

info**byte**

Wardriving

2

INTRO

Whois



- Leonardo Lazzaro
- leonardol@infobytesec.com
- @llazzaro
- github.com/llazzaro



- Nicolás Rey
- rey.nico@gmail.com
- @ReyNico
- github.com/reynico

}

INTRO

Agenda

- Introducción
- Requerimientos para wardriving
- Software custom + raspberrypi
- Post wardriving (Publicación resultados)
- Configuración/consultas
- BusDriving!



1

INTRODUCCIÓN



INTRO

Qué es Wardriving?

- Conducir alrededor de la ciudad buscando la existencia de redes inalámbricas (APs)
- Registrar y localizar estas redes para generar mapas

6

INTRO

Modos operacion dispositivos wifi

- **Monitor:** permite monitorear todo el tráfico recibido por el dispositivo.
- Infrastructure: los clientes se conectan a un access point.
- Ad hoc: los clientes se conectan entre ellos en una suerte de p2p.

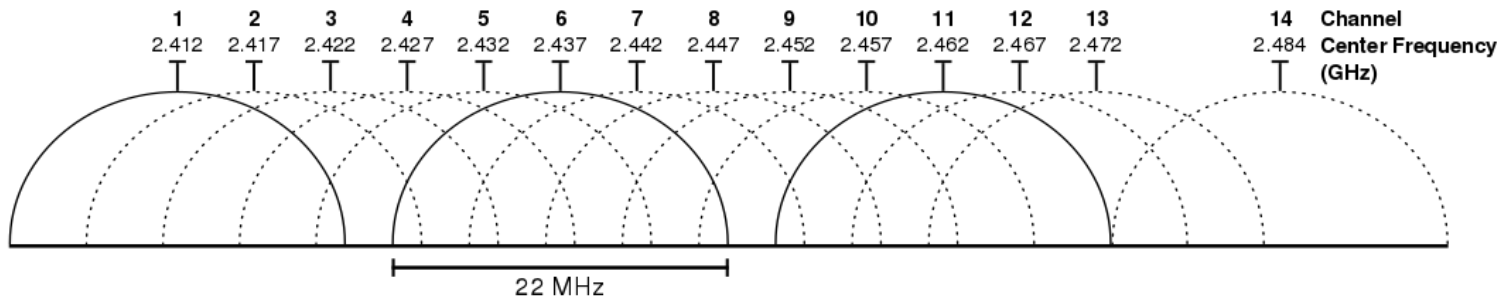
Algunos dispositivos wifi permiten la inyección de paquetes en modo monitor (pasivo).

7

INTRO

Canales y frecuencias

- Canales ideales para transmisión
- Solapamiento de canales y sus desventajas





INTRO

Breve intro a paquetes wifi

Existen distintos tipos de paquetes:

- Management (0): establecer y mantener conexiones.
- Control (1): ack, clear to send, etc
- Data(2): transportan datos, puede ser QoS

Además existen subtipos como por ejemplo:

- Probe request (type=0, subtype=4)
- Deauthentication (type=0, subtype=12)

Paquetes interesantes (wardriving)

- Beacons: Contienen información sobre la red. Se transmiten periódicamente
- Data: Se pueden utilizar para saber si un cliente está conectado a un access point
- Probe request: Los clientes envían este paquete para iniciar la conexión. (privacidad)
- Deauthentication: Lo utilizan los clientes para finalizar la conexión

Que es un 4way handshake?

Es un tipo de protocolo de autenticación establecido en la IEEE-802.11i.

Existen tipos de paquetes para este mecanismo de autenticación.

Depende del algoritmo/configuraciones:

- WPA-PSK(TKIP),WPA2-PSK(AES/TKIP),
WPA/WPA2 Enterprise, etc.



Cómo se realiza el wardriving?

La idea es poder capturar todo el espectro para obtener la mayor cantidad de información.

En general la cantidad de dispositivos wifi es limitada y por esta razón se realiza channel hopping.

