by Mario M. Knopf (homepage)

About the author:

Mario si occupa di Linux, reti e altri temi legati alla sicurezza.

darkstat – un analizzatore di traffico di rete

Abstract:

Questo articolo presenta un analizzatore di traffico di rete, "*darkstat*", e fornisce una panoramica sulla installazione e l'uso del programma.

Translated to English by:
Mario M. Knopf (homepage)

Introduzione

"*darkstat*" [1] è un monitor di rete, che analizza il traffico di rete e genera sulla base di queste delle statistiche HTML. Queste statistiche posso dunque essere fruite con un web browser. A questo scopo l'autore del programma, Emil Mikulic, usava "*ntop*" [2] strumento di vecchia data. Ma era poco soddisfatto della sua stabilità e di alcuni problemi legati all'uso della memoria. Per questo ha sviluppato "*darkstat*". Le statistiche si riferiscono alla comunicazione tra gli host, il traffico generato e le porte usate. In più si possono avere diagrammi sull'intervallo temporale in cui i pacchetti sono stati analizzati.

Installazione

I sorgenti del programma "darkstat" sono qui [3]. Alternativamente ci sono dei mirror [4] e [5]. Chi cercasse il package per Debian cerchi qui [6].

"*darkstat*" dipende, come molti analizzatori di rete, dalla "*libpcap*" [7]. Questa libreria, usata dagli analizzatori di pacchetti, fornisce una comoda interfaccia per catturare e analizzare i pacchetti al livello del dispositivo di accesso alla rete. Per installare "*darkstat*" serve dunque questa libreria.

Si deve poi compilare come al solito "*./configure && make && make install*". Naturalmente l'ultima istruzione deve essere da root.

Cominciamo

"*darkstat*" presenta dei parametri che possono essere impostati all'esecuzione. Comunque, per un primo test, un avvio senza parametri va benissimo. Per poter lavorare il programma deve essere avviato da root o con un "*sudo*" appositamente configurato [8]:

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

Immaginiamo che abbiate le nozioni base di Amministratore di Sistema.
Di solito queste due sono d'oro:

#1) Rispettare la privacy altrui.
#2) Pensare prima di digitare.

Password:
```

Dopo che l'utente autorizzato ha immesso la password, "*darkstat*" parte e stampa diversi messaggi di stato:

