¿Estamos seguros en una red WiFi?

Jesús Rodríguez Heras
Juan Pedro Rodríguez Gracia

8 de mayo de 2018

Índice

WPA2-PSK

¿Qué es WPA2-PSK?

Es un protocolo de seguridad que cifra los mensajes en las redes inalámbricas (Wi-Fi) para permitir comunicaciones seguras.

Espionaje en red WPA2-PSK

Se nos presentan dos situaciones:

1. Conocemos la passphrase (contraseña WiFi).
2. No conocemos la passphrase (contraseña WiFi).

Espionaje en red WPA2-PSK

Se nos presentan dos situaciones:

1. **Conocemos la passphrase.**
2. No conocemos la passphrase.

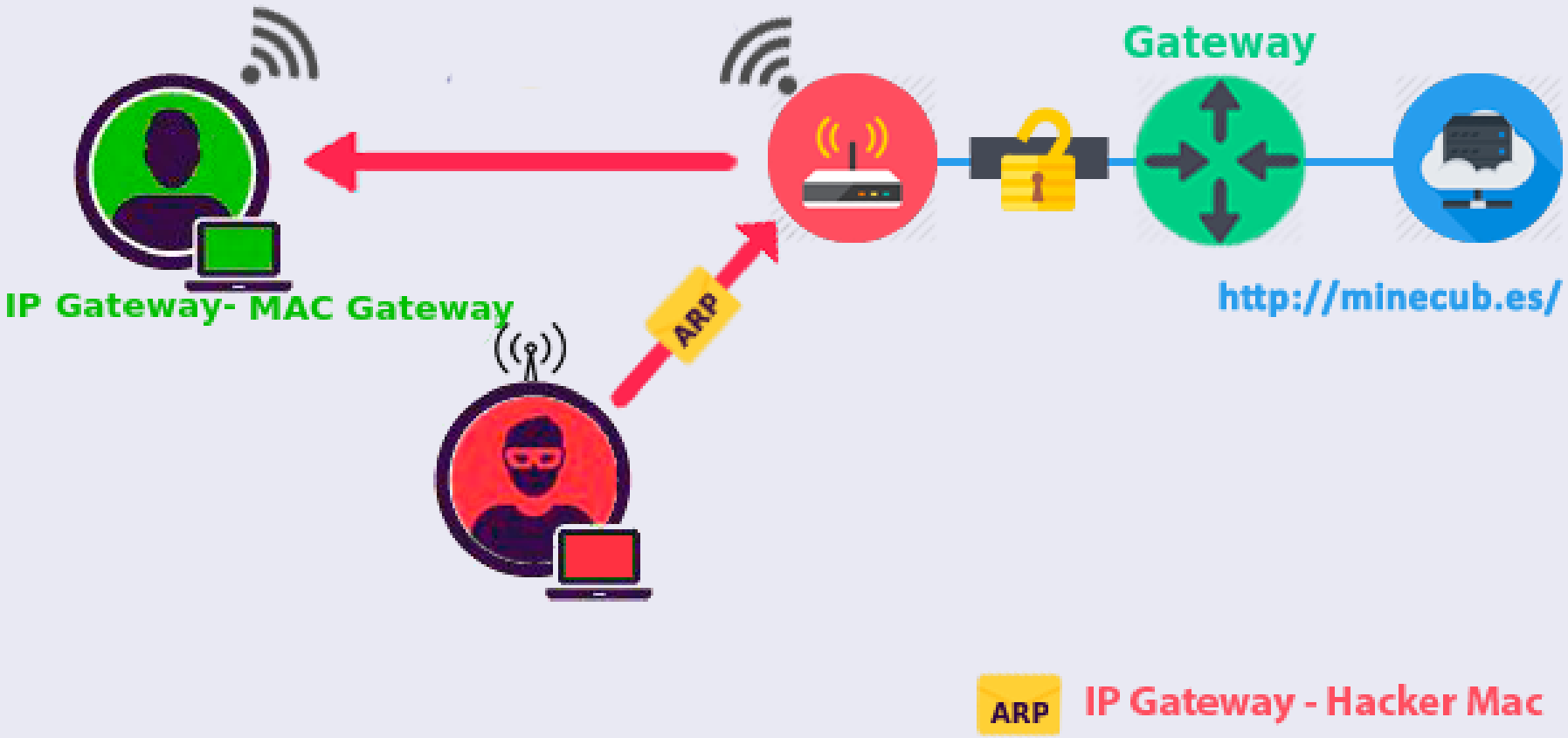
Espionaje en red WPA2-PSK conociendo la passphrase

ARP Poisoning

Es un ataque en el cual se busca engañar a un dispositivo modificando su tabla ARP. En concreto en nuestro ataque buscamos engañar a la victima para poder recibir el tráfico.

