WarDriving

# Opdracht

Ik kreeg de opdracht om de huidige stand van zaken qua wireless security in kaart te brengen in de Stad Antwerpen of een andere gemeente naar keuze, in mijn geval Beveren-waas. De opdracht was ook om 2 uitgebreide wardrive sessies uit te voeren en te analyseren hoe het met de veiligheid van de meeste acces points gesteld is. Er mocht enkel een passieve aanpak uitgevoerd worden, d.w.z. dat er geen actieve hacks uitgevoerd zullen worden.

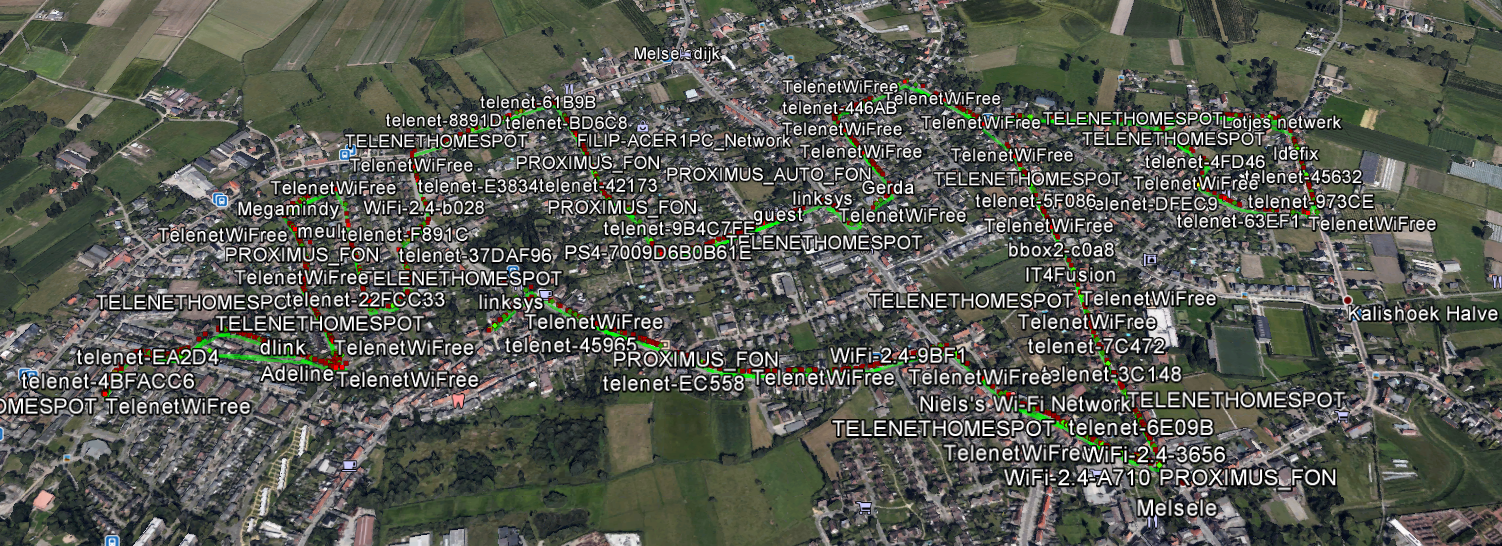
# Gebruikte materialen

* Eigen Laptop
* Raspberry PI
* Gps-module BU-353S4
* Belkin N Wireless wifi module
* Ethernet kabel
* SD kaart 16GB (met Raspbian Jessie erop)

# Algemeen verloop

Allereerst moet er begonnen worden het installeren van Raspbian Jessie op de Raspberry PI. Dit zal dan gaan via een bootable SD-kaartje. Eens het OS geïnstalleerd is, is het de beurt om de juiste installaties uit te voeren. Dit beginnende met het installeren van de gps clients om de gps-module te herkennen en te kunnen testen vooraleer we werkelijk gaan rijden. Daarna moet Kismet geïnstalleerd worden. Hierbij moeten verschillende configuraties gedaan worden voor Kismet in de config file. Het instellen van SSH in het begin van de opdracht maakt het makkelijker om via de laptop te werk te gaan. Tenzij je toetsenbord, scherm en muis allemaal appart liggen hebt. In mijn geval was dit niet het geval dus was SSH gemakkelijk aangezien ik enkel met mijn laptop heb gewerkt dan. Ook was het handig om een bepaald ip address in te stellen op de Rasberry PI omdat dan naar dat netwerk SSH uit te voeren voor als er geen internet aanwezig is in de buurt waarop geconnecteerd kan worden. Na elke sessie zullen er dan enkele bestanden aangemaakt worden waarbij er a.d.h.v. een bepaald scriptje de .netxml kunnen omgezet worden .kml en .kmz bestanden om deze dan in Google Maps of in Google Earth te openen. Zodat we de verschillende Acces points kunnen zien en de route die afgelegd is.

