

Forum:[Hack Forums](#)

Thread: [Wardrive- explanation and tutorial](#)

pomwtin - August 30, 2014, 5:09 pm

Hello :)

I had to do a "wardrive" today for my current project and searched HF for tutorial, but found nothing. So.. i decided to make one, if anyone will ever need it.

There is no any "hacking" here, but it can be used in long-range wifi "hacking" to know where to turn your directional antenna.

If there already is one and i missed it, then i apologise.

What wardrive is:

Calculating approximate location of APs, based on their signals strength and gps position of each signal strength noted, which we get (capture) while driving/walking around with our wifi device synchronized with gps device.

Simple presentation of AP location calculation:

[img]<http://shrani.si/f/40/xZ/2GNt4oXY/wd2.jpg>[/img]

On first place in our database with captured pairs [coordinates,power strength] (and other data) is location 1. Here we noted signal strength [-40] and with knowledge of AP output power (determined by law for each country) and signal strength loss by distance, we can calculate theoretical distance from AP - we get circle (which represents distance) around position 1.

The same steps are repeated for location 2 (where signal strength is [-20], which means smaller distance from AP, which leads to smaller circle compared to location 1) and location 3 (where signal strength is [-90], which means larger distance from AP, which leads to larger circle compared to location 1).

In point, where all three circles meet is theoretical location of AP, marked with red circle.

For presentation i "used" only 3 locations for it to be as simple as possible, but with more logged locations, calculated AP location will be more accurate.

How to do it:

You will need smartphone with GPS and android, computer (laptop) and !preferable! external antenna (signal strength out of a car is better, and you do not want to drive your laptop around on the roof ;))

1) Install BlueNMEA on your cellphone- search in store (it is free)

2) Download Wdrive script (by zatixiz) from here:

http://code.google.com/p/wdrive-bt5/downloads/detail?name=wdrive_2.1.sh&can=2&q=

3) Enable usb debugging on your phone

4) Connect your pc and phone with usb cable

5) Enable usb tethering on your phone

6) Make sure GPS is enabled

- 7) Run BlueNMEA
- 8) Run Wdrive
- 9) Follow Setup instructions
- 10) Go on a trip ?

I stopped explaining setup at 9. step, as Wdrive is completely idiot-proof script- it leads you step by step, so there is no point explaining steps, as you will have on-screen instructions.

Import data to google earth:

At the end you will get your .kml file, which you can import in google earth and see location of APs, with their informations.

If somebody have any problem with process- feel free to ask me :)

?

sp3ctrum - August 30, 2014, 7:27 pm

Nice tutorial, don't think I have seen any write ups on war driving lately, so it's an awesome add. Maybe see if it can get into pandas compilation thread ;)

TheGrayAviator - August 30, 2014, 7:58 pm

(Aug 30, 2014 07:27 PM)-Gator - Wrote: [\[CITE\]](#) Nice tutorial, don't think I have seen any write ups on war driving lately, so it's an awesome add. Maybe see if it can get into pandas compilation thread ;) Panda hasn't been with us, for a very long time.

sp3ctrum - August 30, 2014, 9:04 pm

(Aug 30, 2014 07:58 PM)Greyhat.Infiltrator Wrote: [\[CITE\]](#) Panda hasn't been with us, for a very long time.

Damn, I just assumed he jumped on from time to time. Never really took the time to actually look at his last visit 0.o

TheGrayAviator - August 30, 2014, 9:23 pm

(Aug 30, 2014 09:04 PM)-Gator - Wrote: [\[CITE\]](#) Damn, I just assumed he jumped on from time to time. Never really took the time to actually look at his last visit 0.o We need a new moderator on this session....

zerocool - August 31, 2014, 12:37 am

Nice thread at OP i used to do wardriving using the n900 from time to time, its fun thats for sure. These days i tend to use the app from [here](#) makes life so much easier and you can upload your results to show on a map.

I normally convert the files so i can import them to my own google map.

(Aug 30, 2014 09:23 PM)Greyhat.Infiltrator Wrote: [\[CITE\]](#) We need a new moderator on this session....

And you would fit that job superb.

