zonas privadas con cámaras.

La Inteligencia Artificial está revolucionando el uso de drones:

- **Visión Computarizada:** Reconocimiento de objetos y navegación autónoma.
  - **Rutas Inteligentes:** Optimización en tiempo real basada en condiciones del entorno.
  - **Prevención de Colisiones:** Sensores combinados con algoritmos predictivos.
  - **Ciberseguridad Basada en IA:** Detección de ataques en tiempo real.
- 

- 1. Fotografía Aérea:** Cine y mapeo.
  - 2. Agricultura:** Monitoreo de cultivos y fumigación automatizada.
  - 3. Logística:** Amazon Prime Air para entregas rápidas.
  - 4. Seguridad Pública:** Vigilancia de eventos masivos o áreas de difícil acceso.
  - 5. Emergencias:** Búsqueda y rescate en zonas de desastre.
- 

- 1. Uso de Cifrado Fuerte:** WPA3 para WiFi, VPNs en transmisiones LTE.
  - 2. Monitoreo Continuo:** Detectar actividades sospechosas en tiempo real.
  - 3. Actualizaciones de Firmware:** Parchear vulnerabilidades rápidamente.
  - 4. Geocercas:** Restringir áreas de vuelo mediante GPS.
  - 5. Sensores Redundantes:** Mitigar interferencias GPS.
- 


- 1.Drones Autónomos Complejos:** Capaces de operar sin intervención humana.
- 2.Mayor Integración con IoT:** Sincronización con otros dispositivos inteligentes.
- 3.Ciberseguridad Mejorada:** Protocolos más robustos para proteger comunicaciones.
- 4.Normativas Globales:** Reglas para estandarizar el uso seguro de drones.
- 5.Innovaciones en Energía:** Baterías más ligeras y eficientes para mayor autonomía.

- 1.ESP8266:** Módulo WiFi de bajo costo para ataques como deautenticación y spoofing.
- 2.Raspberry Pi:** Computadora de propósito general ideal para configuraciones avanzadas y análisis en campo.
- 3.WiFi Pineapple:** Herramienta de pentesting para redes WiFi.
- 4.SDR (Software Defined Radio):** Analiza y manipula señales RF utilizadas por drones.
- 5.Antenas de Largo Alcance:** Mejora la capacidad de conexión a redes distantes.


- 1.Aircrack-ng:** Suite para auditorías de redes WiFi, como captura de handshakes y ataques de fuerza bruta.
- 2.Wireshark:** Analizador de paquetes para monitorear y descifrar comunicaciones de drones.
- 3.Bettercap:** Plataforma avanzada para ataques MitM y manipulación de redes.
- 4.GQRX y GNURadio:** Software para análisis de señales RF con SDR.
- 5.Firmware Deauther:** Para ESP8266, diseñado para ataques de desautenticación en redes WiFi




- 1.Escaneo de Redes:** Identificar redes utilizadas por drones.
- 2.Captura de Handshakes:** Para ataques de fuerza bruta o descifrado de contraseñas.
- 3.Identificación de Dispositivos Conectados:** Encontrar controladores y nodos activos.
- 4.Detección de Puertos y Servicios:** Análisis de servicios abiertos en drones.

- 1. Interceptación de RF:** Captura de comandos enviados al dron.
  - 2. Análisis de Protocolos RF:** Detección de vulnerabilidades en señales no cifradas.
  - 3. Ataques Jamming:** Interferencia en la comunicación RF.
  - 4. Repetición de Señales (Replay):** Reenvío de comandos capturados.
- 

- 1. Configuración del ESP8266:** Instalación del firmware para ataques de desautenticación.
- 2. Ejecución de Ataques:** Interrupción de la conexión WiFi del dron con su controlador.
- 3. Impacto:** Cómo afecta la operación del dron.
- 4. Limitaciones:** Distancia efectiva y mitigaciones comunes.

- 1. GPS Spoofing:** Enviar señales falsas para alterar la ubicación del dron.
  - 2. Ataques MitM:** Interceptar y modificar comandos entre el dron y el controlador.
  - 3. Inyección de Paquetes:** Introducir comandos no autorizados para controlar el dron.
  - 4. Exfiltración de Datos:** Robo de telemetría o video transmitido.
- 

- 1.Cifrado de Comunicaciones:** WPA3 para WiFi, autenticación fuerte para RF.
  - 2.Sensores Redundantes:** Mitigación de ataques GPS mediante múltiples sistemas de navegación.
  - 3.Firmware Seguro:** Actualizaciones constantes para prevenir exploits.
  - 4.Monitorización Activa:** Detección de interferencias y ataques en tiempo real.
- 


- 1. Uso Avanzado de IA:** Automatización de ataques y defensas.
- 2. Redes MESH para Drones:** Mayor complejidad y resiliencia en comunicaciones.
- 3. Señales Cuánticas:** Posibles mitigaciones a largo plazo.
- 4. Aumento de la Superficie de Ataque:** Convergencia de IoT y drones.

