

Drive-by hacking



Draadloze netwerken bestaan al langer. Ze zijn echter flink in populariteit toegenomen door de dalende prijzen. De eenvoudigste setup waarbij er een centraal 'base station' staat opgesteld en er een wireless PCMCi-kaartje in een laptop wordt gebruikt kost nog maar 250 euro, goedkoop genoeg om het aantrekkelijk te maken voor de thuisgebruiker die graag in zijn tuin wil kunnen internetten.

En ook goedkoop genoeg om aan te kunnen schaffen binnen een bedrijf, zonder allerlei handtekeningen en goedkeuringen aan te hoeven vragen. De systeembeheerder met de keus tussen het aanleggen van switches en bekabeling, of het neerzetten van een of twee base stations, heeft die keus snel gemaakt. Zonder te beseffen wat de risico's zijn van zo'n draadloos netwerk.

Een vast netwerk met kabels ligt fysiek op een bepaalde plek: in een gebouw of onder de grond, maar is in ieder geval moeilijk bereikbaar voor mensen die er niet op thuishoren. Iemand die van zo'n netwerk gebruik wil maken zal door de fysieke beveiliging heen moeten om het pand binnen te komen, bijvoorbeeld. Een draadloos netwerk heeft deze belangrijke eigenschap niet, de data gaat door de ether en laat zich niet tegenhouden door perceelgrenzen.

Met de opkomst van draadloze netwerken zien we nu ook een toename van het aantal mensen dat met een laptop met wireless kaart in de hand op zoek is naar 'lekkende' base stations, draadloze netwerken die buiten de gebouwen zijn op te vangen. Ook al zendt de apparatuur met weinig vermogen, toch zijn zulke netwerken over afstanden van honderden meters te ontvangen met gewone apparatuur. De telecom-technenuten gaan nog een stapje verder door het aansluiten van externe antennes die het bereik

vergroten tot wel 25km! Alleen de afwezigheid van blokkerende obstakels is vereist.

Het is interessant om te zien hoeveel draadloze netwerken er in de omgeving zijn. Dit jaar heb ik een onderzoek gedaan naar draadloze netwerken in mijn woonplaats Eindhoven. De benodigdheden waren: een vervoermiddel, een laptop met wireless kaart en wat software. Die software is van internet te downloaden, het is nog gratis ook. Voor het gemak had ik ook een omvormer van 12Volt naar 220Volt zodat ik lang kon blijven scannen, en een GPS-ontvanger om automatisch de coördinaten van de gevonden base stations op te slaan. Op die manier is het vrij eenvoudig om base stations te zoeken: je zet de laptop aan, rijdt een rondje, en stopt de resultaten in een kaartprogramma. Het resultaat is een kaart van Eindhoven met puntjes die draadloze netwerken markeren. Ook de namen van de netwerken (door de beheerders van de base stations ingegeven) worden gedetecteerd, en daarnaast wordt waargenomen of ze aan de in de wireless standaard gedefinieerde WEP-versleuteling doen. Die namen geven vaak al interessante informatie, die je eigenlijk liever niet zou weggeven. Dit zoeken naar netwerken vanuit een auto of motor heet wardriving.

Versleuteling

WEP-versleuteling wordt slechts door de helft van de base stations gebruikt. WEP zorgt ervoor dat de IP-pakketten versleuteld worden. Het levert een aantal problemen op, waardoor het vrij eenvoudig is om, na het aftappen van voldoende verkeer, de gebruikte sleutel te achterhalen. Die sleutel is sowieso een probleem: er is er maar een van, die door iedereen wordt gebruikt. Indien het netwerk ook gebruikt wordt door bezoekers, of als het een open netwerk is zoals bij een universiteit, dan is het vrijwel