# C:\Users\keirl\Documents\InfSecWarDrive\InfSec\Wardrivesessie0209.PNGWarDrive Sessie



Zoals ik al zei worden de bestanden omgezet naar KML en KMZ bestanden. Deze bestanden kunnen dan geopend worden in ofwel Google Maps ofwel in Google Earth. Maar ik raad Google Earth aan omdat deze grotere bestanden aankan in tegenstelling tot Google Maps.

## Grafieken en Tabbelen

Beide sessies samen in 1 grafiek. Van de 3799 netwerken die gevonden werden is er 67% (2660) WPA encryption, slechts 1% (48) van de netwerken gebruikt WEP als encryptie, 4% (153) gebruikte helemaal geen encryptie en 28% (1091) gebruikt ook geen encryptie. Deze laatste zijn de netwerken van Proximus Fon en Telenet Homespots. Dus dit zijn de gratis netwerken waarop je kan inloggen afhankelijk bij welke internet provider je aangesloten bent.

|  |  |  |  |
| --- | --- | --- | --- |
| WPA | WEP | None | Other |
| 2660 | 48 | 1091 | 153 |

***Sessie 1;***

|  |  |  |  |
| --- | --- | --- | --- |
| WPA | WEP | None | Other |
| 1207 | 23 | 512 | 56 |

***Sessie 2;***

|  |  |  |  |
| --- | --- | --- | --- |
| WPA | WEP | None | Other |
| 1453 | 25 | 579 | 97 |

Conclusie we zien dat bij twee totaal verschillende ritten er toch eigenlijk weinig verschil in zit en dat de meeste percentages overeenkomen. Wat we wel kunnen concluderen is dat de meeste mensen al WPA encryptie gebruiken wat toch de verbeterde versie is van WEP. Alleen als enige minpunt is er wel dat nog in totaal 4% zonder encryptie werken. Natuurlijk weten we ook niet het fijne van deze netwerken en dit kan ook voor testen thuis zijn ook of dergelijke.

# Meest gebruikte commando’s

Gpsmon

Het commando die de gps data laat zien die de GPS module ontvangt en aan de PI geeft. Dit commando is vaak gebruikt als testing om te zien of de module goed werkt voor we met kismet gaan werken.

Sudo apt-get install screen ncurses-dev libpcap-dev tcpdump libnl-dev wireshark

Het commando om alles te downloaden wat we nodig hebben om Kismet te gebruiken en Kismet zelf te downloaden. Dit zal zich bevinden in een bepaalde zip die we dan moeten uitpakken om van daaruit de installatie te voltooien.

Sudo kismet

Het commando om Kismet op te starten.

Wget http://files.salecker.org/netxml2kml/netxml2kml.py.txt

Het commando om het scriptje te downloaden die de netxml bestanden zal omzetten in kml en kmz bestanden.

Sudo python netxml2kml.py –kmz –kml -o Wardrive kismet-20160816-70-50-1.netxml

Het commando voor het omzetten van de netxml bestanden. Met ‘Wardrive’ als de naam van de kml en kmz bestanden die aangemaakt zullen worden en ‘kismet-20160816-70-50-1.netxml’ is de naam van het bestand dat Kismet aangemaakt heeft bij het afsluiten van de server.

Dmesg

Om hardware te kunnen zien op linux om te zien waar de gps module staat.

Cp [FileName] [USB plaats]

Commando om bestanden te kopiëren. Ik heb deze gebruikt om mijn kml en kmz bestanden over te zetten naar een usb stick.

# Problemen/oplossingen

Het grootste probleem was echter dat er weinig kennis was van linux en Raspberry PI omdat de eerste zit niet echt vlot liep. Maar dit was nu al stilletjes aan beter aan het verlopen en ging telkens beter naarmate ik dit project verliep omdat het wel leuk werken is met een Raspberry PI. Daarna had ik nog een paar kleine problemen want volgens een tutorial moest ik cgps -s gebruiken om de interface van de GPS module te laten zien maar deze installatie lukte nooit dus ben ik een alternatief gaan opzoeken en was gpsmon de eerste oplossing die perfect werkte en heb ik deze gebruikt. Bij het rijden heb ik wel 2 keer gehad dat de Kismet server crashte tijdens het rijden maar dan was ik al een tijdje aan het rijden dit is ook te zien in de route dat er op het einde een stuk van tussen is. Maar hoe dit exact komt dat is me nog niet echt duidelijk. Bij het inladen van KML bestanden in google maps kreeg ik de error dat het kml bestand te groot was dus heb ik eens met google earth geprobeert en dit gaf geen problemen.