```
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.
```

Dato che la partenza è stata buona e che l'output è perentorio, possiamo dare un'occhiata ai possibili parametri che accetta il software.

Opzioni d'avvio

Come detto prima, "*darkstat*" fornisce diverse opzioni, che gli si possono dare all'avvio. I parametri sono:

l'opzione "*−i*" specifica l'interfaccia di rete.

darkstat −i eth1

Avviato senza parametri "*darkstat*" apre la porta 666 (brrr..). Si può cambiare la porta di default col parametro "*−p*":

darkstat −p 8080

Per associare una porta a una specifica interfaccia di rete si può usare l'opzione "*−b*". In quest'esempio è associato l'indirizzo di local loopback:

darkstat −b 127.0.0.1

La risoluzione DNS può essere inibita col parametro "*−n*". Questo può essere utile a coloro che sono senza una linea dedicata.

darkstat −n

L'opzione "−*P*" impedisce a "*darkstat*" di impostare come promiscuo l'accesso alla scheda di rete ("*promiscuous mode*"). Questo non è tuttavia consigliabile perché "*darkstat*" in questo modo intercetta e analizza solo i pacchetti indirizzati al MAC della scheda di rete sulla quale è in ascolto, perdendo così tutto il resto di traffico: inutile direi.

darkstat −P