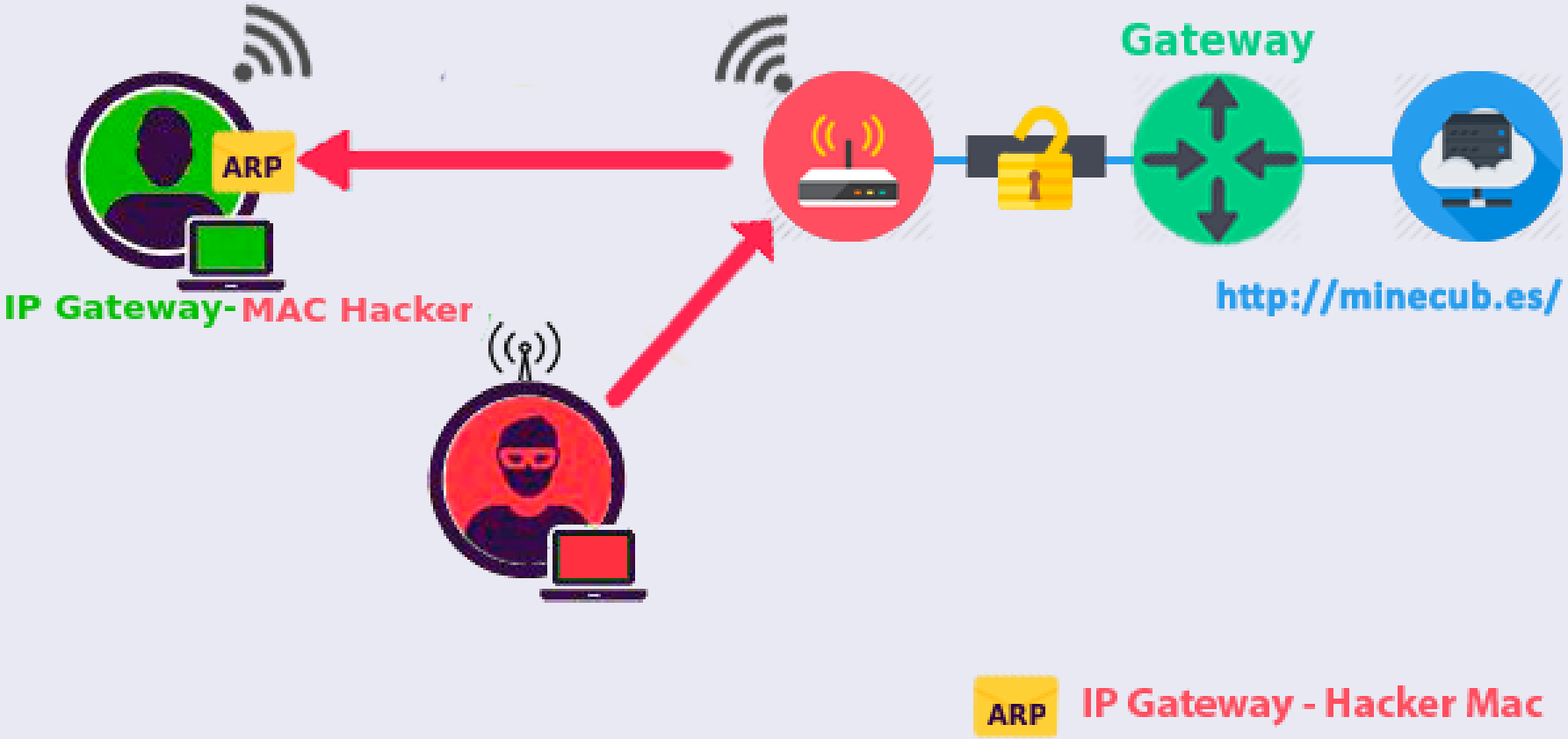
ARP Poisoning

Paso 1. ARP Replay para envenenar la tabla ARP de la víctima



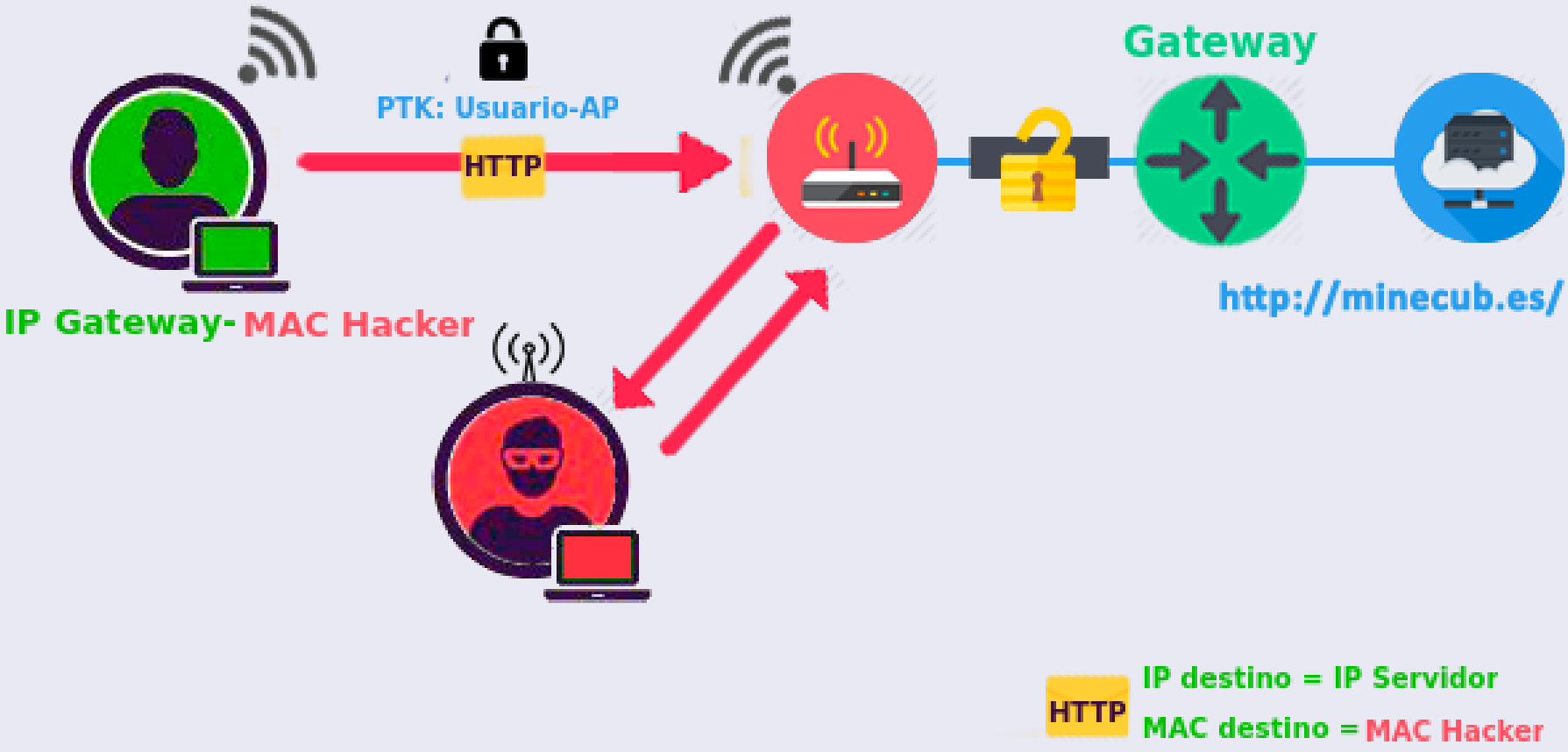
ARP Poisoning

Paso 2. La víctima modifica su tabla ARP



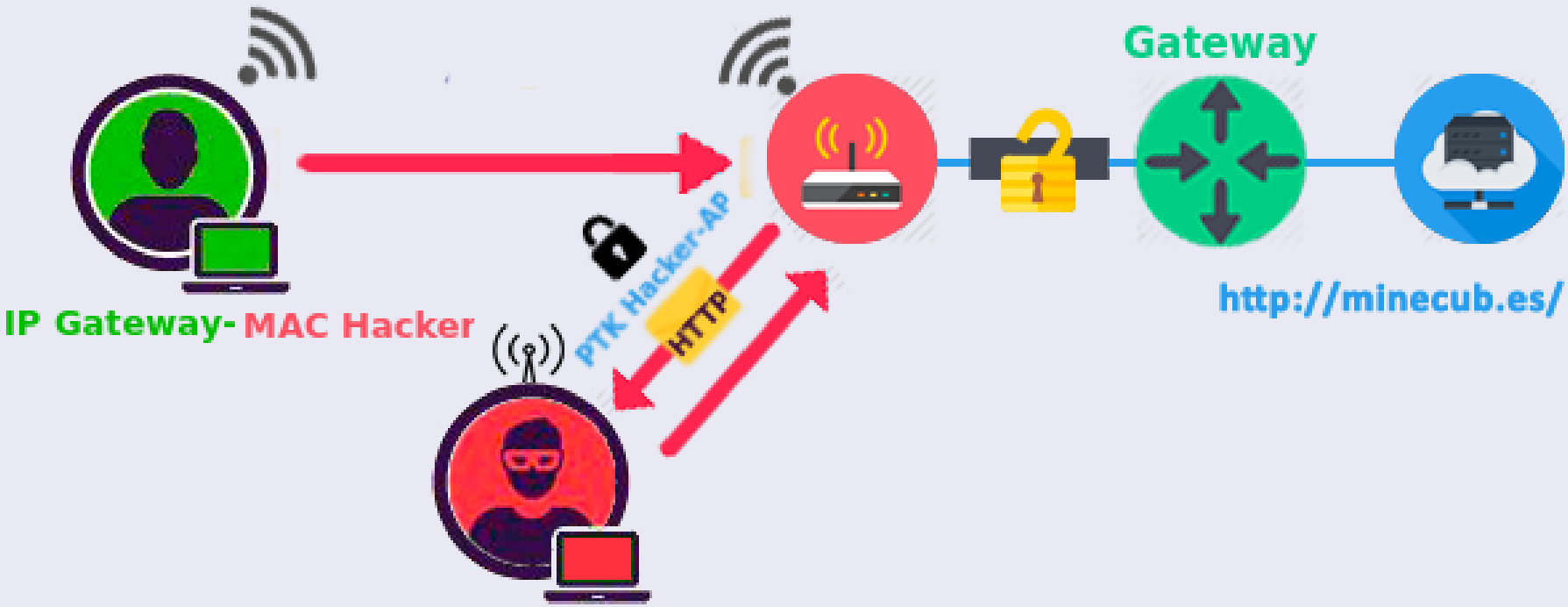
ARP Poisoning

Paso 3. La víctima lanza una solicitud HTTP



