

Seguridad y Auditoría Informática

# Unidad 5 - Wireless Security

Guia de trabajos prácticos 5

| Ing. Fernando Boiero | Año 2024 |
| --- | --- |
|  |  |
|  |  |

## 

## 

[**Unidad 5 - Wireless Security 1**](#_cfqubuy74qsf)

[TP WIFI 01 3](#_yfxqb2njntbk)

[TP WIFI 02 3](#_yzbx3qz8qd29)

[TP WIFI 03 3](#_gen0jz2yfpya)

[**Resoluciones 4**](#_k7cb0gw3dxiv)

[TP WIFI 01 4](#_y3e8oj4jhwne)

[TP WIFI 02 8](#_7nl3g0dhelg)

[Introducción 8](#_2mj2c4fji4bh)

[Problemas de Seguridad en WPA3 8](#_24l2hh5xt85q)

[Impacto de las Vulnerabilidades 9](#_ubaotjgf2mbk)

[Soluciones Implementadas 9](#_zi5howj149br)

[Conclusión 9](#_7l25rucwsmhi)

[Referencias 9](#_xlp36rnbs5m6)

[TP WIFI 03 10](#_yb2rzttblugz)

[Ataque DoS por DeAuth 10](#_b7xkrtgzy3wg)

[Ataque WPA2 para claves numéricas de 9 dígitos 12](#_b5lez7a702cs)

[Introducción 12](#_r39zsgnnyfp5)

[Descripción del Ataque de Fuerza Bruta 12](#_2ych3abkw6ri)

[Mecanismo de Explotación 12](#_f9643p11pisn)

[Impacto del Ataque 12](#_o20c7psejxlo)

[Soluciones y Medidas Preventivas 13](#_un5nz1ugq8hn)

[Conclusión 13](#_42ljswm4xdnx)

[Referencias 13](#_lrsol8c7v94h)

[Arquitectura de Honey Pot Wi-Fi para capturar las contraseñas 14](#_a2rsq3c1mycm)

## 

## TP WIFI 01

Elaborar un informe del ataque KRACK en WPA2.

Detallar cómo se logró, su impacto y soluciones.

## TP WIFI 02

Elaborar un informe de los problemas de seguridad que pospusieron la implementación del WPA3 antes de su lanzamiento.

Detallar mecanismo de explotación teórico su impacto y soluciones.

## TP WIFI 03

Realizar estos tres proyectos adjuntando sus capturas y conclusiones:

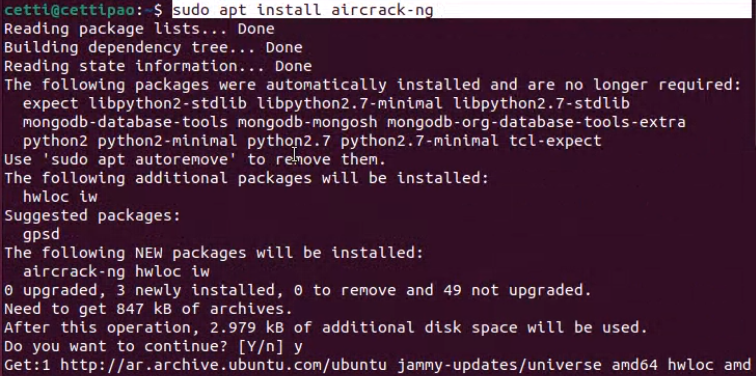
Realizar un ataque de denegación de servicios(DOS) por desautenticación y explicar el paso a paso.

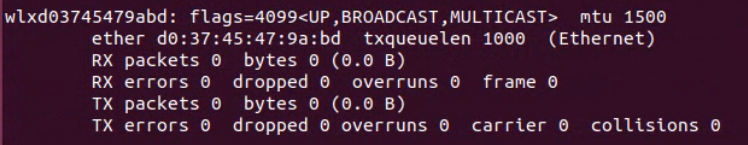
Detallar un ataque WPA2 para un universo de claves numérico de 9 dígitos

Montar una arquitectura de honey pot WIFI y capturar las contraseñas.

