tool view

Albert Mietus'

toolview

Elke ingenieur gebruikt tools en iedereen heeft zijn eigen voorkeur. Vaak op dat wat toevallig als eerste beschikbaar was. Zo ook de ICT-ingenieur. Ook hij gebruikt tools, software-tools wel te verstaan. Daarvan zijn er oneindig veel, waardoor kiezen erg moeilijk is. Veel *handige tools* worden niet gebruikt, eenvoudigweg omdat niet bekend was dat er een tool voor is, specifiek voor dat probleem.

Het leren gebruiken van een tool kost tijd. Maar als je de naam en het doel van het tool kent, loont het gebruik al vaak de moeite. Het leren en inzetten kost vaak minder tijd dan aanmodderen zonder goed tool.

Deze rubriek stelt dergelijke *handige tools* voor; dit keer een netwerk-tool.

Ken je ook een handig tool, schrijf dan ook eens tool(re)view.
Mail me, voor meer info
ALbert dot Mietus at PTS dot nl

door & more

TCPdump

Eén van de oudste en bekendste programma's om een TCP/IP netwerk te bekijken is TCPdump. Het is een typisch Unix programma: een commandline interface en complex in gebruik. Bedoeld voor de expert.

Er zijn veel opvolgers. ***Ethereal*** *is free, opensource en ontwikkeld voor Unix en Windows, volledig grafisch en zelfs te gebruiken door dummy's.*

Alvast een tip: Start het als root/admin. Anders is een 'Capture', het sniffen van het netwerk, niet mogelijk.

Kijk op http://www.ethereal.com voor meer info.
Let op, ***Ethereal*** *heeft slechts één 'r'!*

ethereal

Een netwerk is een geweldige uitvinding; jammer dat het per definitie traag is. Als gebruiker bel je dan de helpdesk, als netwerkspecialist hoop je vaak maar dat het beter wordt. Dat is het nadeel van ICT: het is erg onzichtbaar. Soms zou je willen dat er meer te zien was. Zeker als het te traag is en jij moet zeggen waarom! Een tool als *Ethereal* geeft dat gewenste inzicht. Het 'snift' alle bits van een netwerk; herkent de protocollen en presenteert alle data netjes gelaagd.

het nut van een GUI

Bij een programma als *Ethereal* merk je dat een goede GUI voordelen heeft. Noch voor het 'lezen' van netwerkverkeer, noch voor het analyseren ervan is een user-interface belangrijk. Maar bij het presenteren is er een reëel voordeel. *Ethereal* presenteert de netwerkdata overzichtelijk in 3 windows. Er is een globaal, regel-georiënteerd overzicht. Daaronder worden details van één bericht gepresenteerd, waarbij protocolhiërarchieën inzichtelijk gemaakt worden; in voor iedere ICT'er heldere taal. Het onderste scherm laat vervolgens een 'hexdump' zien; voor als elk detail belangrijk is. Dit overzicht maakt *Ethereal* beter bruikbaar dan andere, niet grafische netwerk-analyse tools; zeker voor de incidentele gebruiker.

protocolkennis

TCP/IP is geen protocol, maar een familie van protocollen. Een grote familie mag gezegd worden. Tel daarbij de Microsoft protocollen, de Ethernet standaarden en andere netwerk-details op en je hebt een encyclopedie aan kennis nodig om een paar KByte aan netwerk-verkeer te analyseren. Echt moeilijk is het niet, maar wel heel veel werk! Met een goed tool hoef je al die detailkennis niet paraat te hebben. *Ethereal* zoekt alles automatisch op. Zodat jij, als gebruiker, je kan concentreren op het waarom. Voor globale vragen is daardoor slechts globale kennis van een protocolstack nodig.

filteren

Netwerken worden steeds sneller, maar het beschikbare geheugen groeit nog sneller. Een weeklang een ADSL lijn sniffen kost nog geen 100M! De vraag is echter hoe je die brij aan data interpreteert. Ook hier is hulp. *Ethereal* kent filters; zowel om te bepalen of hij netwerkdata moet bewaren, als om die te presenteren. Dat laatste eventueel in kleur. Ook hierbij komt de GUI handig van pas; een filter lijkt op een formule, waarbij de ene 'protocol.member' vergeleken wordt met een andere, of met een constante. De GUI biedt een klikbaar overzicht; zodat je niet alle protocolnamen en -velden van buiten hoeft te kennen. Reeds bekende namen kun je ook direct intypen. Wel is het jammer dat beide soorten filters hun eigen syntax hebben. De verklaring is valide; maar voor de af-en-toe gebruiker is het lastig.

sneller en onveiliger

Er bestaan vele netwerktools. Sommige meten hoe druk het netwerk is, of tekenen grafieken van de protocollen die het meest gebruikt worden. Terwijl je met *Ethereal* als het ware in de kabel kunt kijken. Dat gaat eenvoudig en snel. Bij een netwerk dat structureel overbelast is, helpt dat niet. Maar als het netwerk inefficiënt gebruikt wordt, kan je dat zien. Maar let op, *Ethereal* maakt alles zichtbaar; ook wachtwoorden van telnet, ftp of webapplicaties. Dit kan tot misbruik leiden; laat je daartoe niet verleiden!