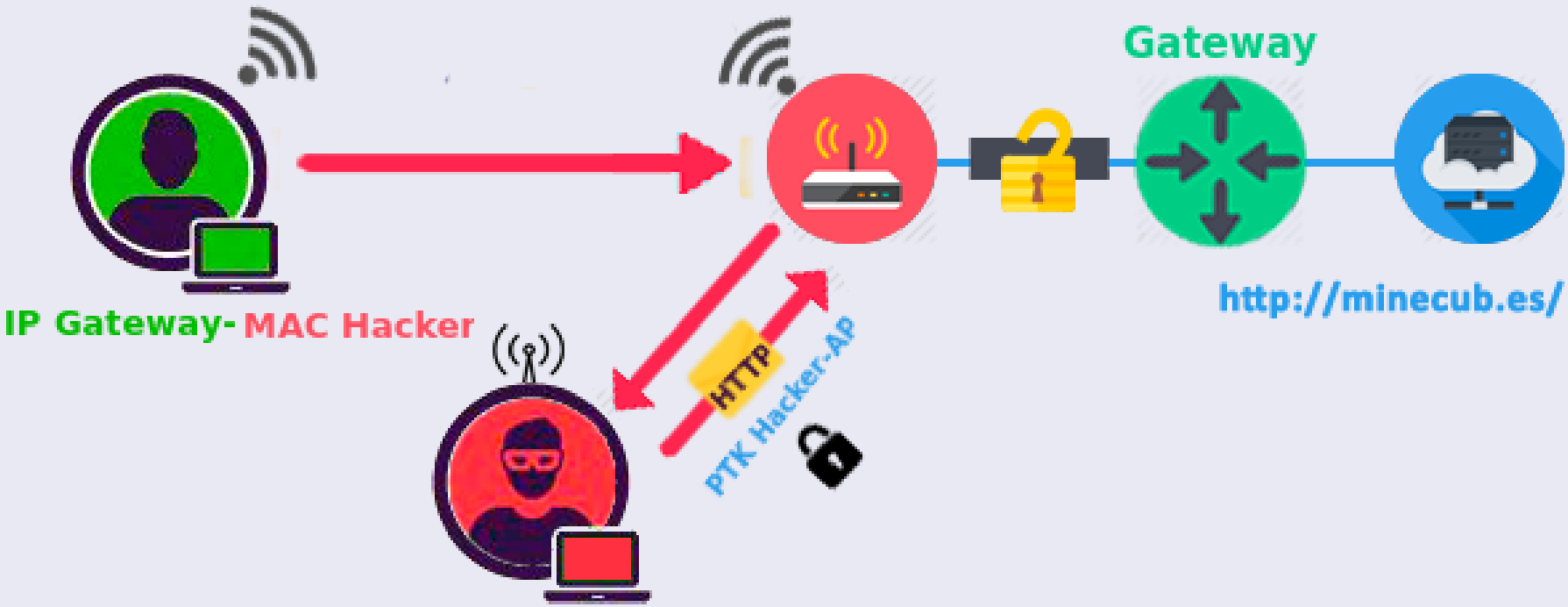
ARP Poisoning

Paso 4. El AP redirecciona el paquete a la MAC del hacker



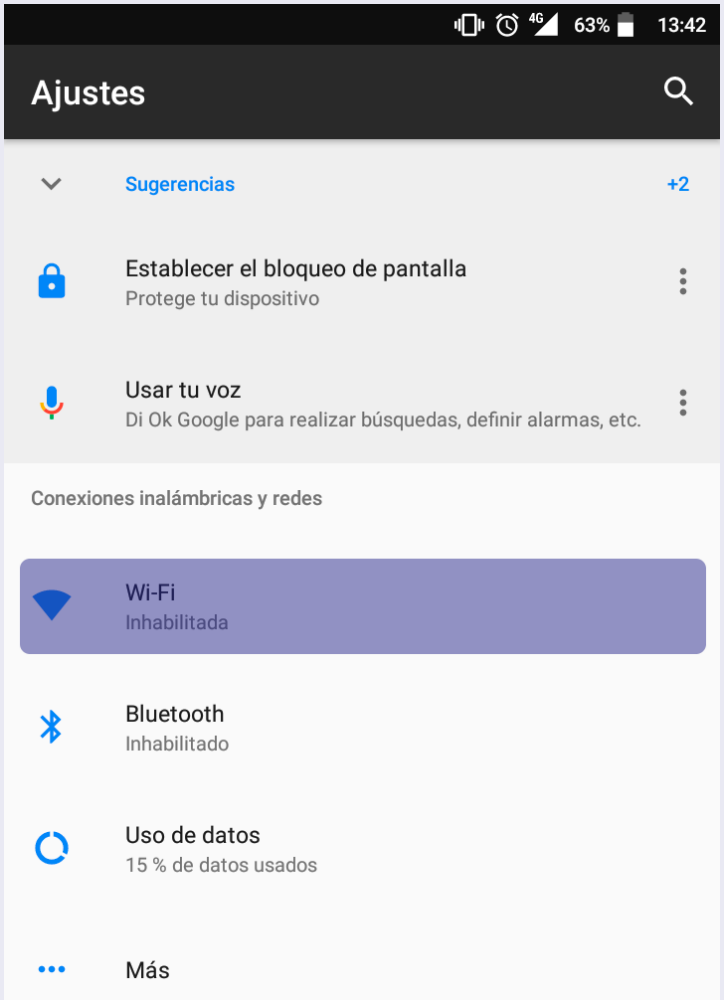
ARP Poisoning

Paso 5. El hacker lee y envía el paquete al destinatario legítimo

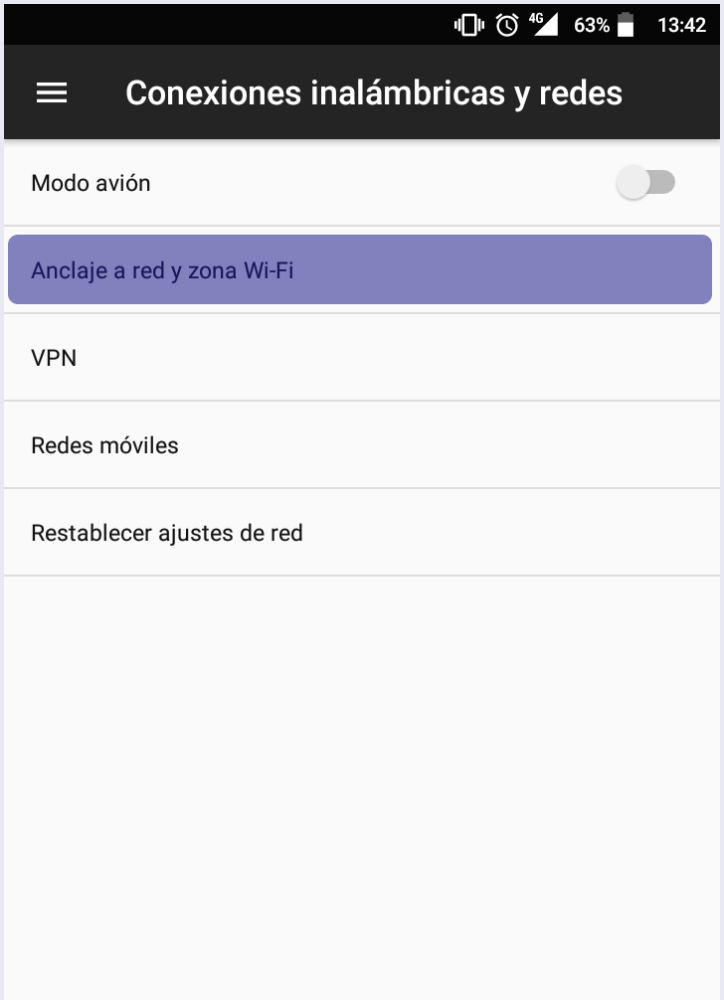


Ejemplo con Ettercap en red segura

Paso 1

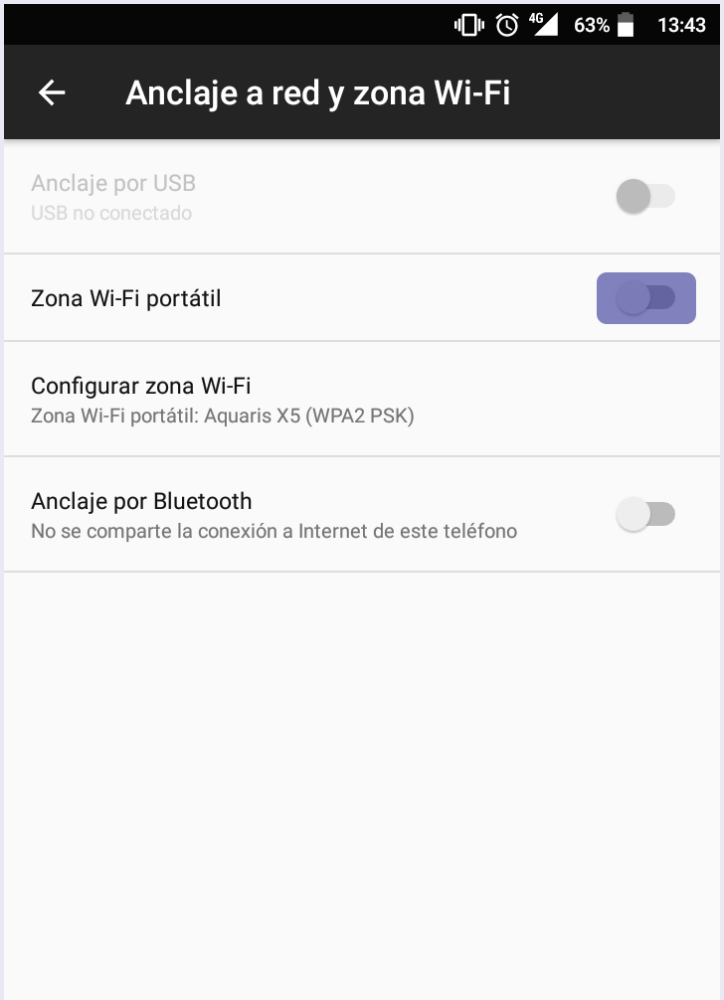