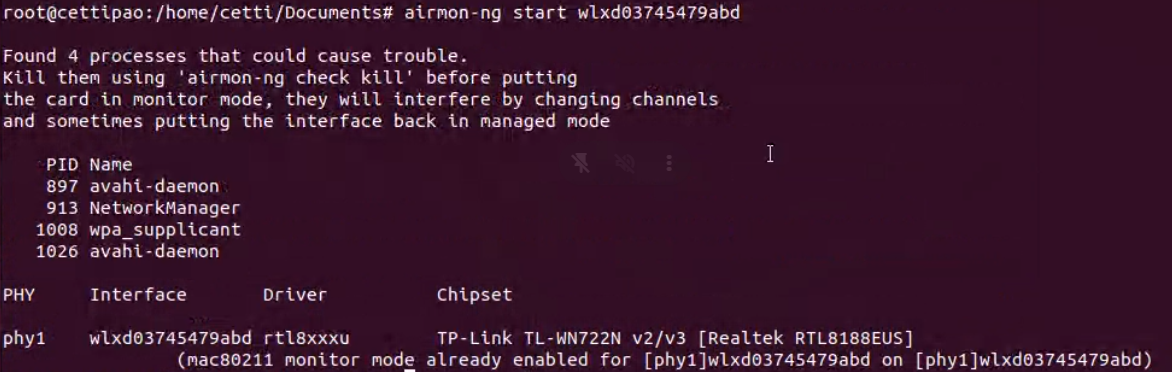
# Resoluciones

## TP WIFI 01

Instalamos la herramienta Aircrack-NG para poder realizar el ataque de KRACK en WPA2.  


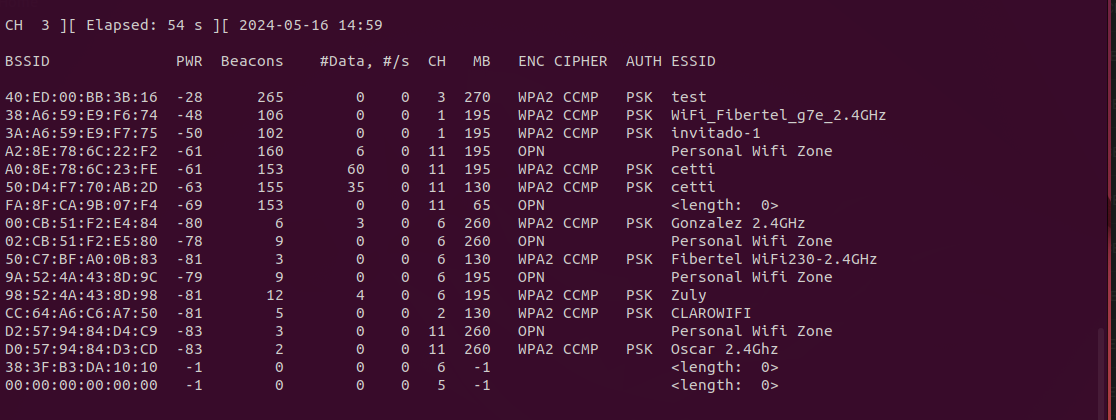
Buscamos con *ifconfig* cual es el nombre de nuestro Wireless Adapter con el que realizaremos el ataque.  


Iniciamos el adaptador inalámbrico en modo MONITOR para poder escanear la red objetivo en busca de dispositivos conectados para poder desautenticarlos y obtener las información que necesitamos.

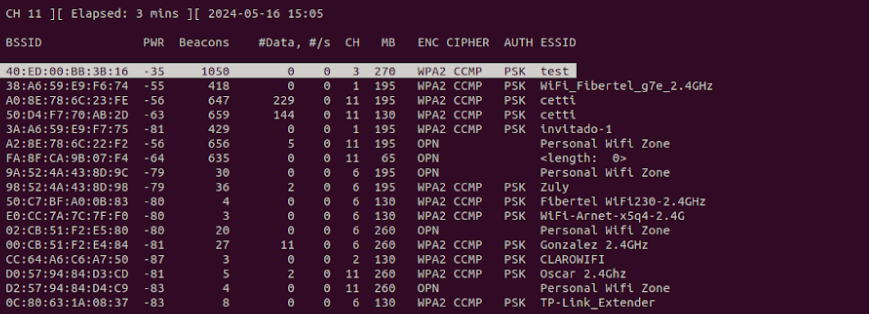


Iniciamos el escaneo de la red utilizando el adaptador previamente configurado como MONITOR.