Il parametro "−*l*" attiva un filtro "*SNAT*"per la rete locale. "*SNAT*" è acronimo di "*Source Network Address Translation*" (Traduzione degli indirizzi sorgente di rete) e significa che il router sostituisce l'indirizzo IP del client (privato) col suo (pubblico). Ogni pacchetto viene dunque instradato in vece del client.

darkstat −l 192.168.1.0/255.255.255.0

Col parametro "−*e*" si può implementare un filtro sul pacchetto.

darkstat −e "port not 22"

Dalla versione 2.5 in poi "*darkstat*" può essere slegato dalla shell ed eseguito come demone.

darkstat −−detach

Col parametro "−*d*" si può specificare dove "*darkstat*" deve creare il suo database.

darkstat −d /directory

L'opzione "−*v*" attiva la modalità prolissa ("*verbose mode*"):

darkstat −v

La versione del software e la sua sintassi completa si ottiene col parametro "−*h*".

darkstat −h

Cattura

Dopo l'avvio di "*darkstat*" si può puntare col browser a "*http://localhost:666/*", di default. Qui ci sono alcune statistiche generate dalla partenza al momento corrente:

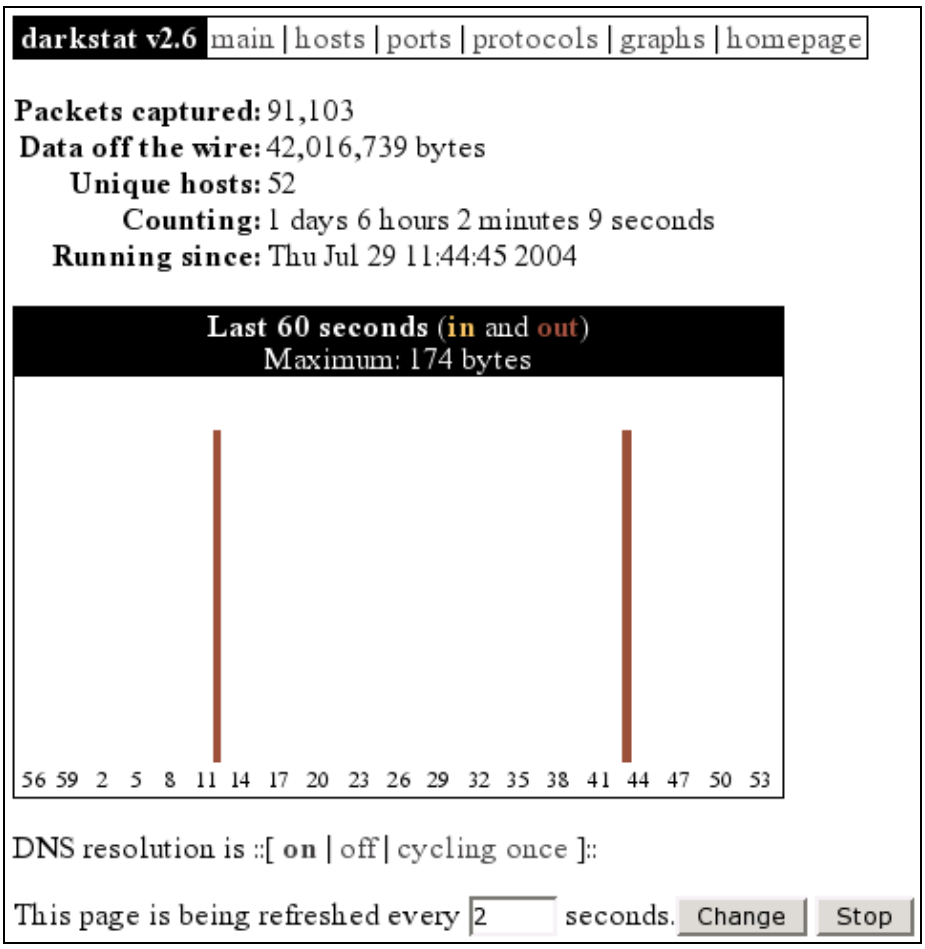
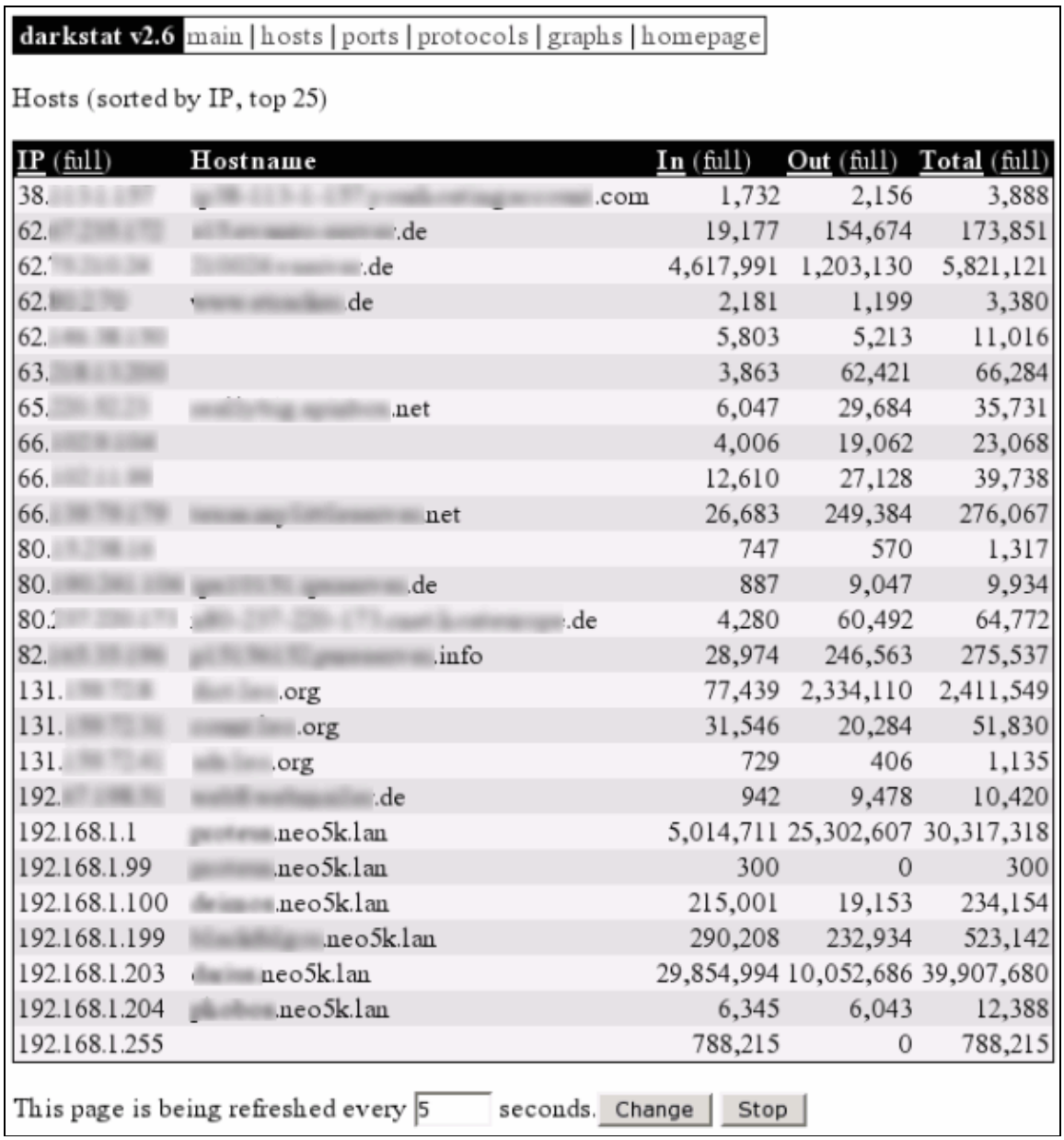


Figura 1: la home di darkstat

Gli "*hosts*" sono tutte la macchine che stanno comunicando. Queste possono essere ordinate in base al traffico generato, oppure per indirizzo IP. In questo modo si possono rapidamente conoscere le macchine che hanno generato più traffico nella LAN. In questo modo l'amministratore di rete può avere informazioni utili a venire a capo di un problema. Per esempio in questo screenshot sarebbe il client con questo IP "*192.168.1.203*".