Channel hopping consiste en cambiar el canal cada cierto intervalo de tiempo. (esto puede traer problema si uno viaja muy rápido).

2

REQUERIMIENTOS

13

REQUERIMIENTOS

Qué necesito?

- Celular/Notebook/Raspberrypi
- Adaptador WiFi
- GPS
- Software

Celular

- Wigle - geolocalización de APs comunitaria
- Podemos hacer entrecruzamiento de información en caso de no tener GPS en la máquina

```
$ sqlite3 wiglewifi\ \2\).sqlite
SQLite version 3.16.0 2016-11-04 19:09:39
Enter ".help" for usage hints.
sqlite> select ssid, capabilities, bestlat, bestlon from network limit 1;
Speedy-FE3140| [WPA-PSK-CCMP+TKIP] [WPA2-PSK-CCMP+TKIP] [ESS] |-34.60846107|-58.41601111
sqlite> █
```

Notebook

Recomendación:

- Kali
- Kismet+tcpdump/airodump-ng
- GPS USB (podemos usar el celular)
- Adaptador WiFi USB con antena externa

Raspberry Pi

Recomendación:

- Kismet+tcpdump/airodump-ng
- Módulo GPS
- Adaptadores WiFi USB
- Software custom para Wardriving

Antenas

Recomendación:

- Antena omnidireccional
- Antenas direccionales/biquad
- Antenas sectoriales

18

REQUERIMIENTOS

SOFTWARE

Kismet

- Analizador del trafico Wi-Fi
- Sistema de detección de intrusiones
- Usa una DB SQLite
- Podemos usar Python para entrecruzar la data de wifgle y enriquecer nuestra información

}

SOFTWARE CUSTOM

Software custom para Raspberry Pi

- Guarda el tráfico en un PCAP para análisis posterior
- Relaciona posición geográfica de los APs, Clients, Probe Requests
- Utiliza dispositivos Bluetooth, NRF24 y los taggea con GPS
- Permite implementar distintas estrategias de Wardriving

Desafios Raspberry Pi

El análisis de paquetes en tiempo real es muy intensivo.

El hardware de la raspberry pi es muy limitado para este tipo de tareas.

Inicialmente el código custom utilizaba scapy sniff en realtime con pcap activado.

Desafios Raspberry Pi

	Low Traffic	Medium Traffic	High Traffic
p_{pli} (tcpdump)	0.0217	0.0239	0.0805
p_{pli} (scapy)	0.2574	0.6721	0.8911
p_{plo}	$1.333 \cdot 10^{-4}$	$2.667 \cdot 10^{-4}$	0.16

(b) Probability of packet loss.

Tabla 1: Probabilidad de pérdida de paquetes usando tcpdump y scapy. No se utilizó una raspberry pi para generar la tabla.

Extraído de Computer Security – ESORICS 2011:
16th European Symposium on Research computer
security

Software custom para Raspberry Pi

Implementación:

- Scripts multiproceso en python
- Usa redis para sincronizar los procesos (no todo es python)
- Usa aircrack-ng (por performance)
- Usa un módulo GPS (opcional)
- Pantalla LCD para monitorear stats
- Permite importar un SQLite de wigle
- Open source en: **github.com/llazzaro/wifi_tools**

Estrategias wardriving

- Channel Hopping
- Targeted: Por posición geográfica o por dir. mac
- 4waydriving*: Monitorea los canales mas usados (fijo)
- Jammer*: Desconecta a todos los clientes
- Static*: Channel hopping, cambia el canal si hay clientes

* No necesariamente matchean una definición estricta de wardriving

Bluetooth

Utiliza pybluez para escanear y cruza la información con gps.

Potencialmente se podría implementar CVE-2017-0785.

NRF24

Utiliza la librería Raspjack para scanear y sniffear.

El modelo nrf24 utilizado no soporta modo promiscuo pero se encontraron formas de hacerlo(*).