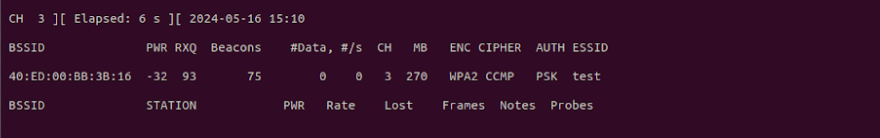


Obtenemos los datos que nos interesan de la red objetivo (ESSID = “*test*”) para ejecutar el comando subsecuente. En este caso el BSSID de la Red y el Channel (CH).

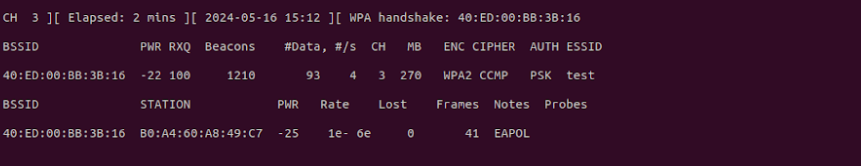


Luego iniciamos el escaneo pero especificando el Canal y la BSSID obtenidos anteriormente, lo que nos va a permitir visualizar las STATIONS (dispositivos) que se conecten o estén conectados a la red objetivo.

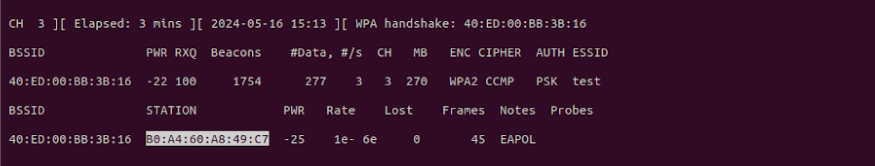




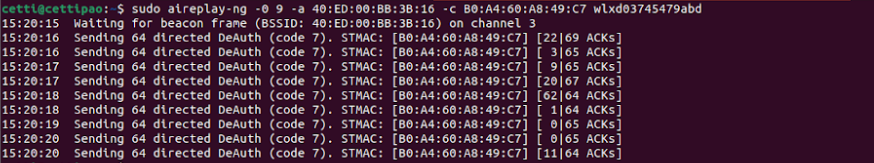
Podemos ver que no hay ningún dispositivo, ya que estamos utilizando una red de prueba nuestra controlada.  
Procedemos a conectarnos con un dispositivo a la red objetivo.



Como podemos ver ahora aparece un dispositivo en la tabla de STATIONS, esta va a ser nuestra víctima.



Utilizamos la MAC Address del dispositivo (STATION) para proceder a atacar al dispositivo víctima con paquetes de DeAuth (desautenticacion).

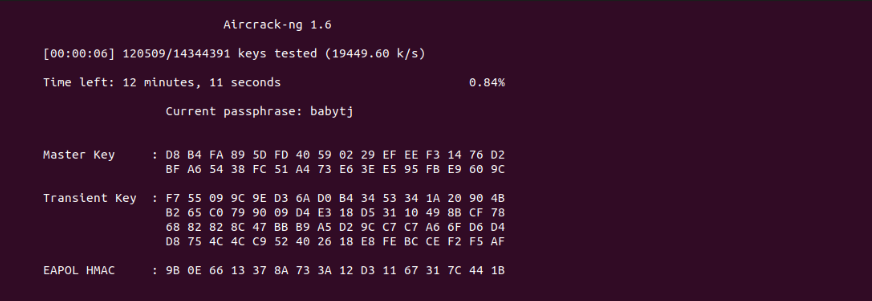


Después de ejecutar este ataque un par de veces logramos lo que necesitamos obtener para poder hacer el ataque de diccionario al sistema de contraseñas de la red con seguridad WPA2, utilizando el diccionario de RockYou más los datos obtenidos del monitoreo a la red objetivo con Airodump-NG (archivos generados con el nombre “auditoria”).