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

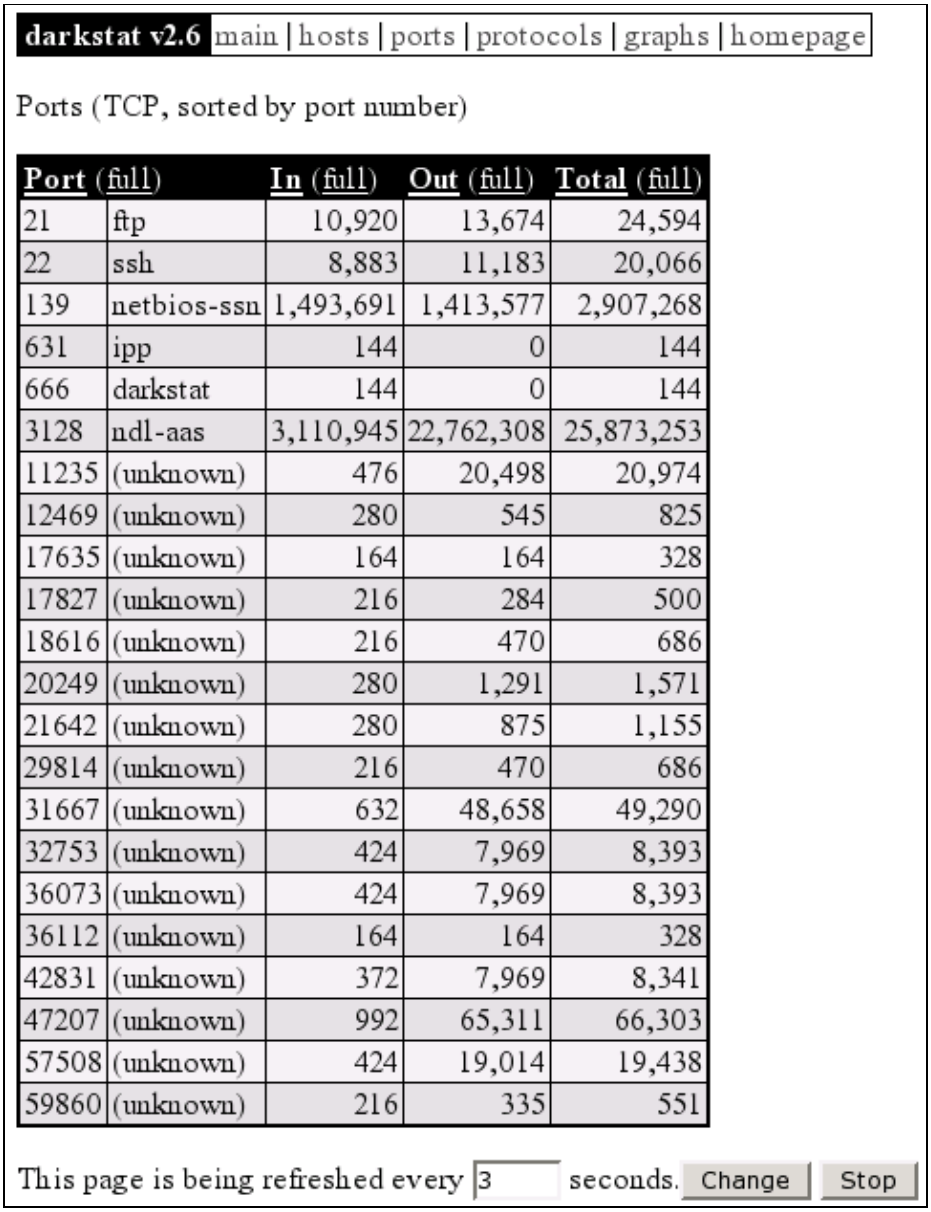
Hosts (sorted by IP, top 25)

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

Figura 2: hosts in darkstat

Nella figura 3 si vedono le porte usate dalle applicazioni server e client. Si possono riconoscere subito le porte usate dei demoni: *21 (FTP)*, *22 (SSH)*, *139 (Samba)*, *631 (CUPS)*, *666 (darkstat)*, *3128 (Squid)*. I due servizi "*dhcpd*" e "*dnsmasq*" non sono visibili perché parlano UDP. Tutte le altre porte sopra la 1024 non sono riservate e sono usate dalle applicazioni client per la comunicazione. Il server proxy "*squid*" fa eccezione, perché utilizza la 3128 di default. Si può avere la lista completa e aggiornata delle porte e dei servizi ad esse associati qui alla IANA [9], organo ufficiale responsabile di queste assegnazioni. Oppure si può andare qui (ma non ci sono tutte) "*/etc/services*".



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

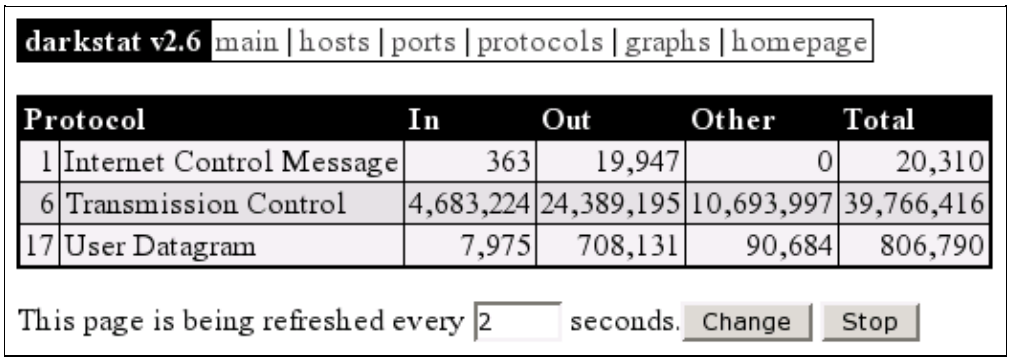
Ports (TCP, sorted by port number)

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	3,110,945	22,762,308	25,873,253
11235	(unknown)	476	20,498	20,974
