LinuxFocus article number 346
http://linuxfocus.org

door Mario M. Knopf
(homepage)

Over de auteur:

Mario houdt zich graag druk bezig met Linux, netwerken en andere beveiligingsgerelateerde onderwerpen.

Vertaald naar het Nederlands door:
Guus Snijders
<ghs(at)linuxfocus.org>

darkstat - een netwerk-verkeer analyzer

Kort:

In dit artikel presenteren we de netwerkverkeer analyzer darkstat en geven we een overzicht van de installatie, het opstarten en het gebruik van dit programma.

Introductie

"*darkstat*" [1] is een tool voor het monitoren van netwerken en het analyseren van opgenomen gegevens. Het kan op basis van deze data verschillende statistieken als HTML-uitvoer produceren. Deze statistieken kunnen comfortabel worden bekeken met een browser. De auteur van het programma heeft eerst lange tijd "*ntop*" [2] gebruikt voor dit doel, maar de stabiliteitsproblemen en slecht geheugen gedrag bevielen toch niet zo goed. Dat heeft geleid tot de ontwikkeling van *darkstat*. De gemaakte statistieken refereren aan de communicatie tussen hosts, het veroorzaakte verkeer, de poortnummers en eventueel de gebruikte transmissie-protocollen. Ook diagrammen van de verzamelde perioden en een korte samenvatting van de geanalyseerde pakketten sinds de programma-start behoren tot de mogelijkheden.

Installatie

De broncode van darkstat kan direct op [3] worden gevonden. Eventueel kan hiervoor ook één van de

twee mirrors ([4], [5]) worden gebruikt. De Debian pakketten kunnen gevonden worden op [6].

Darkstat is ook afhankelijk, net als vele andere tools voor netwerk monitoring, van "*libpcab*" [7]. Dit is een library (bibliotheek) die gebruikt wordt door pakket sniffers en levert een interface voor het opvangen (capturing) en analyseren van pakketten van netwerk apparaten. Voor de installatie van darkstat heb je dus eerst deze library nodig.

Vervolgens kun je compileren met de overbekende drie-stappen-procedure "`./configure && make && make install`". Overigens dient de laatste instructie met root-rechten plaats te vinden.

Start

Darkstat biedt een aantal parameters die bij het starten van het programma kunnen worden meegegeven. Echter, voor een eerste test is een start zonder opties voldoende. Om in staat te zijn werk te verrichten, moet het programma wel als root of met "*sudo*"-privileges [8] gestart worden:

```
neo5k@proteus> sudo /usr/local/sbin/darkstat

We trust you have received the usual lecture from the local System Administrator.
It usually boils down to these two things:

#1) Respect the privacy of others.
#2) Think before you type.

Password:
```

Nadat de geauthoriseerde gebruiker zijn wachtwoord heeft gegeven, start darkstat en geeft een aantal statusberichten:

```
darkstat v2.6 using libpcap v2.4 (i686-pc-linux-gnu)
Firing up threads...
Sniffing on device eth0, local IP is 192.168.1.1
DNS: Thread is awake.
WWW: Thread is awake and awaiting connections.
WWW: You are using the English language version.
GRAPH: Starting at 8 secs, 51 mins, 22hrs, 30 days.
Can’t load db from darkstat.db, starting from scratch.
ACCT: Capturing traffic...
Point your browser at http://localhost:666/ to see the stats.
```

Daar de test succesvol was en de uitvoer zichzelf verklaart is, kunnen we kijken naar de mogelijke opstart-parameters.

