Cómo disfrazarse de Access Point

Franco Lanzillotta | Felipe Evans

¡Advertencia!

Este artículo es sólo para fines educativos. Cualquier acción o actividad relacionada con este material es bajo su exclusiva responsabilidad.

Índice

- ¿Qué es un Access Point?
- Rogue AP y Evil Twin
- Búsqueda de AP
  - Búsqueda activa: Beacon Frame
  - Búsqueda pasiva: Probe Request/Response
- Conexión con un AP
  - Autenticación y Asociación
  - Dynamic Host Configuration Protocol (DHCP)
  - Deasociación y Deautenticación
- Ejemplos prácticos

¿Qué es un Access Point?

¿Qué es un Access Point?

Un Access Point (AP) es un dispositivo de red que permite a otros dispositivos conectarse a una red de manera inalámbrica a través de Wi-Fi.

Rogue AP y Evil Twin

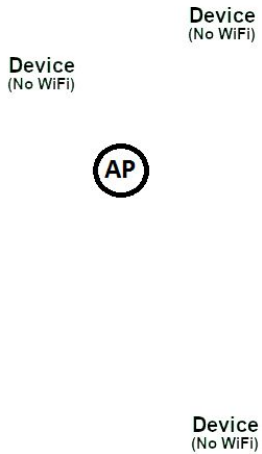
Rogue AP y Evil Twin

Un **Rogue AP** es aquel que ha sido instalado en una red sin una autorización explícita del administrador de la red.

Un **Evil Twin** o **Fake AP** es un dispositivo que simula ser un AP conocido.