Paso 2

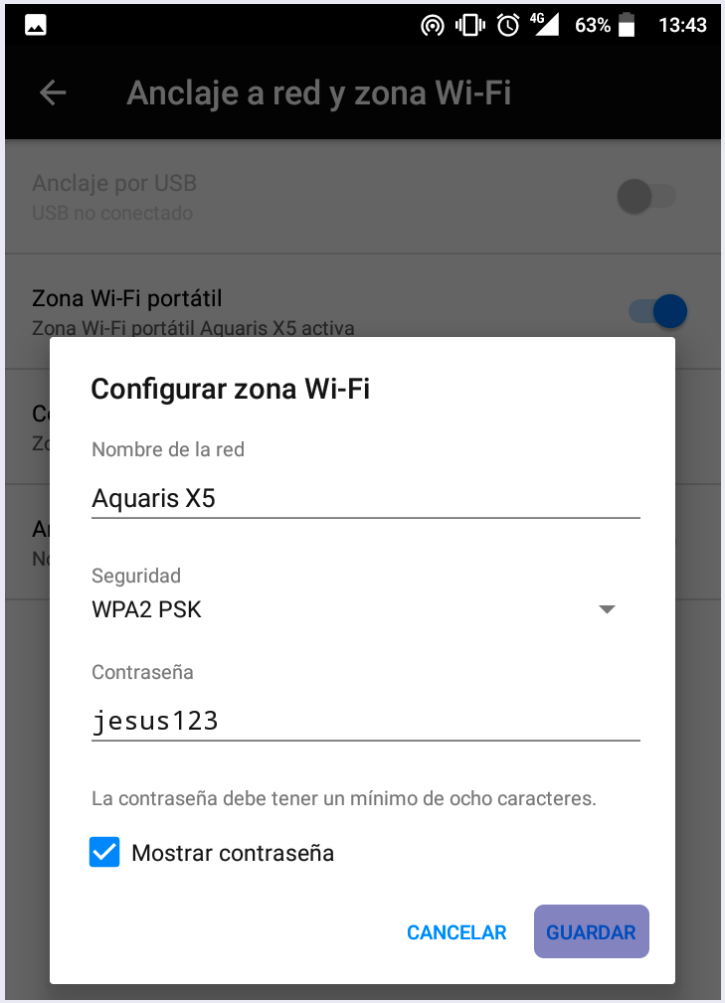


Ejemplo con Ettercap en red segura

Paso 3

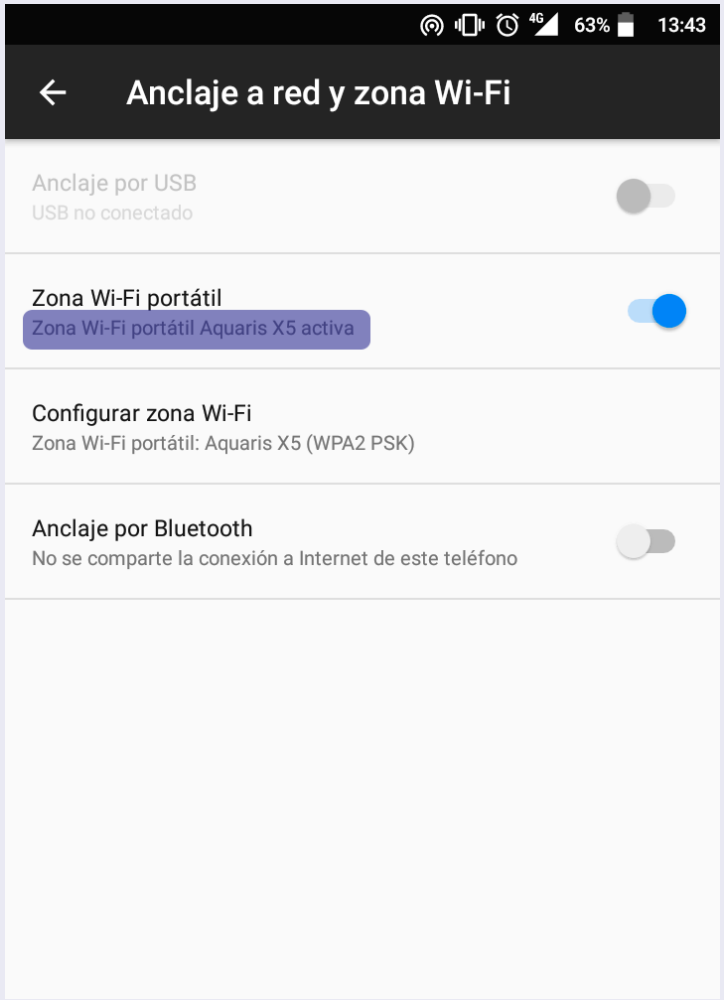


Paso 4



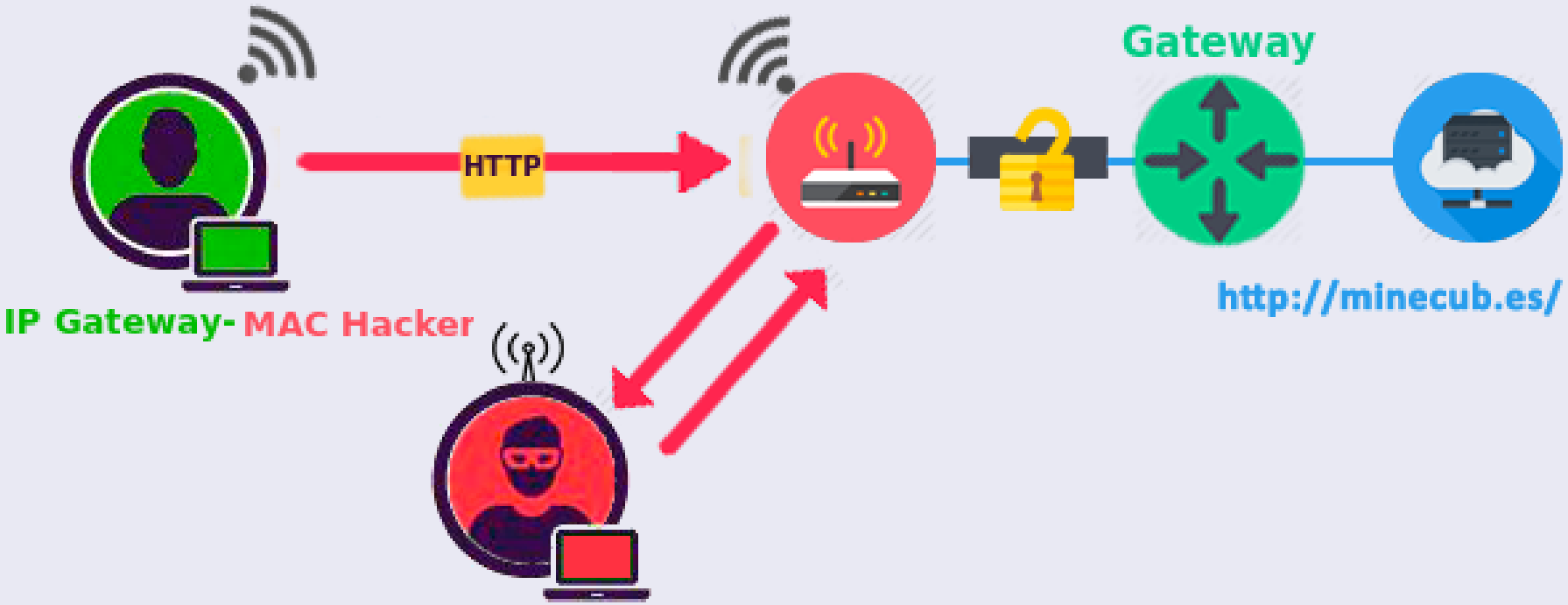
Ejemplo con Ettercap en red segura

Paso 5. Red segura



Ejemplo con Ettercap en red segura

Escenario



¿Qué es HTTPS?

Definición