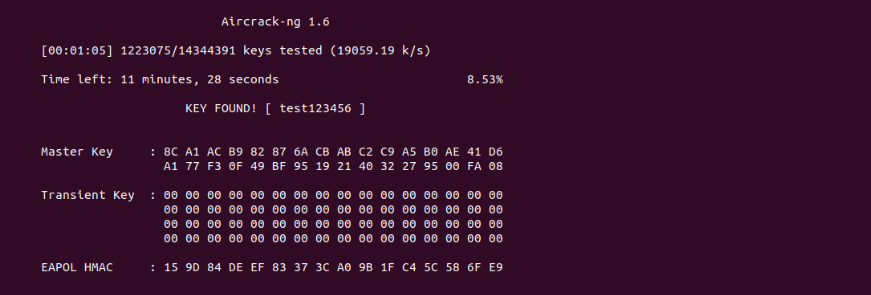
Ya teniendo esto avanzamos con el ataque de diccionario apoyándonos sobre la herramienta Aircrack-NG.



Esperamos a que ejecute…. (Brute forcing passwords)



Y lo logramos!!!



La contraseña era: ***test123456***

## 

## TP WIFI 02

### Introducción

El protocolo WPA3 (Wi-Fi Protected Access 3) fue diseñado para mejorar la seguridad en las redes Wi-Fi, superando las limitaciones de WPA2. Sin embargo, antes de su lanzamiento, se identificaron varios problemas de seguridad que retrasaron su implementación. Este informe analiza estos problemas, los mecanismos teóricos de explotación, su impacto y las soluciones adoptadas.

### Problemas de Seguridad en WPA3

* **Vulnerabilidades Dragonblood**
  + Descripción: Dragonblood es un conjunto de vulnerabilidades en el protocolo Dragonfly, utilizado por WPA3 para establecer conexiones seguras.
  + Mecanismos de Explotación Teóricos:
    - Ataque de Degradación (Downgrade Attack): Los atacantes pueden forzar a un dispositivo a usar el protocolo WPA2, menos seguro, facilitando ataques conocidos.
    - Ataques de Canal Lateral (Side-Channel Attack): A través del análisis de tiempo y caché, los atacantes pueden extraer la contraseña de la red.
  + Impacto: Estas vulnerabilidades permiten a un atacante obtener la contraseña de la red, comprometiendo la seguridad general.
  + Soluciones: Mejoras en la implementación del protocolo Dragonfly, incluyendo protecciones contra ataques de análisis de tiempo y caché​ (Cryptology Eprint)​​ (Mathy Vanhoef Papers)​.
* **Ataques de Reinstalación de Claves (KRACK)**
  + Descripción: Aunque más relevantes para WPA2, los KRACK también plantearon preocupaciones sobre su mitigación en WPA3.
  + Mecanismos de Explotación Teóricos:
    - Un atacante puede forzar la reinstalación de una clave de cifrado en un dispositivo, permitiendo la interceptación y manipulación del tráfico.
  + Impacto: Riesgo de que un atacante descifre y manipule el tráfico de red, comprometiendo la confidencialidad e integridad de los datos.
  + Soluciones: Mejoras en la gestión de claves y actualizaciones de firmware para asegurar que las claves no se reinstalen de manera insegura​ (Mathy Vanhoef Papers)​.
* **Problemas de Compatibilidad hacia Atrás**
  + Descripción: Mantener compatibilidad con dispositivos más antiguos introdujo vulnerabilidades.
  + Mecanismos de Explotación Teóricos:
    - Ataques utilizando dispositivos antiguos con WPA2 como vector para comprometer dispositivos WPA3.
  + Impacto: La seguridad de la red puede verse comprometida a través de dispositivos más antiguos y menos seguros.
  + Soluciones: Estrategias de aislamiento de dispositivos antiguos y mejoras en la gestión de compatibilidad hacia atrás​ (Cryptology Eprint)​.

### Impacto de las Vulnerabilidades

* **Confidencialidad**: Los atacantes podrían interceptar y descifrar datos sensibles.
* **Integridad**: Posibilidad de manipulación del tráfico de red.
* **Disponibilidad**: Ataques de denegación de servicio (DoS) que interrumpen la conectividad de la red.

### Soluciones Implementadas

* **Actualizaciones de Software y Firmware:**
  + Fabricantes lanzaron actualizaciones para abordar las vulnerabilidades, reforzando la seguridad del protocolo Dragonfly y mejorando la gestión de claves.
* **Mejoras en el Protocolo:**
  + Cambios en WPA3 para fortalecer las defensas contra ataques de canal lateral y análisis de tiempo.
  + Mecanismos para mitigar ataques de reinstalación de claves, asegurando que las claves de cifrado no se reinstalen de manera insegura.
* **Educación y Concienciación:**
  + Iniciativas para educar a los usuarios sobre la importancia de mantener sus dispositivos y redes actualizados.

