WarXing

Project	WarXing
Description	
Status	Running
Contact	prometheus
Participants:	

WarXing is the hypernym for every activity that is related to war<*put_in_verb_or_noun*>ing.

Wardriving

Invalid Link
Laptop, Antenna, GPS - A hackers way to pwn some WiFi

"Wardriving is the act of searching for Wi-Fi wireless networks by a person in a moving vehicle, using a portable computer, smartphone or personal digital assistant (PDA)." (Source: Wikipedia - Wardriving)

Warchalking

Invalid Link
Common Warchalking signs

"Warchalking is the drawing of symbols in public places to advertise an open Wi-Fi wireless network. Inspired by hobo symbols, the warchalking marks were conceived by a group of friends in June 2002 and publicised by > Matt Jones who designed the set of icons and produced a downloadable document containing them." (Source: Wikipedia: Warchalking)

More informations

We did a radio show about the WarXing culture. Tune in :)

Software



Our 20dBi antenna in action! No, that's not a rocket launcher.

- kismet
- giskismet
- aircrack-ng
- pykismetkml - A Python program for plotting Kismet logs on Google Earth

Hardware

Antennas

- Alfa AWUS036NEH +- 20€
- ALFA 9dBi 2,4GHz WLAN RP-SMA-Hochleistungsantenne +- 6€
- Alfa 20dBi 2.4GHz - 2.5GHz high-Gain Yagi Antenne +- 99€

GPS

All listed navigation devices work with gpsd.

To visualize your tracks quick and online: http://www.gpsvisualizer.com/

What to do when an Access Point shows up several times, but with slightly different positioning coordinates? –> Coordinates average?

Plug & Play

- NaviLock 402-U +- 45€



look for */dev/gps0*

Garmin Oregon 450

Garming Oregon 450 +- 220€

<sxh bash;> ~:$ modprobe garmin_gps ~:$ ls /dev | grep ttyUSB0 ttyUSB0 # this should be your device, 0 can differ </sxh>

Connect the device to your computer and choose "No", if being asked to use the Oregon as a mass storage device.

Here's our WifiSec bash startup script:

<sxh bash;> #!/usr/bin/bash

modprobe first modprobe garmin_gps pid=`pidof gpsd` kill -9 $pid # kill gpsd because fuck you gpsd /dev/ttyUSB0 # restart kismet -f /etc/kismet/wifisec.conf # run kismet with wifisec config </sxh>

From:
https://wiki.c3l.lu/ - **Chaos Computer Club Lëtzebuerg**

Permanent link:
https://wiki.c3l.lu/doku.php?id=projects:security:warxing

Last update: **2021/10/19 12:35**