Start opties

Zoals eerder genoemd, biedt darkstat verschillende opties die bij het starten kunnen worden meegegeven. Deze parameters zijn:

Met optie "-*i*" kun je opgeven welke interface je wilt monitoren.

darkstat -i eth1

Zonder speciale parameters opent darkstat de gepriviligeerde poort 666. Je kunt deze gewoonte voorkomen door te starten met de parameter "-*p*":

darkstat -p 8080

Om te binden aan een bepaalde poort van een specifieke interface, kun je optie "-*b*" gebruiken. In het volgende voorbeeld wordt het local loopback adres gebruikt:

darkstat -b 127.0.0.1

Persistente DNS-Resolutie kan worden voorkomen met de parameter "-*n*". Dit kan vooral handig zijn voor mensen zonder flat-fee of vaste lijn.

darkstat -n

Gebruik de optie "-*P*" om te voorkomen dat darkstat de interface in "*promiscuous mode*" plaatst. Dit is echter niet aan te raden omdat darkstat dan alleen die pakketten opvangt en analyseert die gericht waren aan het MAC-adres van de gemonitorde netwerk-interface. Alle andere pakketten worden genegeerd.

darkstat -P

De parameter "-*l*" activeert correct "*SNAT*" -gedrag in het locale netwerk. SNAT staat voor "*Source Network Address Translation*" en betekent dat je router het lokale IP adres van de client maskeert met zijn eigen publieke. Dan verstuurt de router dus de aanvraag voor de client die de oorspronkelijke vraag stelde.

darkstat -l 192.168.1.0/255.255.255.0

Met de parameter "-*e*" kun je een pakketfilter-expressie uitvoeren.

darkstat -e "port not 22"

Vanaf versie 2.5 kun je darkstat "detacheren" van de terminal. Dan functioneert hij dus als een daemon.

darkstat --detach

Met de parameter "-*d*" geef je de directory op waar darkstat zijn database creëert.

darkstat -d /directory

De optie "-*v*" activeert de "*verbose mode*":

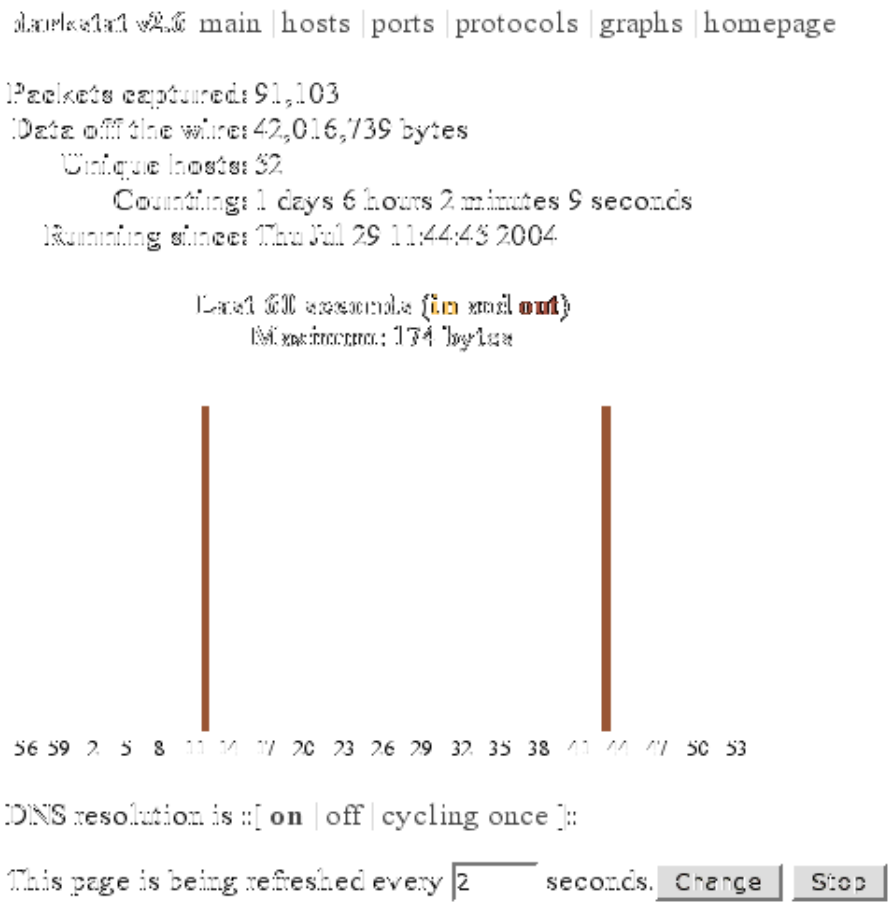
darkstat -v

Als je het versienummer van darkstat wilt bekijken, of hulp wilt bij het gebruik en de syntax, kun je de parameter "*-h*" proberen.