**1. Definición:** Consiste en saturar la red o los sistemas de control del dron, impidiendo su funcionamiento normal.

## **2. Métodos Comunes:**

1. Enviar grandes volúmenes de tráfico a la red WiFi del dron.
2. Sobrecargar el controlador mediante peticiones falsas.

**3. Impacto:** El dron pierde conexión y puede detenerse, aterrizar o volver al punto de origen.





**1.Descripción:** Uso de paquetes de desautenticación para desconectar el dron de su controlador.

**2.Herramientas:**

1. ESP8266 con Deauther.
2. Aircrack-ng.

**3.Proceso:**

1. Identificar la red del dron.
2. Enviar paquetes de desautenticación al controlador o al dron.

**4.Limitaciones:** Necesita proximidad al dron y puede ser mitigado con WPA3.



**1.Descripción:** Enviar señales GPS falsas para alterar la ubicación percibida del dron.

**2.Impacto:**

1. Cambiar la ruta del dron.
2. Hacer que aterrice en una ubicación específica.

**3.Herramientas:**

1. SDR con GNURadio para generar señales falsas.
2. Ataques simples mediante repetición de señales.

**4.Contramedidas:** Uso de GPS redundante y señales cifradas.



## 1.WiFi:

1. Captura de paquetes con Wireshark.
2. Decodificación de transmisiones de video o telemetría.

## 2.RF:

1. SDR para escuchar comandos no cifrados.
2. Replay de comandos capturados para replicar acciones.

**3.Impacto:** Acceso a datos sensibles y control indirecto del dron.

**1.Descripción:** Interceptar y modificar las comunicaciones entre el dron y el controlador.

**2.Ejemplo de Ataques:**

1. Inyección de comandos falsos para alterar el comportamiento del dron.
2. Intercepción de imágenes o video transmitidos.

**3.Herramientas:**

1. Bettercap.
2. Ettercap para inyección de comandos.

**4.Impacto:** Control total o parcial del dron.

**1.Definición:** Introducir comandos no autorizados para manipular el dron.

**2.Método:**

1. Interceptar la comunicación.
2. Inyectar comandos mediante herramientas como Bettercap.

**3.Ejemplo:** Desviar el dron a otra ubicación o modificar su comportamiento en vuelo.

**4.Requisitos:** Acceso a la red WiFi o al protocolo RF del dron




**1.Descripción:** Uso de interferencias para bloquear las comunicaciones del dron.

**2.Tipos de Jamming:**

- 1. WiFi Jamming:** Saturar la frecuencia 2.4 GHz o 5 GHz.
- 2. RF Jamming:** Interrumpir el canal de radiofrecuencia.
- 3. GPS Jamming:** Impedir que el dron reciba señales de navegación.

**3.Impacto:** El dron queda inmovilizado o en modo de emergencia.



- 1.Cifrado Avanzado:** Implementación de WPA3 y autenticación robusta.
  - 2.Detección de Spoofing:** Uso de GPS redundantes y software anti-spoofing.
  - 3.Firmware Seguro:** Actualizaciones constantes para prevenir exploits.
  - 4.Monitoreo de Redes:** Herramientas para identificar ataques en tiempo real.
  - 5.Aislamiento de Sistemas:** Redes segmentadas para drones críticos.
- 

- El ESP8266 es un microcontrolador WiFi de bajo costo y alto rendimiento desarrollado por **Espressif Systems**. Este módulo es ampliamente utilizado en proyectos de IoT (Internet of Things), domótica y ciberseguridad debido a sus capacidades de conectividad y flexibilidad en la programación.
- Características principales:
  - 1.WiFi integrado:** Soporta redes 802.11 b/g/n, ideal para conexiones inalámbricas.
  - 2.CPU:** Procesador de 32 bits Tensilica Xtensa LX106 con una velocidad de hasta 80 MHz o 160 MHz.
  - 3.Memoria:** 64 KB de RAM para instrucciones, 96 KB de RAM para datos y capacidad adicional de almacenamiento flash.
  - 4.Soporte de Protocolo:** TCP/IP, UDP, HTTP, MQTT, y más.
  - 5.GPIOs:** Pines de entrada y salida para conectar sensores, actuadores u otros dispositivos.