Es un protocolo de aplicación basado en el protocolo HTTP, destinado a la transferencia segura de datos de Hipertexto, es decir, es la versión segura de HTTP.

¿Cómo funciona?

El sistema HTTPS utiliza un cifrado basado en SSL/TLS para crear un canal cifrado (cuyo nivel de cifrado depende del servidor remoto y del navegador utilizado por el cliente). De este modo se consigue que la información sensible no pueda ser usada por un atacante que haya conseguido interceptar la transferencia de datos de la conexión, ya que lo único que obtendrá será un flujo de datos cifrados que le resultará imposible de descifrar.

Espionaje en red WPA2-PSK

Se nos presentan dos situaciones:

1. Conocemos la passphrase.
2. **No conocemos la passphrase.**

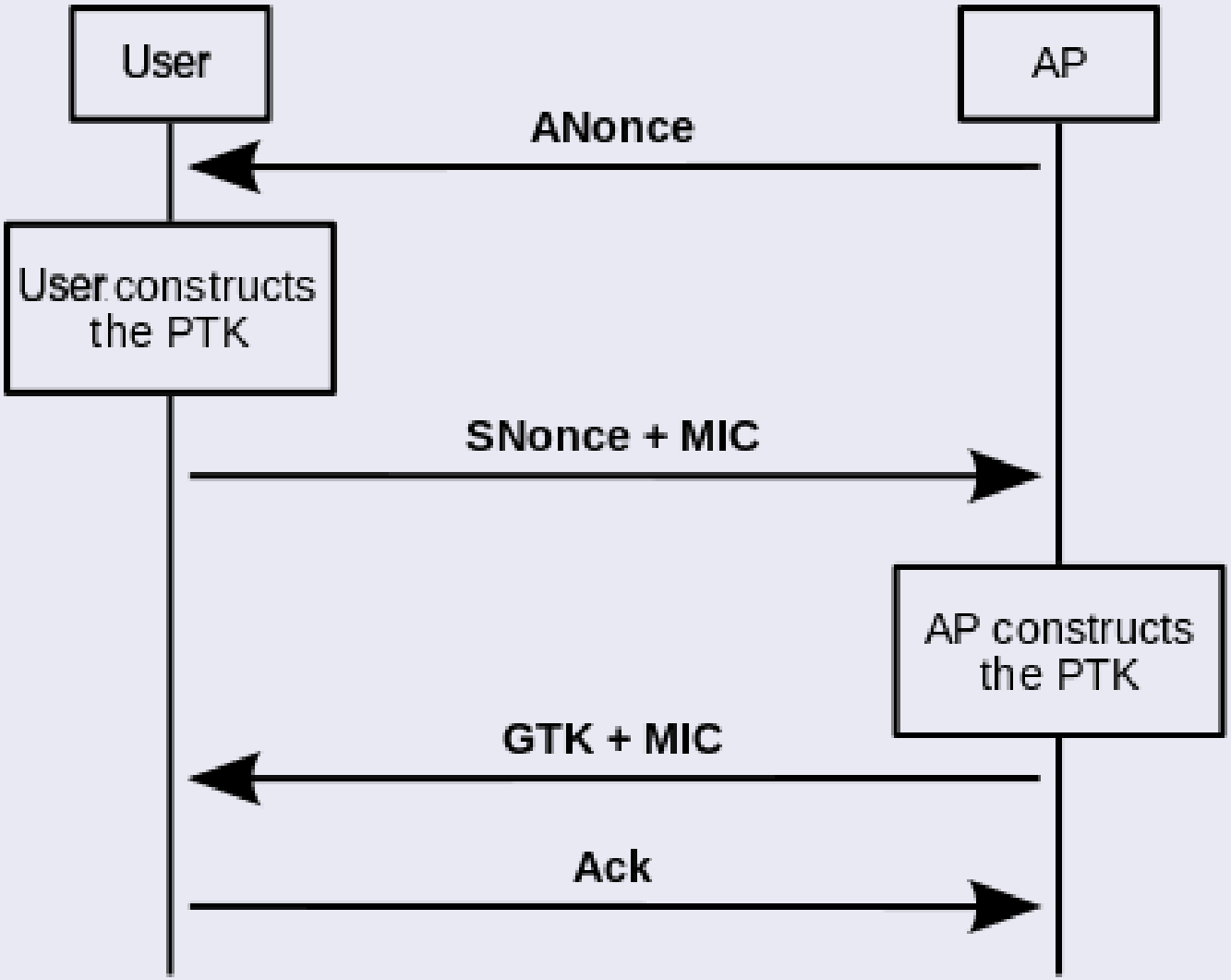
Espionaje en red WPA2-PSK sin conocer la passphrase

KRACK

Key Reinstallation Attack: Se basa en forzar el reuso del SNonce de tal forma que se puedan desencriptar los datos. No es necesario el conocimiento de la clave Wi-Fi.