darkstat -h

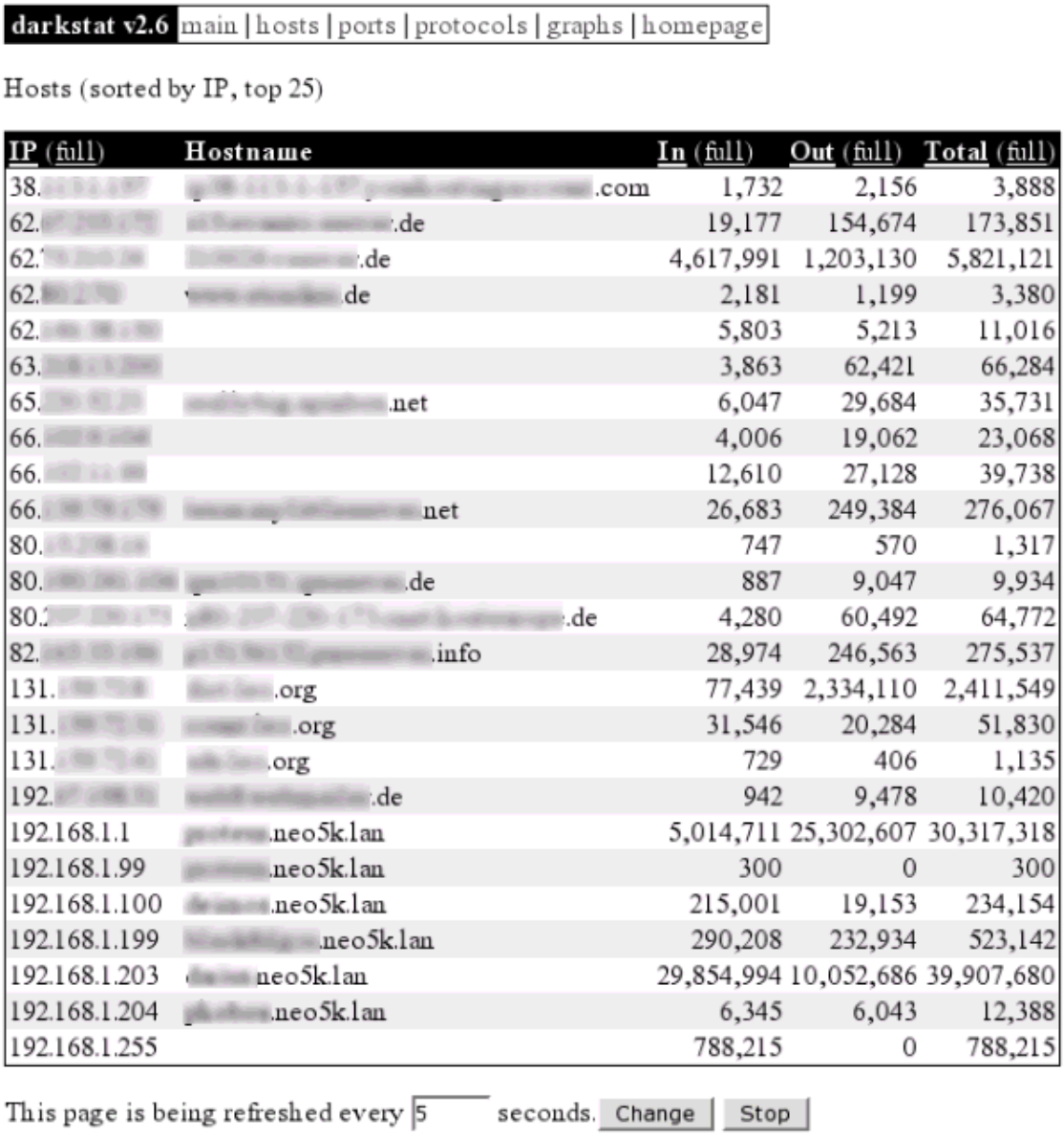
Gebruik

Na de eerste start van darkstat kun je je browser sturen naar "*http://localhost:666*", dit is de standaard instelling. Nu kun je kijken naar een korte samenvatting van de statistieken en enkele grafieken, gegenereerd sinds het starten van het programma:



