Koppelen van Raspberry-PI aan het internet

Datum:27-7-2015 ver 1.1

INFO: PD0POU@AMSAT.ORG

Voorwoord:

Beste amateur.

In dit document beschrijf ik wat er kan gebeuren als men de Raspberry-PI open zet voor het internet.

Het document heeft ook links waar u meer informatie kan krijgen over het besproken onderwerp.

Na het lezen van dit document hoop ik dat u meer beschermt bent voor ongenodigde gasten die proberen u netwerk te hacken via u Rasberry-PI.

Voor de techneuten onder ons, ik beschrijf in Jip en Janneke taal wat er kan gebeuren.

U verwijs ik ook naar de links waar u meer technische informatie kan terug vinden over het besproken onderwerp.

Ik zal in document niet ingaan op de tools die gebruikt worden voor hacking. Dit stookt in tegen alle normen en waarde. Ik zal ook **geen** antwoord geven op vragen over dit onderwerp.

Voor de rest wil ik u veel lees plezier wensen en als u nog niet op vakantie bent geweest wens ik u een fijne vakantie

PD0POU,

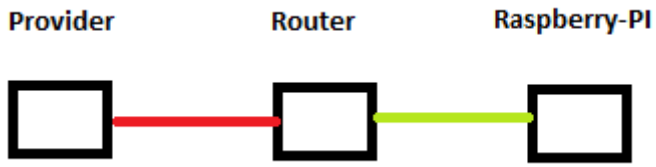
Balte de Wit

Index

Hoofdstuk 1 : Introductie provider

Veel providers leveren hu eigen router / modem, denk aan Ziggo , KPN etc.

Deze routers werken als volgt, men sluit de Wan (externe)aansluiting aan op de aansluiting die uit de muur komt (kan glas, adsl , kabel etc) zijn. Aan de Lan (interne) aansluiting zit vaak WIFI of/en een vaste aansluiting voor u computer. De werking van deze aansluiting werkt als volgt.



De provider levert u een extern ip adres , dit ip adres is uniek voor u provider. In hoofdstuk 3 beschrijf ik u hoe u dit kan opvragen. De router zet het externe ip adres om naar een intern ip adres.

Men moet dit ook wel local ip adres, deze bestaan vaak uit een klasse A, B, C. De meeste providers gebruiken de standaard van het door hun geleverde router (192.168.X.X / 24) dit is een klasse C.

Deze interne ip reeksen zijn niet bruikbaar op het internet , alleen op u interne netwerk.

http://www.vlsm-calc.net/ipclasses.php

Hoofdstuk 2 : Settingen van u router

Standaard staat de geleverde router van u provider dicht , dit betekend dat de poort voorwaarding uitstaat. In de router kunt u deze voorwaarding aanzetten voor bijvoorbeeld u Raspberry-PI.

Door het interne ip adres van u Rapberry-PI in u router te voorwaarden kunt u extern (vanaf internet) bv met VNC bij u Raspberry-PI. Dit betekend ook dat u niet alleen deze mogelijk heeft maar de hele wereld.

http://portforward.com

Hoofdstuk 3 : Opvragen u Extern ip adres

Zoals al aangegeven in Hoofdstuk 1 hier de beschrijving voor het opvragen van u extern IP adres.

http://whatismyipaddress.com

(voorbeeld)

Dit is het externe ip adres geleverd door u provider , door dit ip adres in u VNC viewer in te type krijgt u verbinding met u Raspberry-PI (als u de poort voorwarding aan heeft staan).

Hoofdstuk 4 : Ik wil jou ip adres, en die vind ik zelf wel

Zo nu weet wat een intern en extern ip adres is gaan we in op de gevaren die dit met zich mee kan brengen. U weet nu wat u extern ip adres is waar u Raspberry-PI op aangesloten is. U weet ook dat hij bereikbaar is via VNC poort 590x.

Nou even voor u, op het internet zijn er groepen (genaamd script kiddies) actief.

Deze groep gebruikt bestaande tools, programma's zoals poortscanners om te kijken of u wat open heeft staan. Dit geld ook voor VNC aangezien dit een bekende poort is in de ICT wereld.

http://www.pctools.com/security-news/script-kiddie

Ja zult u denken maar dn weet hij niet dat dat externe ipadres mijn ip adres is.

Daar heeft men een andere trucs voor, ik zal een voorbeeld beschrijven hoe men dit doet.

De eerste stap is het achterhalen van u email adres , dit is simpel (google maar op je call)

De tweede stap is send een mail : vb hallo OM mijn Dstar software werkt niet welke gebruik jij ?

De derde stap is wachten op de respons mail.

De vierde stap is haal uit de retourmail het externe ip adres

De vijfde stap mag u zelf raden.

https://www.eenmanierom.nl/ip-adres/

Hoofdstuk 5 : ik neem jou netwerk over zonder dat jij het weet.

Hoop dat de spanning voor u nog te dragen is, We gaan er nu vanuit dat de hacker in u Raspberry pi zit. Natuurlijk denkt u maar er stat een paswoord op mijn VNC, als u het standaard paswoord niet heeft aangepast is de kans dat Raspberry kan zijn (default paswoorden zijn wil google te vinden)

Ok even verder, de hacker zit op u Rasberry-PI wat kan hij zo uit halen. De eerste stap die de hacker zal uithalen is een nieuwe gebruiker aanmaken (vb systemroot oid) Deze gebruiker krijgt de Root (Admin) rechten van u systeem. Deze gebruiker kan buiten u zicht werken zonder dat u zicht heeft wat hij uitvoerd. Ook al zal u het Root wachtwoord veranderen zal deze gebruiker altijd instaat zijn in te loggen en te wijzigen .

Een voorbeeld wat je kan uithalen op een Raspberry-PI

Door dat de hacker toegang heeft op de Raspberry-PI kan hij remote software installeren.

Een veel gebruikte tool is Wireshark, of Tshark met dit programma kunt u via de Raspberry-PI u locale net werk scannen. De hierbij aan alle systemen die zich daar bevinden dus ook u Ipad , SAN , NAS , Iphone. Door deze toepassing kan men wachtwoorden achterhalen die plain over u net werk gaan.

Voorbeeld : inloggen mail server , inloggen router , inloggen u netwerkschijf op u thuis netwerk.

U ziet wat men kan achterhalen en nog zonder dat u het ziet ook.

http://www.networkworld.com/article/2225683/cisco-subnet/raspberry-pi-as-a-network-monitoring-node.html

Hoofdstuk 6 : Tips

Ja nu denkt u wat nu, hierbij heb ik wat tips voor u.

Tip 1 : Vervang standaard wachtwoord van u Raspberry-PI (maakt het moeilijk gebruik hoofdletters en special leestekens)

Tip 2 : Vervang het VNC wachtwoord (maakt het moeilijk gebruik hoofdletters en special leestekens)

Tip 3: Als er geen noodzaak is voor het openzetten van poort voorwaarding zet het dan uit. Zet het alleen op als het nodig is.

Tip 4: vervang regelmatig wachtwoorden op u systemen, let wel op niet zoals audia4 of u kenteken.

Vind u het moeilijk om zo'n wachtwoord te maken , vervang de klinkers door cijfers:

BaltedeWit zal dan worden B1lt3d3W7t