12469	(unknown)	280	545	825
17635	(unknown)	164	164	328
17827	(unknown)	216	284	500
18616	(unknown)	216	470	686
20249	(unknown)	280	1,291	1,571
21642	(unknown)	280	875	1,155
29814	(unknown)	216	470	686
31667	(unknown)	632	48,658	49,290
32753	(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
57508	(unknown)	424	19,014	19,438
59860	(unknown)	216	335	551

This page is being refreshed every 3 seconds. Change Stop

Figura 3: porte darkstat

In questa figura si vedono i protocolli "*ICMP*", "*TCP*" e "*UDP*" per la trasmissione dei file, che sono parte di una sessione di comunicazione. Chi fosse interessato in questi protocolli troverà in questi RFC una introduzione [10], [11] e [12].



darkstat v2.6 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	24,389,195	10,693,997	39,766,416
17	User Datagram	7,975	708,131	90,684	806,790

This page is being refreshed every 2 seconds. Change Stop

Figura 4: protocolli darkstat

L'ultimo screenshot mostra un sommario degli ultimi grafici:

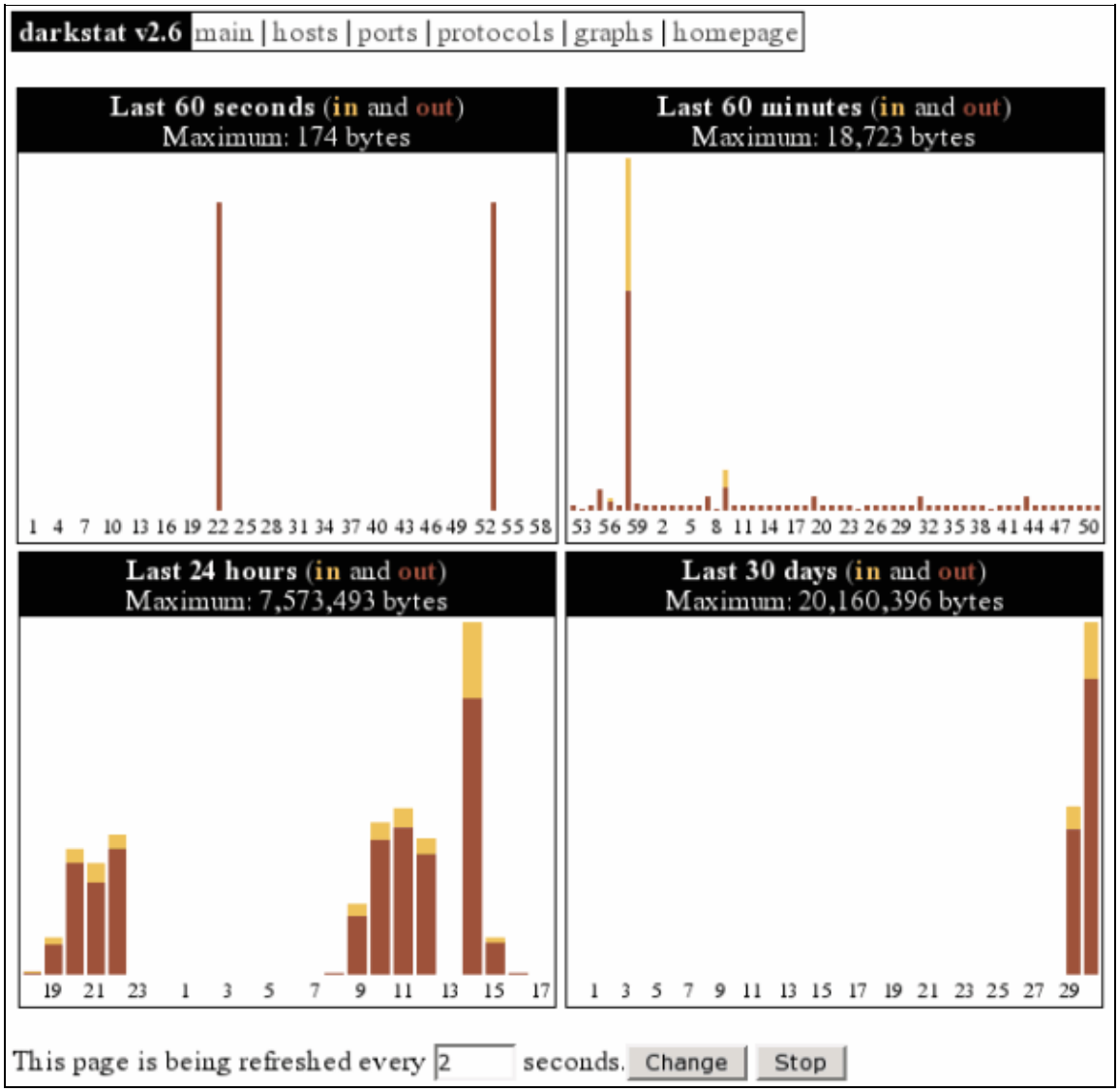


Figura 5: un grafico darkstat

Sviluppi Futuri

La versione 2.6 di "*darkstat*" della quale abbiamo discusso è sfortunatamente dipendente da "*pthreads*". Questo causa problemi in alcune piattaforme (per esempio NetBSD). Per questo l'autore ha deciso di interrompere il progetto 2.x e di aprire il branch 3.x per eliminare questa limitazione.