Afbeelding 1: darkstat openingspagina

Op de "*hosts*" pagina kun je alle machines zien die deelnemen in de communicatie. Deze kunnen gesorteerd worden op veroorzaakt verkeer of op hun specifieke IP adres. Met deze mogelijkheid kun je snel de machines achterhalen die het meeste verkeer op je lokale netwerk hebben veroorzaakt. Daarbij heeft de verantwoordelijke systeembeheerder een kans om problemen tot op de bodem uit te zoeken. In het volgende screenshot is dit bijvoorbeeld de cliënt met het lokake IP adres "*192.168.1.203*".



darkstat v2.6 main | hosts | ports | protocols | graphs | homepage

Hosts (sorted by IP, top 25)

IP (full)	Hostname	In (full)	Out (full)	Total (full)
38.	.com	1,732	2,156	3,888
62.	.de	19,177	154,674	173,851
62.	.de	4,617,991	1,203,130	5,821,121
62.	.de	2,181	1,199	3,380
62.		5,803	5,213	11,016
63.		3,863	62,421	66,284
65.	.net	6,047	29,684	35,731
66.		4,006	19,062	23,068
66.		12,610	27,128	39,738
66.	.net	26,683	249,384	276,067
80.		747	570	1,317
80.	.de	887	9,047	9,934
80.	.de	4,280	60,492	64,772
82.	.info	28,974	246,563	275,537
131.	.org	77,439	2,334,110	2,411,549
131.	.org	31,546	20,284	51,830
131.	.org	729	406	1,135
192.	.de	942	9,478	10,420
192.168.1.1	.neo5k.lan	5,014,711	25,302,607	30,317,318
192.168.1.99	.neo5k.lan	300	0	300
192.168.1.100	.neo5k.lan	215,001	19,153	234,154
192.168.1.199	.neo5k.lan	290,208	232,934	523,142
192.168.1.203	neo5k.lan	29,854,994	10,052,686	39,907,680
192.168.1.204	.neo5k.lan	6,345	6,043	12,388
192.168.1.255		788,215	0	788,215

This page is being refreshed every 5 seconds. Change Stop

Afbeeldign 2: darkstat hosts

In afbeelding 3 kun je de poortnummers zien die gebruikt worden door server en client applicaties. Je kunt onmiddelijk de poortnummers herkennen die door de volgende daemons worden gebruikt: *21 (FTP), 22 (SSH), 139 (Samba), 631 (CUPS), 666 (darkstat), 3128 (Squid)*. Echter, de twee services "*dhcpd*" en "*dnsmasq*" zijn niet zichtbaar, omdat deze services communiceren via "*UDP*". Alle poorten boven 1024 zijn niet gepriviligeerd en worden gebruikt door client applicaties voor communicatie. De proxy server "*squid*" vormt een uitzondering, deze gebruikt standaard de poort 3128. Je kunt een bijgehouden lijst van alle poortnummers vinden bij IANA [9], deze is verantwoordelijk voor deze lijst. Eventueel kun je ook in het bestand "*/etc/services*" kijken.

darkstat v4.6 main | hosts | ports | protocols | graphs | homepage

Ports (TCP, sorted by port number)

Port	(full)	In	(full)	Out	(full)	Total	(full)
21	ftp	10,920		13,674		24,594	
22	ssh	8,883		11,183		20,066	
139	netbios-ssn	1,493,691		1,413,577		2,907,268	
631	ipp	144		0		144	
666	darkstat	144		0		144	
3128	ndl-aas	3,110,943		22,762,308		25,873,253	
11233	(unknown)	476		20,498		20,974	
12469	(unknown)	280		543		823	
17633	(unknown)	164		164		328	
17827	(unknown)	216		284		500	
18616	(unknown)	216		470		686	
20249	(unknown)	280		1,291		1,571	
21642	(unknown)	280		853		1,133	
29814	(unknown)	216		470		686	
31667	(unknown)	632		48,658		49,290	
32733	(unknown)	424		7,969		8,393	
36073	(unknown)	424		7,969		8,393	
36112	(unknown)	164		164		328	
42831	(unknown)	372		7,969		8,341	
47207	(unknown)	992		65,311		66,303	
57308	(unknown)	424		19,014		19,438	
59860	(unknown)	216		333		551	

