Wardriving armando y aprendiendo de las señales RF (Wi-FI, BLE, IoT)

Por: Adrian González (d3vnullv01d)

About me

- Egresado del IPN
- Ingeniero de Software
- Aprendiz y apasionado de romper cosas y aplicaciones
- Aprendiz en todo experto en lo que caiga

Contenido

Motivación

¿Qué es el wardriving?

¿Qué se necesito para hacerlo?

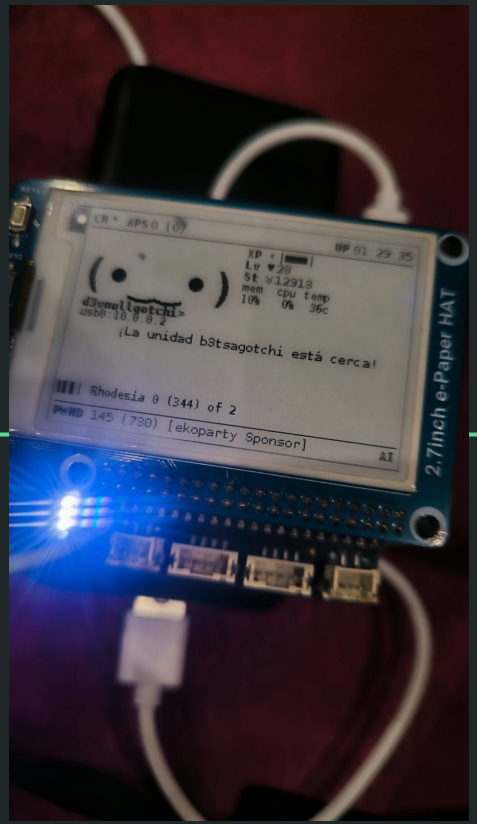
Tipos de wardriving

Demo

Disclaimer

La información y demo es meramente con fines educativos para la creación de espacios de aprendizaje de redes inalámbricas y de dispositivos que usan alguna radio frecuencia, toda información de la demo mostrada será eliminada.

Motivaciones



¿Qué es el wardriving?

El término procede de la película de 1983 *WarGames*. En la película, el personaje interpretado por Matthew Broderick lleva a cabo una actividad llamada marcación de guerra, que consiste en usar una computadora para marcar varios números de teléfono con el fin de identificar un módem que funcione.

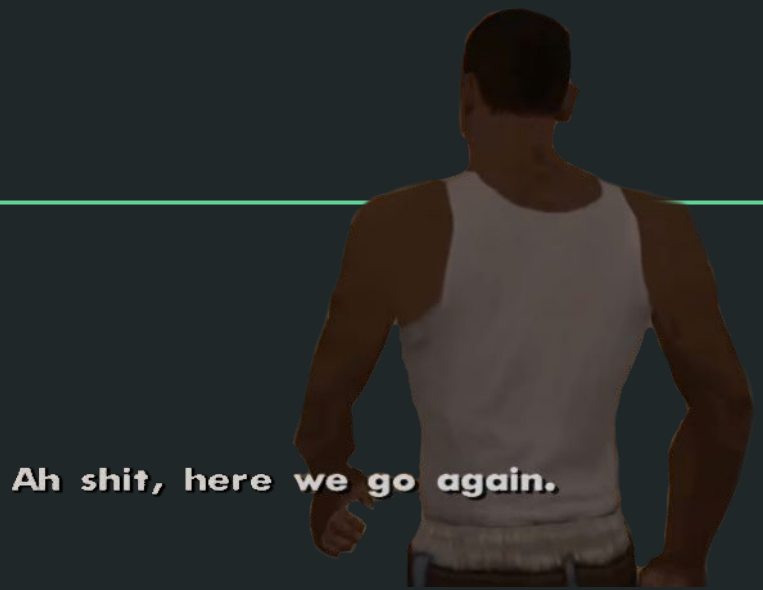
En ciberseguridad, el "wardriving" es el acto de buscar redes y actualmente se incluyen la búsqueda de dispositivos que emitan alguna radio frecuencia. (BLE, IoT, Telefonía, etc)

Director: John Badham

¿Que necesito para hacer wardriving?

- Hardware compatible con la tecnología / Equipo de computo
- Almacenamiento
- Módulo GPS
- Ganas de conocer cómo funciona tu hardware y el cómo interaccionan con dicha tecnología
- (Y lo más importante $$$)

Tipos de Wardriving



Wi-FI

Datos importantes que se pueden recopilar:

- MAC/BSSID (Basic Service Set ID)
- SSID (Service Set ID)
- Tipo de Banda (2.4GHz, 5GHz, 6GHz)
- Canal (hasta 14 en 2.4, 25 en 5, 59 en 6)
- Tipo de autenticación (WEP, WPA, etc)
- RSSI (Received Signal Strength Indicator)

Para más aspectos técnicos con dicha tecnología revisar estándar IEEE 802.11 a, b, ac, ax

BLE / Bluetooth

Datos importantes que se pueden recopilar:

- MAC / Random Address
- Canal
- RSSI
- Local Name

Para verificar más aspectos técnicos revisar página oficial de Bluetooth dependiendo sus la versión de interés.