Para lograrlo reducen la longitud de la direccion.

(*)<http://yveaux.blogspot.com.ar/2014/07/nrf24l01-sniffer-part-1.html>

27

POST WARDRIVING

Qué es Faraday?

- Gestor de vulnerabilidades
- Colaborativo
- 60+ Plugins
- Open source (<http://github.com/infobyte/faraday>)
- Compromiso con la comunidad



3 Plugins de wardriving para Faraday

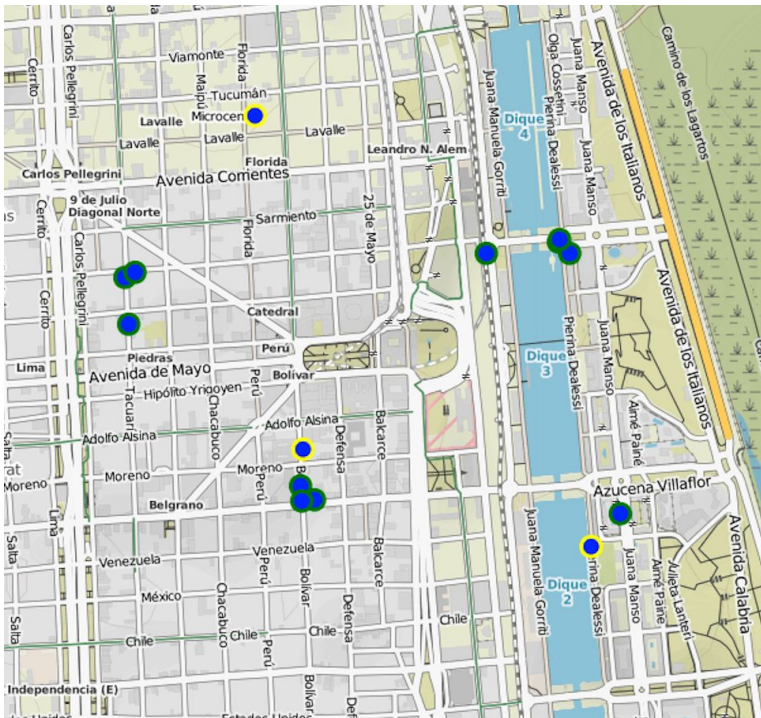
- Mapa con Posición de los APs (plugin wicle).
- Analisis trafico no encriptado.
- Importación de hosts, reporte de handshakes encontrados.