Búsqueda de AP

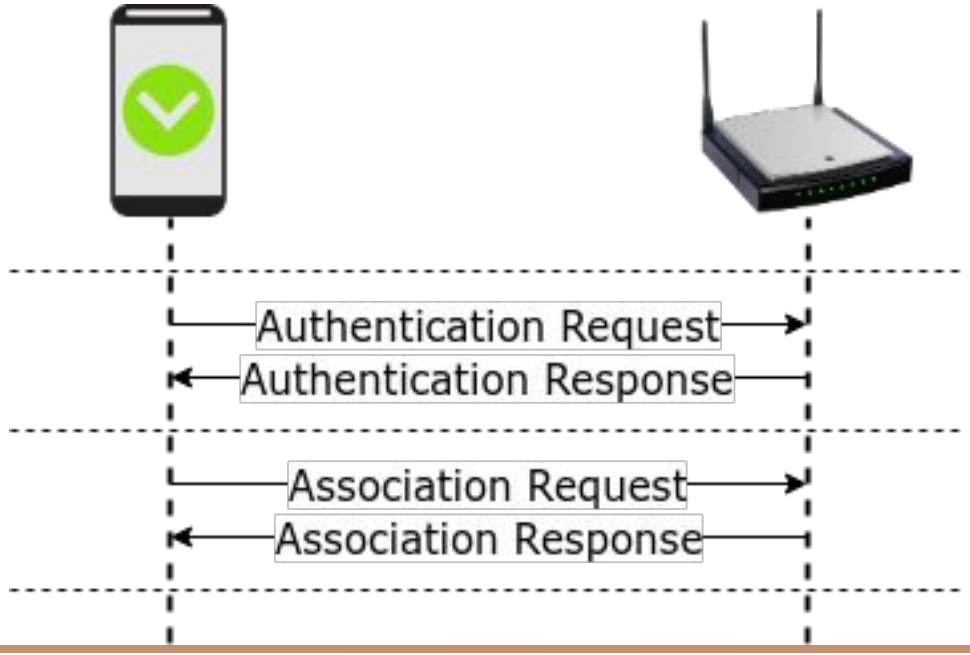
Búsqueda pasiva: Beacon Frame



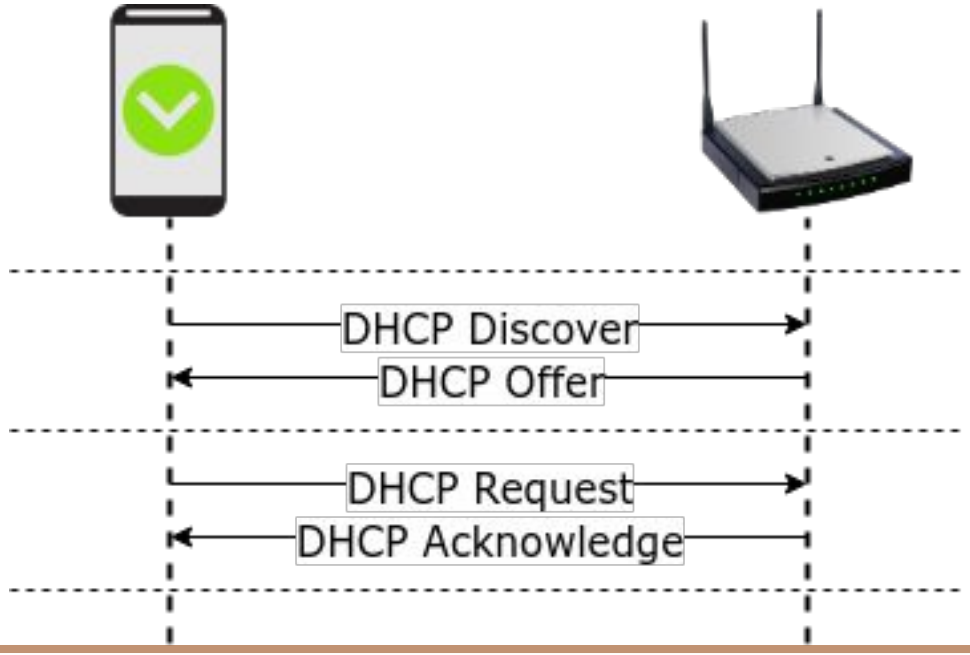
Búsqueda activa: Probe Request/Response

Conexión con un AP

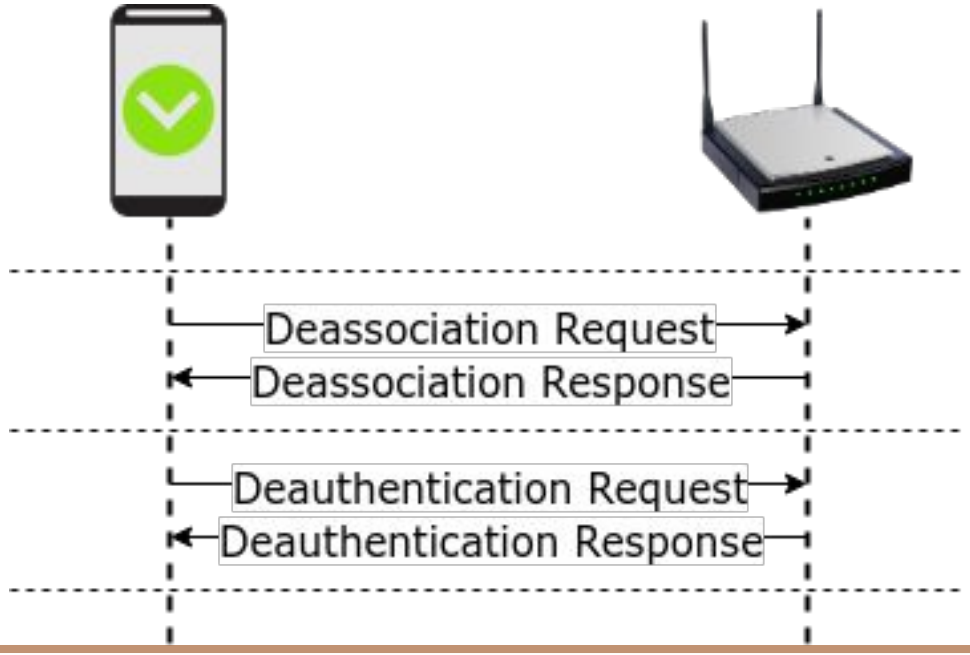
Autenticación y Asociación



Dynamic Host Configuration Protocol (DHCP)



Deasociación y Deautenticación



Ejemplos prácticos

Ejemplos prácticos: Herramientas

wifiphisher

python™

El material se encuentra disponible en:

https://github.com/francolanzi/FakeAP

¡Muchas gracias!

¿Preguntas?