## **1.Domótica:**

1. Control de luces, termostatos y otros dispositivos del hogar.
2. Integración con asistentes como Alexa o Google Home.

## **2.IoT:**

1. Recolección y transmisión de datos desde sensores ambientales.
2. Monitoreo remoto en tiempo real.

## **3.Ciberseguridad:**

1. Pruebas de penetración en redes WiFi.
2. Creación de herramientas como jammers, spoofers y escáneres de redes.

## **4.Proyectos Educativos:**

1. Aprendizaje de programación y electrónica.
2. Creación de prototipos económicos.

- 1. Bajo Costo:** Precio accesible comparado con alternativas como Raspberry Pi o Arduino con módulos WiFi.
- 2. Consumo Energético:** Diseñado para proyectos que requieren eficiencia energética.
- 3. Compatibilidad:**
  1. Soporta lenguajes como C, Python (MicroPython) y Lua.
  2. Compatible con entornos como Arduino IDE.
- 4. Comunidad Activa:** Gran cantidad de documentación, proyectos y soporte de desarrolladores.
- 5. Flexibilidad:** Fácilmente programable para diversos casos de uso

## **1. Procesador:**

1. Tensilica Xtensa LX106, altamente optimizado para tareas de conectividad y computación básica.

## **2. Módulo WiFi:**

1. Controlador completo de WiFi integrado.
2. Soporte para modos de operación: Estación, Punto de Acceso (AP) y Mixto.

## **3. Memoria Flash:**

1. Almacenamiento externo (normalmente 1 MB o más) para programas y datos.

## **4. Pines GPIO:**

1. Hasta 17 pines disponibles para control de dispositivos externos.

## **5. ADC (Convertidor Analógico a Digital):**

1. Permite leer señales analógicas (como sensores de voltaje o temperatura).

## **1.Estación (STA):**

1. Conecta el ESP8266 a una red WiFi existente, similar a cómo funciona un dispositivo cliente.
2. Ideal para enviar datos a servidores o plataformas como MQTT.

## **2.Punto de Acceso (AP):**

1. El ESP8266 crea su propia red WiFi, permitiendo que otros dispositivos se conecten.
2. Usado en herramientas como el Deauther para pruebas de seguridad.

## **3.Modos Mixto:**

1. Combina STA y AP para permitir conexiones simultáneas como cliente y servidor.

## **1. Memoria Limitada:**

1. No es adecuado para aplicaciones que requieren procesamiento intensivo.

## **2. Consumo Energético:**

1. Aunque optimizado, el consumo en modo WiFi activo puede ser alto para proyectos con baterías pequeñas.

## **3. Soporte de Frecuencia:**

1. Opera únicamente en la banda de 2.4 GHz, no soporta 5 GHz.

## **4. Seguridad WiFi:**

1. Vulnerable a ataques si no se configuran correctamente las credenciales y cifrados.

## 1.ESP32:

1. Soporta WiFi y Bluetooth.
2. Mayor capacidad de procesamiento y pines adicionales.

## 2.Arduino con Módulo WiFi:

1. Más caro y menos eficiente en tareas de conectividad.

## 3.Raspberry Pi:

1. Potente, pero menos eficiente energéticamente y más caro.
- El ESP8266 destaca por su simplicidad y costo para proyectos específicos de redes WiFi y ciberseguridad.

## **1.Optimización del Código:**

1. Usa bibliotecas ligeras y elimina funciones innecesarias.

## **2.Seguridad:**

1. Implementa cifrado TLS para comunicaciones seguras.
2. Cambia las contraseñas predeterminadas en el firmware.

## **3.Gestión Energética:**

1. Usa modos de ahorro de energía cuando sea posible.

## **4.Actualización del Firmware:**

1. Mantén el firmware actualizado para corregir vulnerabilidades conocidas

## **1.Herramientas de Análisis de Redes:**

1. Escaneo de redes y dispositivos conectados.
2. Monitoreo del tráfico para identificar vulnerabilidades.

## **2.Ataques Simulados:**

1. Ejecución de pruebas como desautenticación, beacon flood y spoofing.

## **3.Creación de Redes Seguras:**

1. Simulación de entornos de prueba para validar contramedidas de seguridad.

## **4.Entrenamiento:**

1. Ideal para enseñar conceptos básicos de ciberseguridad y redes



El **Deauther** es un firmware diseñado específicamente para el **ESP8266**, desarrollado por **Spacehuhn Technologies**, que permite realizar pruebas de seguridad en redes WiFi. Su función principal es realizar ataques de desautenticación, pero también incluye otras herramientas avanzadas para análisis y simulación de redes.