Just saying ?

pomwtin - August 31, 2014, 3:31 am

Thanks for replies, i'm glad you like it :)

@Z3RO COOL i have tried that, its interesting thingie but my problem was wifi receiver of my

mobile phone... it captured like only 40% of APs captured with this method

Mad76e - August 31, 2014, 5:28 am

Nje.. I need you to put more work on that one. Its a good start tho. i give it a +5 of 10.

Im not trying to be an arse or anything. But i would hope you mention..

kismet, The best Old school Wardriver tool out there (need external GPS tho)

You already mention the BlueNMEA..

Wardrive app for smartphones <https://play.google.com/store/apps/details?id=ki.wardrive4>

Wirgle wardrive app for smartphones

<https://play.google.com/store/apps/details?id=net.wigle.wigleandroid>

Something more about the hardware aswell.

You mention Google Earth and .KML files (you can save your database as an KML file)

Also i would expect that you told something about www.wigle.net and the interactive map, that you can discover AP over the whole damn world just Zoom in on your area of the world

Heh.. It was years ago i was connected to that database.. Nowadays im saving em for myself

zerocool - August 31, 2014, 5:31 am

(Aug 31, 2014 05:28 AM)mad76e™ Wrote: [\[CITE\]](#) Nje.. I need you to put more work on that one. Its a good start tho. i give it a +5 of 10.

Im not trying to be an arse or anything. But i would hope you mention..

kismet, The best Old school Wardriver tool out there (need external GPS tho)

You already mention the BlueNMEA..

Wardrive app for smartphones <https://play.google.com/store/apps/details?id=ki.wardrive4>

Wirgle wardrive app for smartphones

<https://play.google.com/store/apps/details?id=net.wigle.wigleandroid>

Also i would expect that you told something about www.wigle.net and the interactive map, that you can discover AP over the whole damn world just Zoom in on your area of the world

Heh.. It was years ago i was connected to that database.. Nowadays im saving em for myself

Maybe if you had read the whole thread you would see i already did mention wigle to this user.

(Aug 31, 2014 03:31 AM)pomwtin Wrote: [\[CITE\]](#) Thanks for replies, i'm glad you like it :)

@Z3RO COOL i have tried that, its interesting thingie but my problem was wifi receiver of my mobile phone... it captured like only 40% of APs captured with this method

I have tried on n900 and samsung galaxy s3 both had no issues picking up access point's, the only issue i find is the GPS location isn't accurate enough for me.

I like to use kismet for this job to works great if not the best.

Mad76e - August 31, 2014, 5:55 am

(Aug 31, 2014 05:31 AM)Z3RO COOL Wrote: [\[CITE\]](#) Maybe if you had read the whole thread you

would see i already did mention wile to this user.
My fault! I only read OP. Sorry abt that :)

(Aug 31, 2014 05:31 AM)Z3RO C00L Wrote: [\[CITE\]](#) I have tried on n900 and samsung galaxy s3 both had no issues picking up access point's, the only issue i find is the GPS location isn't accurate enough for me.

I like to use kismet for this job to works great if not the best.

Well nowadays im only using wardrive to locate vuln ap (to hack). I seldom save any databases

zerocool - August 31, 2014, 6:43 am

(Aug 31, 2014 05:55 AM)mad76e™ Wrote: [\[CITE\]](#) My fault! I only read OP. Sorry abt that :)

Well nowadays im only using wardrive to locate vuln ap (to hack). I seldom save any databases

I'm the same these days, last time i did a run there was so many open or vunruble AP's scatted every where i was little shocked.

You have got few more AP's than me

[\[img\]http://wile.net/bi/62YWTs49JxJwgq95OJ9QKg.png\[/img\]](http://wile.net/bi/62YWTs49JxJwgq95OJ9QKg.png)

Shame that it log's the GPS location as soon as it see's the AP cause depending how good wifi is it can be out but its close enough to work it out.

PinkPanther - August 31, 2014, 8:32 am

(Aug 31, 2014 06:43 AM)Z3RO C00L Wrote: [\[CITE\]](#) Shame that it log's the GPS location as soon as it see's the AP cause depending how good wifi is it can be out but its close enough to work it out.