30

POST

WARDRIVING

Mapa access points















31

POST

WARDIVING

Analisis trafico no encriptado

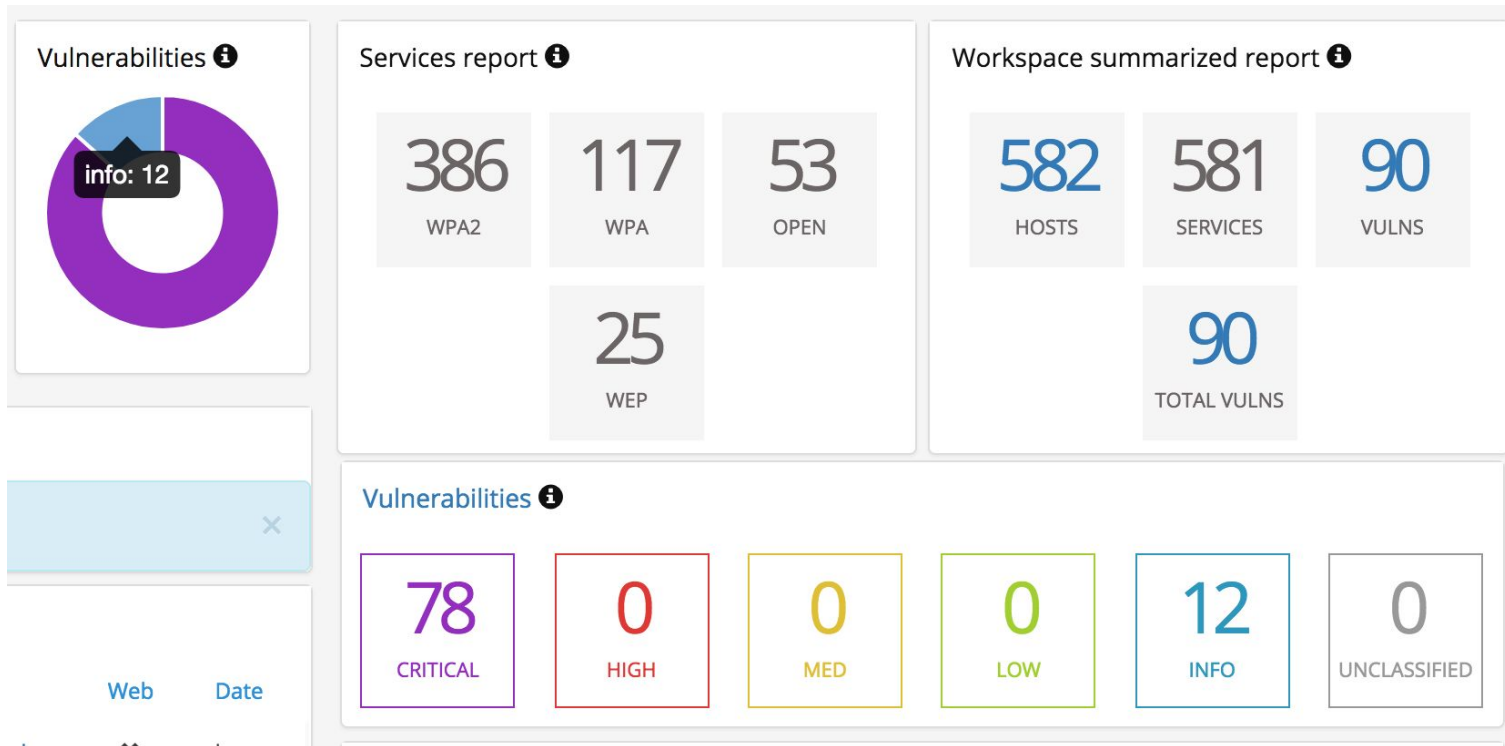
✓	DATE ✕	NAME ✕	SEVERITY ✕	SERVICE ✕	HOSTNAMES ✕	TARGET ✕
		Cookies JSESSIONID sent via unencrypted channel				
  	09/22/2017	Cookies JSESSIONID sent via unencyr...	MED	(80/tcp) http	fbzauth.fibertel.com.ar	10.0.0.6
  	09/22/2017	Cookies JSESSIONID sent via unencyr...	MED	(80/tcp) http	fbzauth.fibertel.com.ar	10.0.0.6
  	09/22/2017	Cookies JSESSIONID sent via unencyr...	MED	(80/tcp) http	fbzauth.fibertel.com.ar	10.0.0.6
  	09/22/2017	Cookies JSESSIONID sent via unencyr...	MED	(80/tcp) http	fbzauth.fibertel.com.ar	10.0.0.6

32

POST

WARDRIVING

Estadísticas





ANALISIS

Reporte Wardriving

Con el tráfico guardado presentaremos un reporte en **github.com/infobyte/wardriving** con:

- Estadísticas, Mapas, Vendors
- Plugins faraday
- Workspace para faraday
- Probe request ssid mas comunes
- Workshop faraday **Jueves a las 13:50hs sala D**

34

Q&A

35

LINKS

Gracias por venir!

- Resultados en: github.com/infobyte/wardriving
- El bus sale a las 15:30! (hay otro el viernes, 14:30)
- leonardol@infobytesec.com
- [@llazzaro](https://twitter.com/llazzaro)
- github.com/llazzaro
- rey.nico@gmail.com
- [@ReyNico](https://twitter.com/ReyNico)
- github.com/reynico