### Conclusión

La implementación del WPA3 se retrasó debido a problemas de seguridad críticos que debían resolverse. Las vulnerabilidades, aunque en muchos casos teóricas, destacaron la necesidad de fortalecer el protocolo para asegurar que las redes Wi-Fi sean robustas frente a atacantes sofisticados. Las soluciones implementadas, incluyendo actualizaciones de software, mejoras en el protocolo y esfuerzos educativos, han sido cruciales para garantizar que WPA3 ofrezca una protección fiable y robusta en entornos de redes Wi-Fi.

### Referencias

* [Dragonblood: Analyzing the Dragonfly Handshake of WPA3 and EAP-pwd - Mathy Vanhoef y Eyal Ronen](https://papers.mathyvanhoef.com/dragonblood.pdf)
* [Dragonblood: Analyzing the Dragonfly Handshake of WPA3 and EAP-pwd - Cryptology ePrint Archive](https://eprint.iacr.org/2019/383)

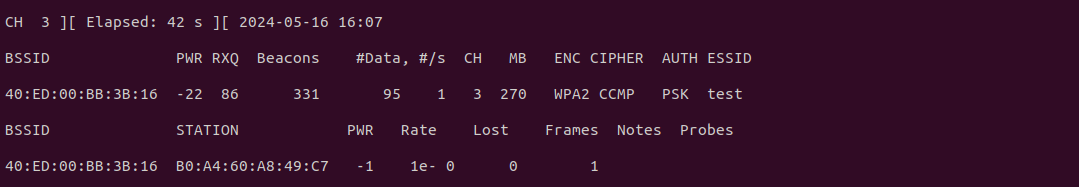
## 

## TP WIFI 03

### Ataque DoS por DeAuth

Para lograr este ataque debemos simplemente dejar andando de manera indefinida el comando de Aireplay-NG que anteriormente utilizamos para el ataque KRACK para desautenticar el dispositivo y obtener los datos que necesitábamos para conseguir la contraseña de la red. En este caso si dejamos los paquetes de desautenticación enviandose permanentemente el dispositivo permanecerá desautenticado, por lo tanto sin acceso al servicio, logrando nuestro objetivo.

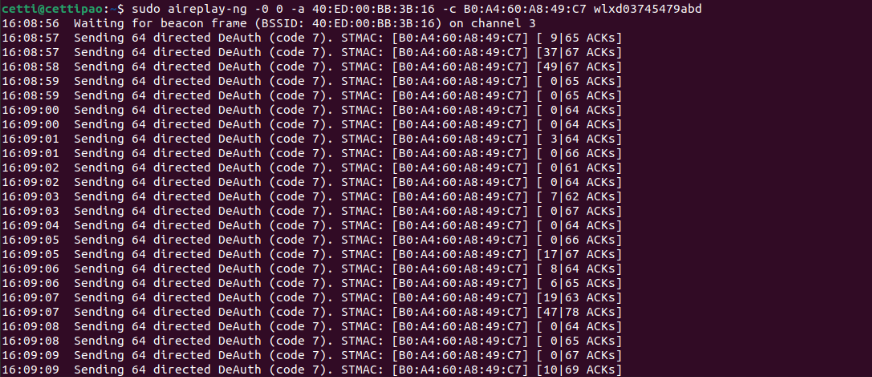
Comenzamos ejecutando el Airodump-NG en la BSSID de nuestra red *test* para monitorear el estado de los paquetes del dispositivo conectado.

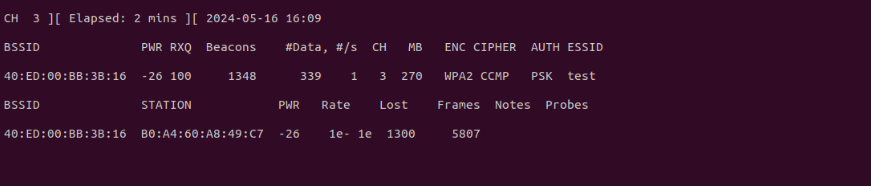


Como se puede observar hay un solo dispositivo conectado (el mismo de la última vez) y este va a ser nuestra víctima.

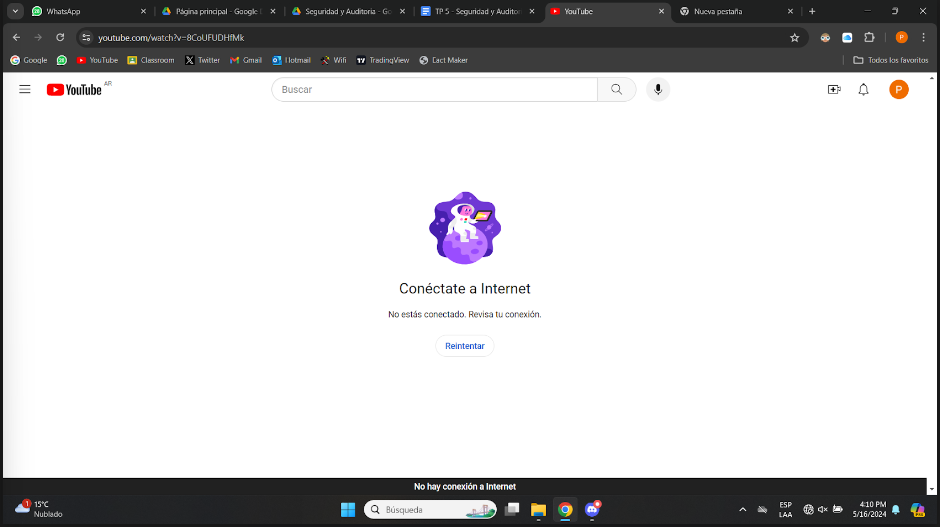
Ahora ejecutamos el Aireplay-NG sobre la víctima.

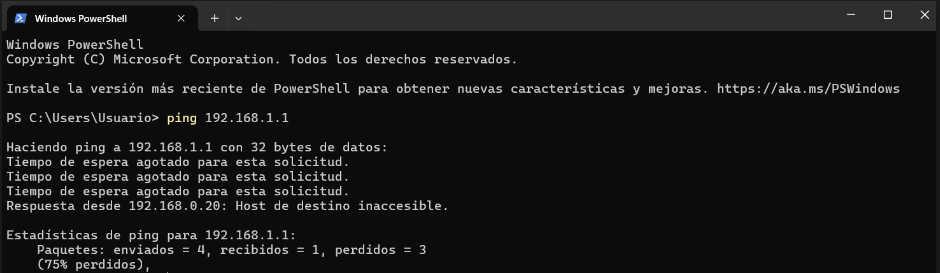




Podemos ver que tras ejecutar el ataque la columna “*Lost*” de paquetes que perdió el dispositivo, empezó teniendo un valor de 0 antes de iniciar y ahora tiene valores incrementales.  


Desde la perspectiva de la computadora objetivo, está perdió conexión total al estar desautenticada del servicio.





Logramos el objetivo!!

### 

### Ataque WPA2 para claves numéricas de 9 dígitos

#### Introducción

WPA2 (Wi-Fi Protected Access II) es un protocolo de seguridad ampliamente utilizado para proteger redes inalámbricas. Sin embargo, es vulnerable a ciertos tipos de ataques, especialmente si las contraseñas utilizadas son débiles o fáciles de adivinar. Un ataque específico es el ataque de fuerza bruta dirigido a un universo de claves numéricas de 9 dígitos. Este informe detalla cómo se puede llevar a cabo este ataque, su impacto y las medidas preventivas.

#### Descripción del Ataque de Fuerza Bruta

* **Recolección de Handshake WPA2:**
  + El primer paso en un ataque de fuerza bruta es capturar el "handshake" (apretón de manos) WPA2, que es el proceso de autenticación entre el cliente y el punto de acceso (AP).
  + Utilizando herramientas como Wireshark, Aircrack-ng o Kismet, un atacante puede interceptar y capturar este handshake.
  + Se debe poner la tarjeta de red en modo monitor para poder escuchar todo el tráfico de la red Wi-Fi.
* **Universo de Claves:**
  + Un universo de claves numéricas de 9 dígitos comprende todas las combinaciones posibles desde 000000000 hasta 999999999.
  + Esto da un total de 1,000,000,000 posibles combinaciones.
* **Ataque de Fuerza Bruta**:
  + Con el handshake capturado, el atacante utiliza una herramienta de fuerza bruta como Hashcat o John the Ripper.
  + Estas herramientas prueban sistemáticamente cada combinación posible del universo de claves numéricas hasta encontrar la correcta.