Good point, A hacker AP with a grid might show up half a mile away from where it actually is (on one side anyway).

(Aug 30, 2014 05:09 PM)pomwtin Wrote: [\[CITE\]](#) ?

I've never used BlueNMEA, I'll have to give it a try one day.

Mad76e - August 31, 2014, 9:40 am

(Aug 31, 2014 08:32 AM)PinkPanther Wrote: [\[CITE\]](#) Good point, A hacker AP with a grid might show up half a mile away from where it actually is (on one side anyway).

Yeah i prefer a smaller omnidirectional Outdoor antenna 4-6dBi (on a magnetic foot on the roof of a car), however an indoor antenna will do the trick inside the car aswell, however the cars metal chassis may reflect some of the weaker AP's.

Best is to warwalk or warbicycle and have the equipment in a backpack, or using any of the smartphone wardriving apps out there, however as said before those apps are not 100% accurate, it can be a 5-30 meters off or something like that

However the newest Wardriving app called Wardrive does change the point to the strongest source as long as you still have it in the database. So you can see those moving along with your driving. first on the right side of the road then the left side if the signal is stronger there

SW4T - August 31, 2014, 12:50 pm

Is this possible to do with just a normal iPhone?

zerocool - August 31, 2014, 12:55 pm

(Aug 31, 2014 12:50 PM)InfSec Wrote: [\[CITE\]](#) Is this possible to do with just a normal iPhone?

Best of trying the apple store do a search for wardriving also seen this post here

<https://wicle.net/phpbb/viewtopic.php?t=1361>

SW4T - August 31, 2014, 1:02 pm

(Aug 31, 2014 12:55 PM)Z3RO C00L Wrote: [\[CITE\]](#)

Best of trying the apple store do a search for wardriving also seen this post here

<https://wicle.net/phpbb/viewtopic.php?t=1361>

Doing some searching but lots of the iPhone apps aren't available anymore

EDIT: Anyone have an iPhone alternative to BlueNMEA?

EDIT2: Found NMEAGps and gpsRecorder in the App store. Gonna try 'em out.

canibusfan - August 31, 2014, 10:05 pm

people are still wardriving?? I havent done that in years

zerocool - September 1, 2014, 1:17 am

(Aug 31, 2014 10:05 PM)canibusfan Wrote: [\[CITE\]](#) people are still wardriving?? I havent done that in years

Not as much as i used to back in the day, but now an then when it's needed.

DrPanda - September 1, 2014, 2:30 pm

Wingle for android is another good wardriving app yeah its still done.... its more war flying now cause of the drones and stuff ...

mattybeds - September 1, 2014, 2:40 pm

I use an RPi for doing this with a few tools, I used to hate going out now i love it :D Theres loads of devices and networks you can play with on the street. If you have bluetooth enabled you can also attack devices such as cars, phones, printers, epos etc etc. I seriously recommend you install arch linux on your iphone or android then you have all the tools you need :)

Mad76e - September 1, 2014, 3:25 pm

(Sep 1, 2014 02:40 PM)mattybeds Wrote: [\[CITE\]](#) I use an RPi for doing this with a few tools, I used to hate going out now i love it :D Theres loads of devices and networks you can play with on the street. If you have bluetooth enabled you can also attack devices such as cars, phones, printers, epos etc etc. I seriously recommend you install arch linux on your iphone or android then you have all the tools you need :)

Damn man.. You just gave me an idea to a Raspberry/wardriving tut, however i don't have the time to write it now.. Lets see if anybody takes the challenge

Giving you +1 for the Idea

A Raspberry PI would be almost the perfect hardware platform (or any other like the BBB and such) its small and you can connect to it with Putty or RDP/VNC.. you could hide all hardware in a small belt bag

mattybeds - September 1, 2014, 4:23 pm

<https://drive.google.com/folderview?id=0B-QDzmQw9u48ZVBFVUFfcHZHS0E&usp=sharing>

INFECTED]

Like street.pdf lol

SW4T - September 1, 2014, 4:56 pm

Wow some extremely amazing ideas just popped up here.