- El Deauther es útil en pruebas de penetración y ciberseguridad para:

## **1. Ataques de Desautenticación:**

1. Desconecta dispositivos específicos de una red WiFi al enviar paquetes de desautenticación.

## **2. Beacon Flood:**

1. Genera puntos de acceso falsos (fake APs) para confundir o atraer dispositivos.

## **3. WiFi Jamming:**

1. Saturación de un canal WiFi para interrumpir comunicaciones.

## **4. Escaneo de Redes:**

1. Identifica redes WiFi disponibles y dispositivos conectados.

## **5. Simulación de Redes No Seguras:**

1. Útil para entrenamiento y validación de configuraciones de seguridad

- 1. Compatibilidad Total:** El Deauther aprovecha al máximo las capacidades del ESP8266, como su conectividad WiFi.
- 2. Bajo Costo:** Ideal para proyectos educativos o pruebas rápidas.
- 3. Portabilidad:** Su tamaño pequeño permite llevarlo a cualquier lugar.
- 4. Simulación Realista:** Reproduce escenarios de ataque reales en entornos controlados

## **1. Ataque de Desautenticación:**

1. Explota la forma en que el estándar 802.11 gestiona las conexiones WiFi.
2. Envía paquetes "deauth" a dispositivos conectados a una red para desconectarlos.

## **2. Creación de Redes Falsas:**

1. Genera puntos de acceso con SSIDs configurados para confundir a los usuarios o recolectar información.

## **3. Escaneo Pasivo:**

1. Monitorea redes y dispositivos sin interactuar directamente con ellos.

**1.ESP8266:** NodeMCU.

**2.Firmware Deauther:** Descargado desde el repositorio oficial ([Spacehuhn](#)  
[GitHub](#)).

**3.Herramientas de Flasheo:**

1. NodeMCU PyFlasher (GUI).
2. Esptool (línea de comandos).

**4.Cable Micro-USB:** Para conectar el ESP8266 a la computadora.

## 1.Preparación:

- Conecta el ESP8266 a la computadora usando un cable micro-USB.
- Asegúrate de que los drivers del ESP8266 estén instalados.

## 2.Descarga del Firmware:

- Ve al repositorio oficial y descarga el archivo .bin más reciente del Deauther.

## 3.Uso de NodeMCU PyFlasher:

- Abre la herramienta y selecciona el puerto COM donde está conectado el ESP8266.
- Carga el archivo .bin del Deauther.
- Inicia el proceso de flasheo.

## 4.Verificación:

- Una vez completado, reinicia el ESP8266.
- Busca una nueva red WiFi llamada "pwned".


## **1. Conexión al Punto de Acceso:**

- Conéctate a la red WiFi creada por el ESP8266 ("pwned").
- Usa la contraseña predeterminada: deauther.

## **2. Acceso a la Interfaz Web:**

- Ingresa 192.168.4.1 en un navegador web.

## **3. Opciones Disponibles:**

- Escaneo de redes.
  - Configuración de ataques de desautenticación y beacon flood.
  - Personalización de SSIDs y canales.
- 

## **1.Pruebas de Seguridad:**

1. Identificar redes con configuraciones débiles.
2. Evaluar la resistencia de dispositivos frente a ataques de desautenticación.

## **2.Simulación de Escenarios de Ataque:**

1. Entrenamiento en entornos controlados.

## **3.Validación de Contramedidas:**

1. Verificar la efectividad de WPA3, VPNs y otras soluciones.



- 1. Autorización:** Solo realizar pruebas en redes con consentimiento.
- 2. Entornos Controlados:** Evitar el uso en redes públicas o privadas sin permiso.
- 3. Propósito Educativo:** Utilizar el Deauther como una herramienta para mejorar la seguridad, no para actividades malintencionadas.

- 1.Rango Limitado:** Depende de la potencia de transmisión del ESP8266.
- 2.Incompatibilidad con Redes Seguras:** No funciona contra WPA3 o redes con autenticación fuerte.
- 3.Interrupciones Temporales:** Los ataques no suelen generar daños permanentes.