This page is being refreshed every 3 seconds. Change Stop

Afbeelding 3: darkstat poorten

In de volgende afbeelding kun je de protocollen "*ICMP*", "*TCP*" en "*UDP*" zien, welke betrokken waren bij de communicatie-gebeurtenis. Geïnteresseerden kunnen goede introducties vinden in de RFCs op [10], [11] en [12].

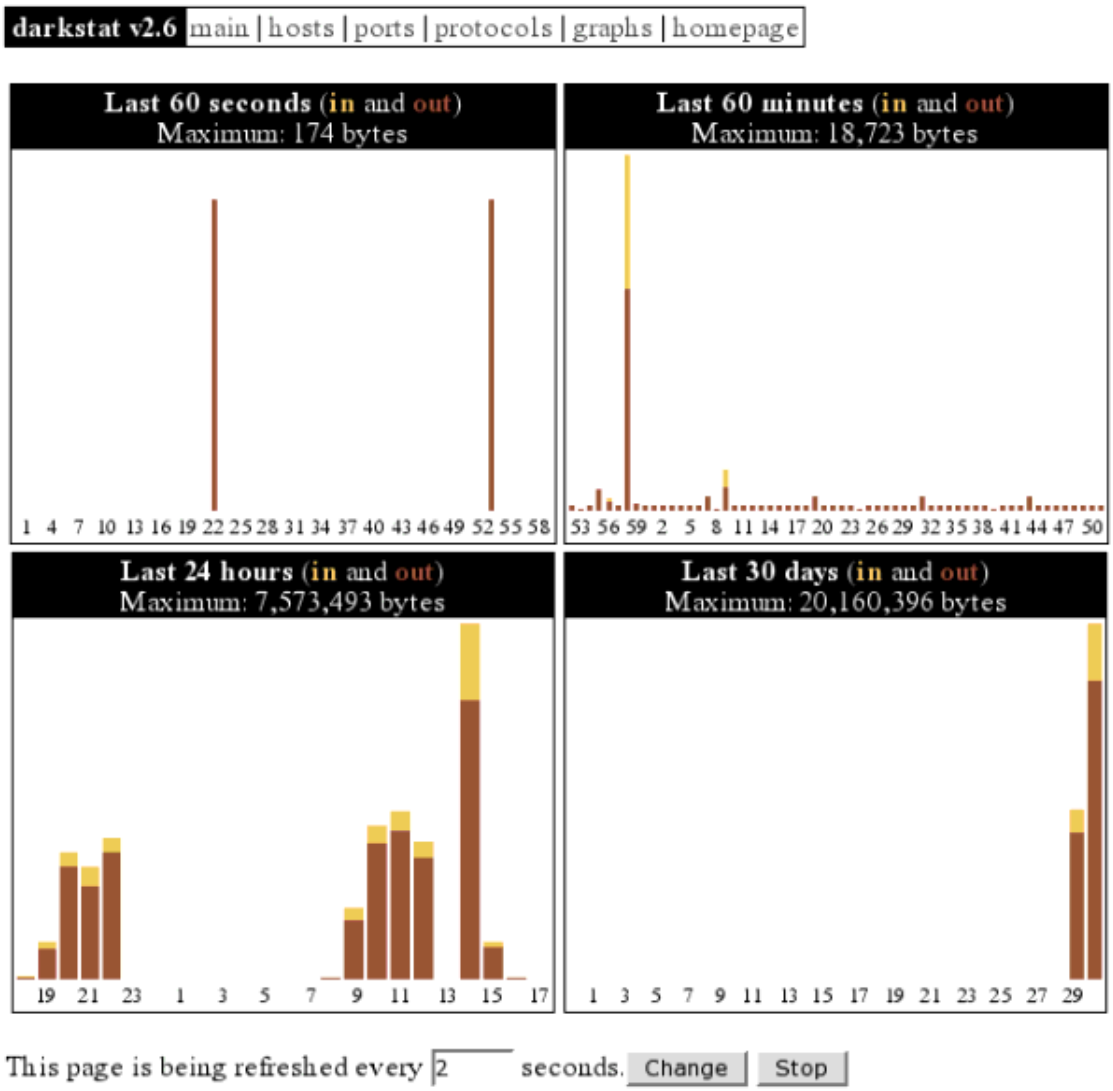
darkstat v4.6 main | hosts | ports | protocols | graphs | homepage

Protocol		In	Out	Other	Total
1	Internet Control Message	363	19,947	0	20,310
6	Transmission Control	4,683,224	24,389,193	10,693,997	39,766,416
17	User Datagram	7,973	708,131	90,684	806,790

This page is being refreshed every 2 seconds. Change Stop

Afbeelding 4: darkstat protocollen

Het laatste screenshot geeft een samenvatting van de bekeken periodes als grafieken:



Afbeelding 5: darkstat grafieken

Vooruitzichten

Versie 2.6 van darkstat, die we hier besproken hebben, is helaas afhankelijk van "*pthreads*". Dit veroorzaakt problemen op andere platformen, zoals NetBSD. Om deze reden heeft auteur Emil Mikulic besloten om de huidige versie 2.x niet verder te ontwikkellen en in plaats daarvan al te werken aan 3.x

In de nieuwe versie worden zoaken geïmplementeerd zoals het capturen van pakketten van meerdere interfaces tegelijk, een configuratiebestand parser, een optisch verbeterde uitvoer van diagrammen (vergelijkbaar met de RRDtool [13]), een aanpasbaar CSS-bestand, admin login en bewerken van de

database via de web interface, enzovoort.

Conclusie

Darkstat is een erg stabiele en snelle netwerk monitoring tool, die precies doet wat' ie moet doen - verkeer analyseren. Verder werkt het zonder enige problemen, ondergaat continue ontwikkeling en zal in de komende versie veel nieuwe en interessante mogelijkheden bieden. Voorlopig wens ik je veel succes met de jacht op "verkeers-overtreders" op je lokale netwerken!

Links

[1] http://purl.org/net/darkstat [Homepage van darkstat]
[2] http://www.ntop.org/ [Homepage van ntop]
[3] http://dmr.ath.cx/net/darkstat/darkstat-2.6.tar.gz [Download]
[4] http://yallara.cs.rmit.edu.au/~emikulic/_/darkstat-2.6.tar.gz [Download Mirror #1]
[5] http://neo5k.de/downloads/files/darkstat-2.6.tar.gz [Download Mirror #2]
[6] http://ftp.debian.org/debian/pool/main/d/darkstat/ [Debian Pakketten]
[7] http://www.tcpdump.org/ [Home van libpcap]
[8] http://www.courtesan.com/sudo/ [Home van sudo]
[9] http://www.iana.org/assignments/port-numbers [IANA Poort-Nummers]
[10] ftp://ftp.rfc-editor.org/in-notes/rfc792.txt [RFC 792 - ICMP]
[11] ftp://ftp.rfc-editor.org/in-notes/rfc793.txt [RFC 793 - TCP]
[12] ftp://ftp.rfc-editor.org/in-notes/rfc768.txt [RFC 768 - UDP]
[13] http://people.ee.ethz.ch/~oetiker/webtools/rrdtool/ [Home van RRDtool]

Site onderhouden door het LinuxFocus editors team	Vertaling info:
© Mario M. Knopf	de --> -- : Mario M. Knopf (homepage)
"some rights reserved" see linuxfocus.org/license/	de --> en: Mario M. Knopf (homepage)
http://www.LinuxFocus.org	en --> nl: Guus Snijders <ghs(at)linuxfocus.org>

2005-01-14, generated by lfparser_pdf version 2.51