Espionaje en red WPA2-PSK sin conocer la passphrase

Saludo de 4 vías de WPA2-PSK



Espionaje en red WPA2-PSK sin conocer la passphrase

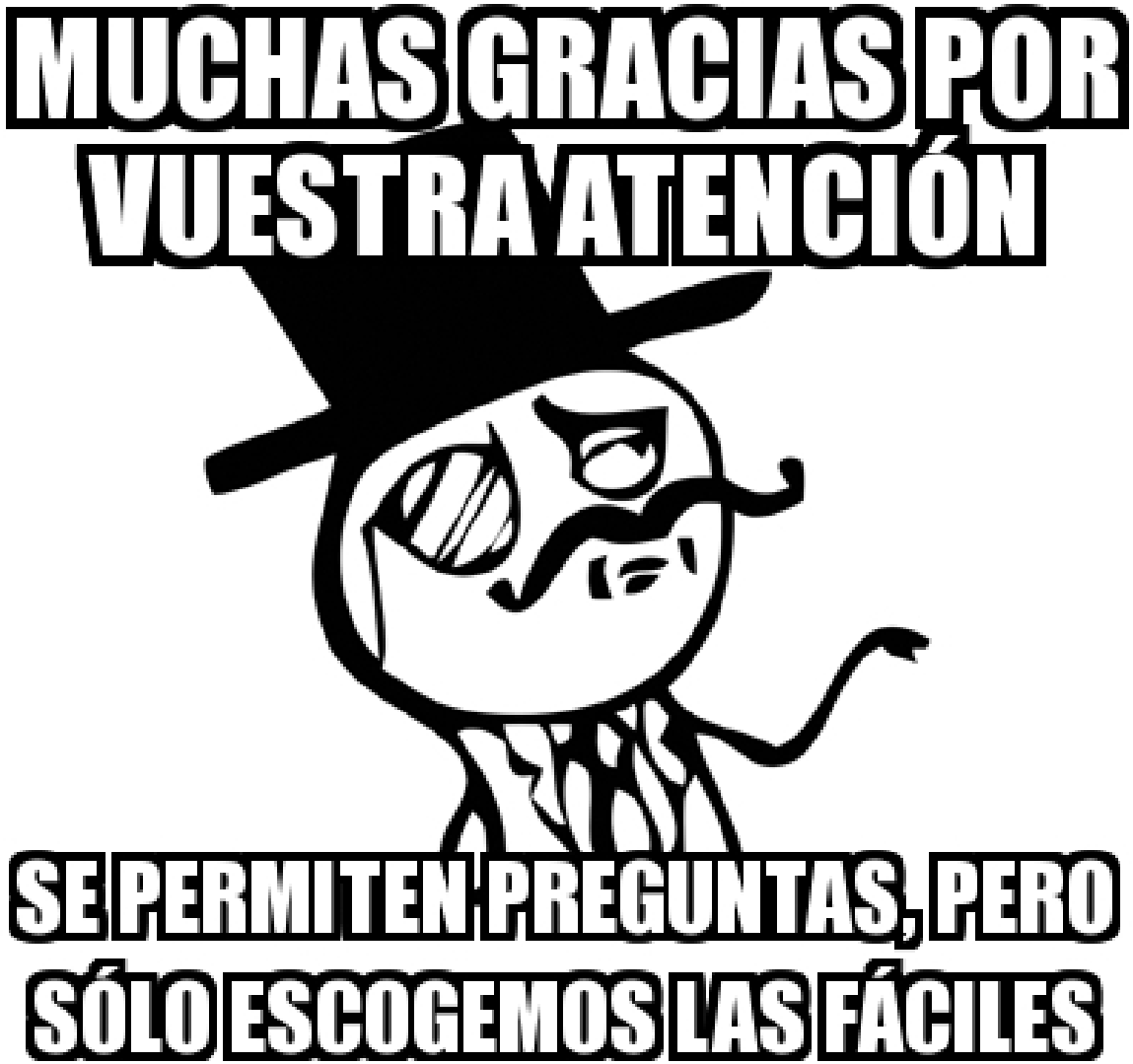
Recursos a usar en KRACK

- Rogue-AP.
- Man-in-the-middle.
- Script KRACK.
- SSLStrip.
- Un sniffer.

Paso a paso

1. Montamos un Rogue-AP.
2. Preparamos el Man-in-the-middle.
3. Ordenamos un cambio de canal.
4. Activamos el script KRACK.
5. Abrimos el sniffer.

Gracias


MUCHAS GRACIAS POR VUESTRA ATENCIÓN
SE PERMITEN PREGUNTAS, PERO SÓLO ESCOGEMOS LAS FÁCILES