#### Mecanismo de Explotación

* **Captura del Handshake:**
  + Instrucción:

airodump-ng --bssid [BSSID] --channel [CH] -w [FILE] [INTERFACE]

* + Esta instrucción captura el tráfico específico del punto de acceso de interés.
* **Fuerza Bruta con Hashcat:**
  + Instrucción:

hashcat -m 2500 [handshake\_file.hccapx] -a 3 ?d?d?d?d?d?d?d?d?d

* + “**-m 2500**” indica el modo de WPA-EAPOL-PBKDF2.
  + “**?d**” representa un dígito numérico (0-9).

#### Impacto del Ataque

* **Confidencialidad**: Una vez obtenida la contraseña, el atacante puede acceder a toda la información transmitida a través de la red, incluyendo datos sensibles como correos electrónicos, credenciales de acceso y más.
* **Integridad**: El atacante puede modificar los datos transmitidos, introduciendo potencialmente malware o alterando la información.
* **Disponibilidad**: El atacante puede llevar a cabo ataques de denegación de servicio (DoS) o cambiar la configuración del punto de acceso para desconectar usuarios legítimos.

#### Soluciones y Medidas Preventivas

* **Contraseñas Fuertes:**
  + Utilizar contraseñas largas y complejas que incluyan una combinación de letras, números y caracteres especiales.
  + Evitar el uso de claves numéricas simples o predecibles.
* **Autenticación Multifactor (MFA):**
  + Implementar MFA en la red Wi-Fi para agregar una capa adicional de seguridad.
* **Actualización de Firmware:**
  + Mantener el firmware del router y los dispositivos actualizados para proteger contra vulnerabilidades conocidas.
* **Monitoreo y Detección:**
  + Utilizar sistemas de detección de intrusos (IDS) para monitorear y detectar actividad sospechosa en la red.
* **Redes Invitadas:**
  + Configurar una red separada para invitados que no tenga acceso a la red principal.

#### Conclusión

Los ataques de fuerza bruta contra redes WPA2 utilizando un universo de claves numéricas de 9 dígitos son factibles y pueden comprometer gravemente la seguridad de la red. Implementar contraseñas robustas y medidas de seguridad adicionales es crucial para protegerse contra estos ataques.

#### Referencias

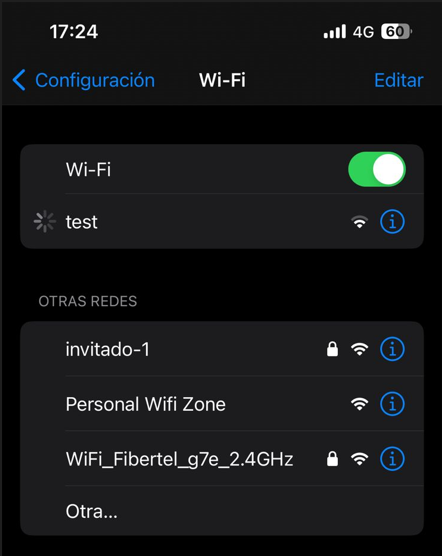
* [Dragonblood: Analyzing the Dragonfly Handshake of WPA3 and EAP-pwd - Cryptology ePrint Archive](https://eprint.iacr.org/2019/383)
* [WPA/WPA2 – Key Reinstallation Attacks (KRACK)](https://www.krackattacks.com/)

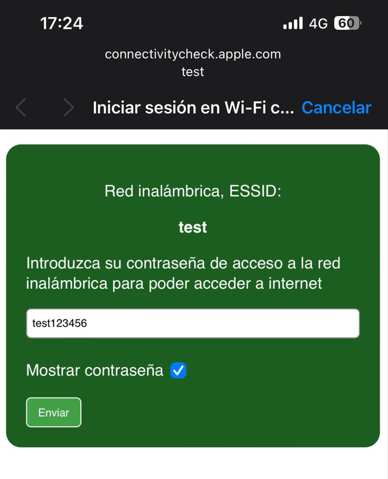
### 

### Arquitectura de Honey Pot Wi-Fi para capturar las contraseñas

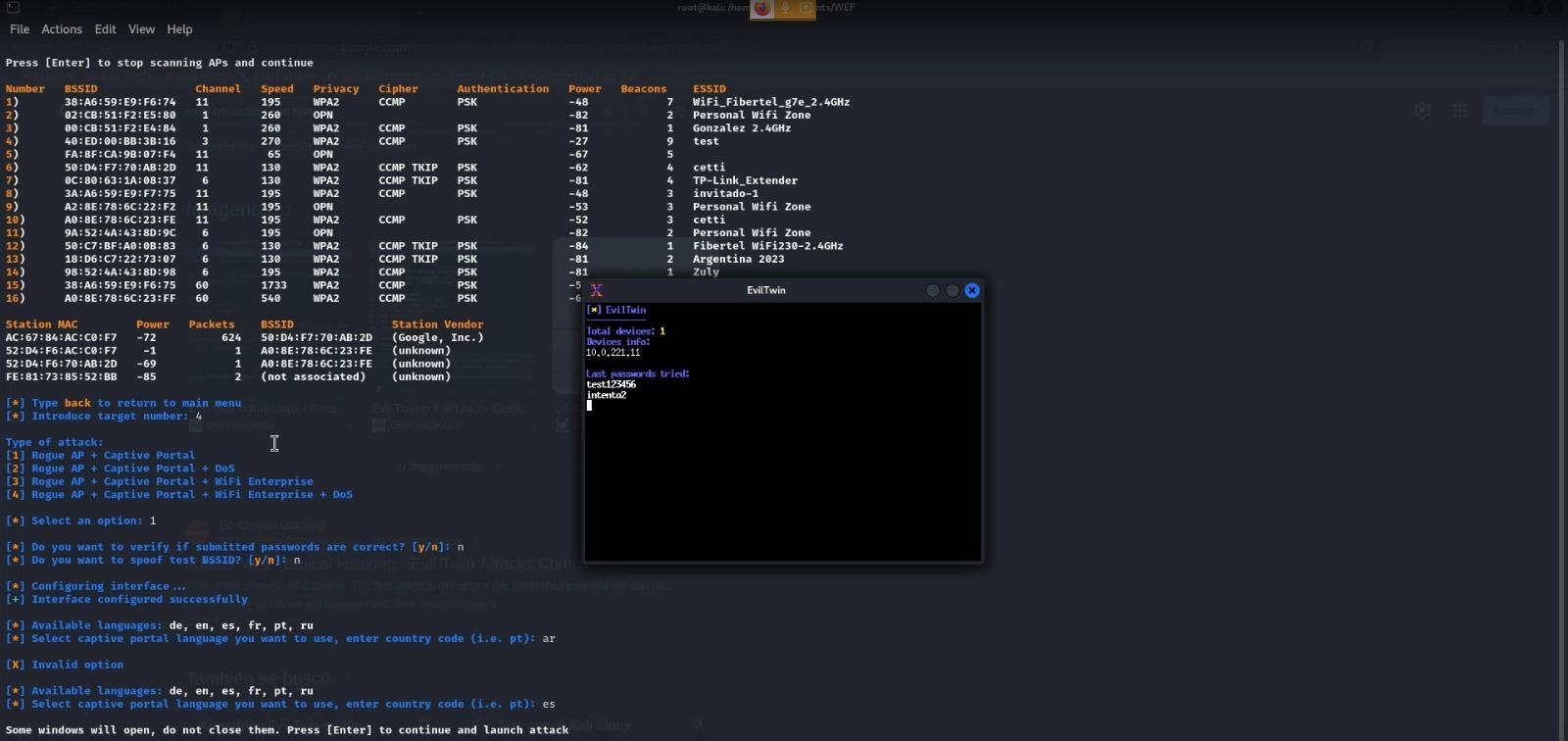
Para llevar a cabo esta actividad, utilizamos el framework ***WEF*** *(WiFi Exploitation Framework)*, que incorpora librerías como *hostapd*. Estas librerías permiten que una tarjeta de interfaz de red funcione como un punto de acceso y servidor de autenticación.

Configuramos y activamos una red Honey Pot Wi-Fi llamada “test”. Esta red pública, al conectarse, redirige a los usuarios a una página de autenticación donde se solicita una contraseña, la cual será capturada. Generalmente, esta red adopta el nombre de una red existente cuyo acceso estamos intentando obtener.











Lo logramos! Obtuvimos la contraseña “***test123456***” que un usuario utilizó para intentar acceder a nuestra red gemela.