Nella prossima versione verra introdotta la possibilità di catturare i pacchetti da più interfacce simultaneamente. Verrà introdotto un parser per un file di configurazione, una miglioria nel layout grafico dei diagrammi (comparabile con il RRDtool [13]), un CSS customizzabile, un sistema di logon e la possibilità di editare il DB dal web e altro ancora.

Conclusioni

"*darkstat*" è uno strumento di monitoraggio di rete molto stabile e veloce, che fa bene quello che deve fare: analizzare il traffico. In più non ha preoblemi, è in continuo sviluppo e presto nelle nuove versioni avrà numerose novità interessanti. Così vi auguro di scovare con successo chi fa il "furbo" nella vostra rete.

Links

[1] http://purl.org/net/darkstat [Home of darkstat]
[2] http://www.ntop.org/ [Home of 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 Packages]
[7] http://www.tcpdump.org/ [Home of libpcap]
[8] http://www.courtesan.com/sudo/ [Home of sudo]
[9] http://www.iana.org/assignments/port−numbers [IANA Port−Numbers]
[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 of RRDtool]

Translation information:
de −−> −− : Mario M. Knopf (homepage)
de −−> en: Mario M. Knopf (homepage)
en −−> it: Davide Lo Vetere <glitch/at/tiscali.it>

2005−01−10, generated by lfparser_pdf version 2.51