IoT (Zigbee/Thread)

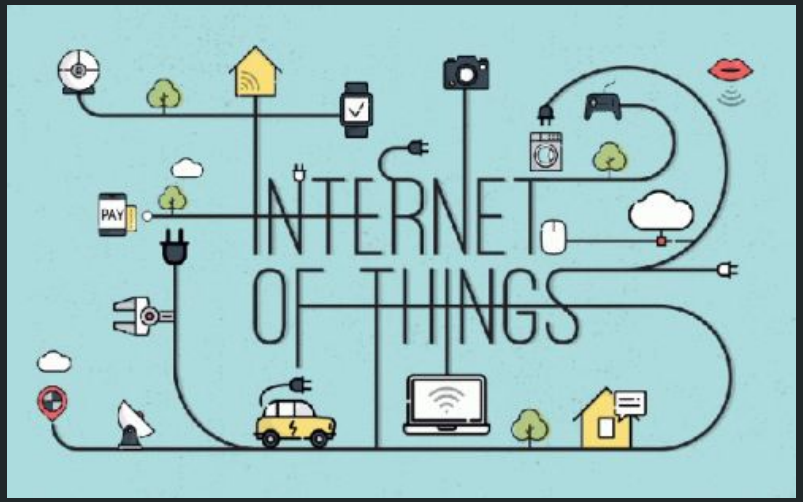
En Zigbee:

- PAN ID (Personal Area Net ID)
- Dirección Fuente/Destino
- Canal
- RSSI
- Autenticación o seguridad

En Thread:

- Destino PAN
- MAC
- Canal
- Protocolo de encapsulamiento (CoAP, MLE, ICMPv6)
- Puerto UDP Origen/Destino

Para más información revisar IEEE 805.15.4 y páginas oficiales de Zigbee y Thread



GPS

Componentes:

- Latitud/Longitud (Altitud)
- Precisión

En resumen

Real-Plastic-4303 • 1y ago

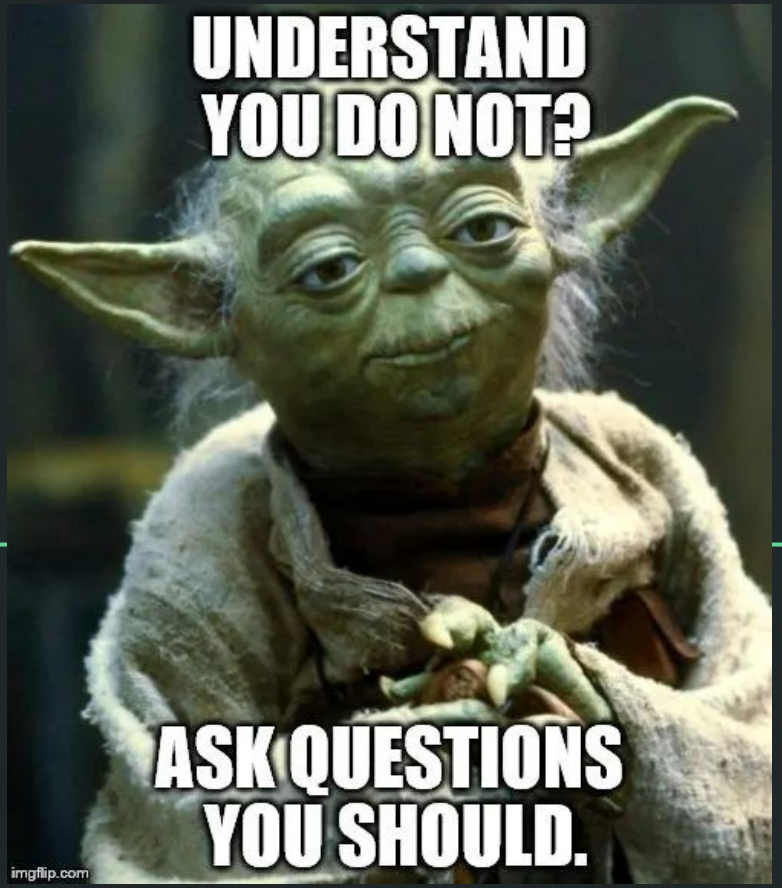
El wardriving no se trata de explotar redes ni de hacer nada malicioso. Es un acto de reconocimiento pasivo. Los ataques que mencionaste no están relacionados; el wardriving solo implica recopilar datos que ya están en el dominio público. Dicho esto, la gente puede usar estos datos por una variedad de razones; al igual que el fuego 🔥 tiene una gran variedad de usos (el fuego no solo se usa para el incendio provocado, también se usa para la artesanía, cocinar, calentar, etc.)

¿Por qué hacerlo?

El wardriving implica recopilar información sobre SSID y MAC de wifi, celulares y dispositivos bluetooth. La gente usa esta información por una variedad de razones; mapeo de cobertura, investigaciones OSINT, auditoría de seguridad de red, incluso protección de testigos/víctimas. Mapear y analizar continuamente los dispositivos a tu alrededor también es una excelente manera de aumentar tu conciencia situacional en general.

Demo

Dudas, preguntas



Muchas gracias por su atención

Contacto:

Proyecto: