by Mario M. Knopf (homepage)

About the author:

O Mario gosta de se manter ocupado com o Linux, redes e outros tópicos relacionados com segurança.

darkstat – Um analisador de tráfego

Abstract:

Este artigo apresenta o analisador de tráfego "*darkstat*" e dá uma perspectiva acerca da instalação e da utilização deste programa.

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

Introdução

O "*darkstat*" [1] é um programa de monitorização de redes que analisa o tráfego resultante de uma rede e gera com base nestes dados várias estatísticas no formato de HTML. Estas estatísticas podem ser vistas num browser de um modo comfortável. Para este propósito o autor do programa, Emil Mikulic, utilizou o "*ntop*" [2] durante um longo período de tempo. Mas ele ficou descontente com os seus problemas de estabilidade e má utilização da memória. Por esta razão desenvolveu o "*darkstat*". As estatísticas apresentadas referem–se à comunicação entre as diferentes máquinas, o tráfego que consequente e o número das portas utilizados, alternativamente os protocolos envolvidos na transmissão. Adicionalmente podem ser vistos gráficos com períodos de tempo e um pequeno resumo dos pacotes analisados desde que o programa foi iniciado.

Instalação

As fontes do programa "darkstat" podem ser obtidas directamente em [3]. Em alternativa os dois mirrors podem ser visitados em [4] e [5]. Se alguém procura por pacotes Debian pode encontrá–los em [6].

O "*darkstat*" também depende, como muitos outros programas de monitorização, do ficheiro da "*libpcap*"[7]. Este é uma biblioteca que é usada por sniffers e fornece–lhes uma interface para capturar e analisar os pacotes dos dispositivos de rede. Assim para instalar o "*darkstat*" precisa desta biblioteca.

Depois tem de o instalar com os três passos bem conhecidos "*./configure && make && make install*". É importante que a última instrução seja feita com permissões de root.

Inicio

O "*darkstat*" oferece alguns parÃ¢metros que podem ser definidos no arranque do programa. Contudo para começar um arranque sem nenhuma opção basta. Mas o programa tem de ser iniciado como root ou com privilégios "*sudo* [8]:

```
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:
```

Depois do utilizador ter introduzido a sua palavra−passe, o "*darkstat*" arranca e apresenta várias mensagens de estado:

```
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.
```

Visto que o teste ocorreu com sucesso e o output produzido explica−se a si mesmo, podemos dar uma vista de olhos aos possíveis parâmetros de arranque.

Opções de arranque

Como referido anteriormente o "*darkstat*" fornece várias opções, algumas das quais podem ser dadas durante o arranque. Os tais parâmetros são:

Com a opção "*−i*" pode especificar qual a interface a ser monitorizada.

darkstat −i eth1

Iniciado sem nenhum parâmetro especial o "*darkstat*" abre a porta priveligiada 666. Pode prevenir−se deste hábito, quando o arranca com o parâmetro "*−p*":

darkstat −p 8080

No sentido de registar num determinado porto e numa determinada interface, pode usar a opção *−b*. Neste exemplo, o registo é feito no endereço de loopback:

darkstat −b 127.0.0.1

A resolução de DNS persistente pode ser prevenida com o parâmetro "*−n*". Isto pode ser bom para as pessoas sem uma linha dedidada ou alguma largura de banda.

darkstat −n

Use a opção "*−P*" para prevenir que o "*darkstat*" ponha a interface no "*modo promíscuo*". Contudo isto não é recomendável visto que assim o "*darkstat*" só captura e analisa pacotes que são destinada ao MAC da interface de rede da estação monitorizada e todos os outros pacotes são rejeitados.

darkstat −P

O parâmetro "*−l*" activa o comportamento correcto "*SNAT*" na rede local. O "*SNAT*" significa "*Source Network Address Translation*" e quer dizer que o seu router (encaminhador) mascára os endereços locais IP do cliente com o seu próprio endereço público. Depois envia o pedido original do cliente.

darkstat −l 192.168.1.0/255.255.255.0

Com o parâmetro "*−e*" pode fazer filtragem de pacotes.

darkstat −e "port not 22"

A partir da versão 2.5 pode separar o "*darkstat*" do terminal de arranque. Assim trabalha como um demónio.

darkstat −−detach

Através do parâmetro "*−d*" pode especificar o directório onde o "*darkstat*" cria a sua base de dados.

darkstat −d /directory

A opção "*−v*" activa o "*modo verboso*":

darkstat −v

Se estiver interessado na versão do "*darkstat*" ou na sua utilização mais completa e sintaxe, pode experimentar o parâmetro "*−h*".

darkstat −h

Utilização

Depois do arranque do "*darkstat*" pode apontar o seu browser para "*http://localhost:666/*", o que é o comportamento por omissão. Agora pode dar uma vista de olhos pelas estatísticas resumidas e por alguns gráficos gerados desde que o programa arrancou:

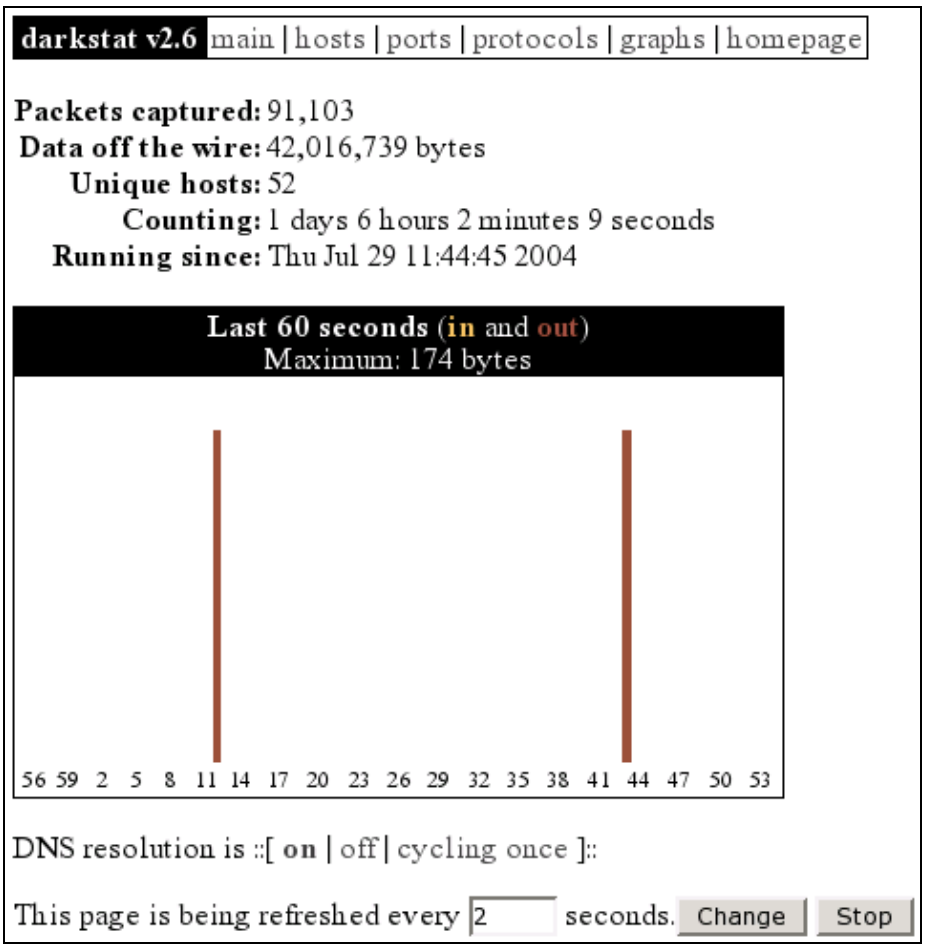
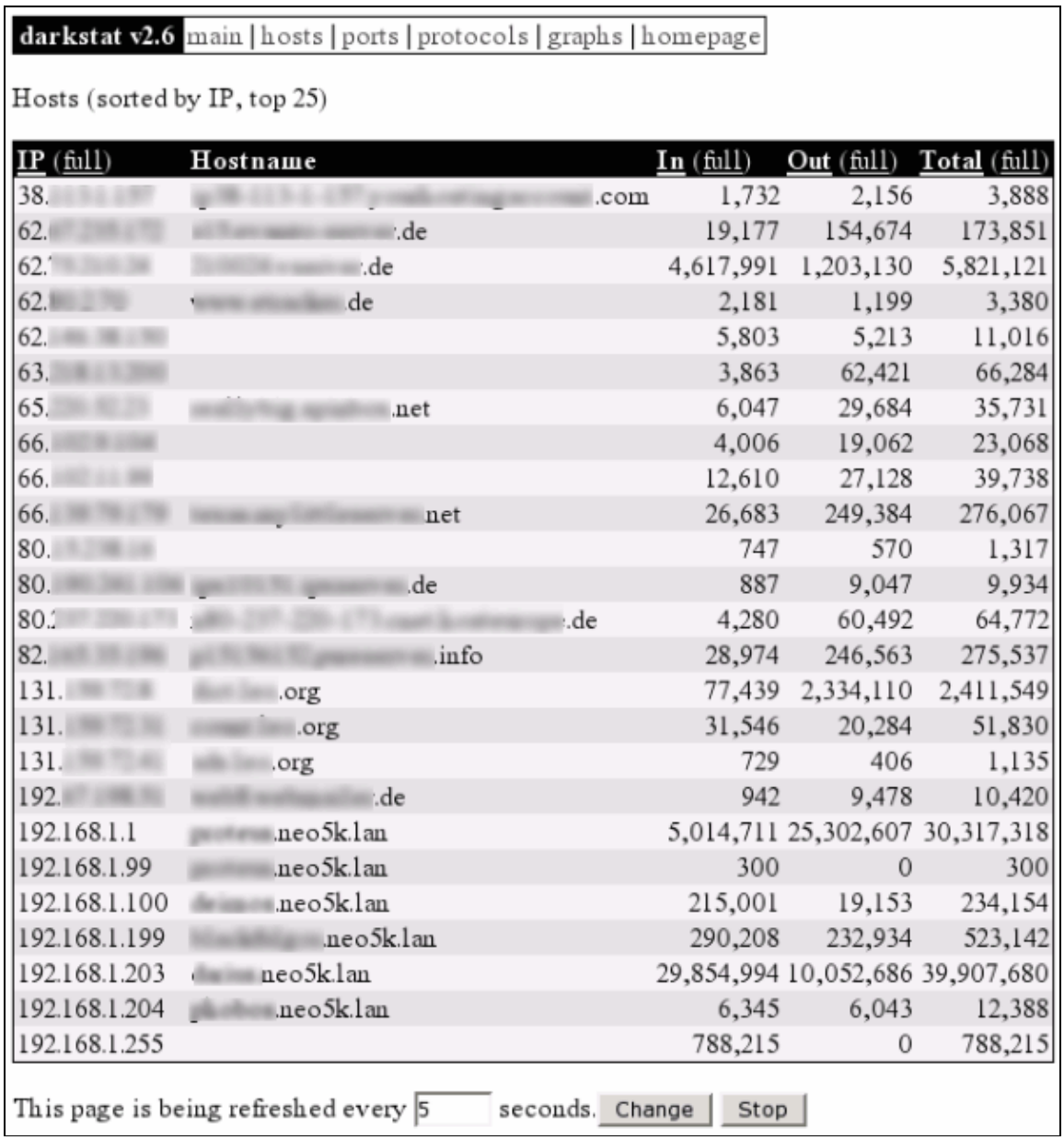


Ilustração 1: darkstat main

Na parte dos "*hosts*" pode ver todas as máquinas que tomam partido na comunicação. Tal pode suceder−se dado o tráfego causado ou pelo endereço IP. Através desta possibilidade é possível detectar as máquinas que mais tráfego produziram na rede local, de um modo rápido. Assim um adaministrador de sistema tem possibilidade de obter a razão de algum problema. Por exemplo no próximo ecrã tal corresponderia ao cliente com o endereço local "*192.168.1.203*".



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

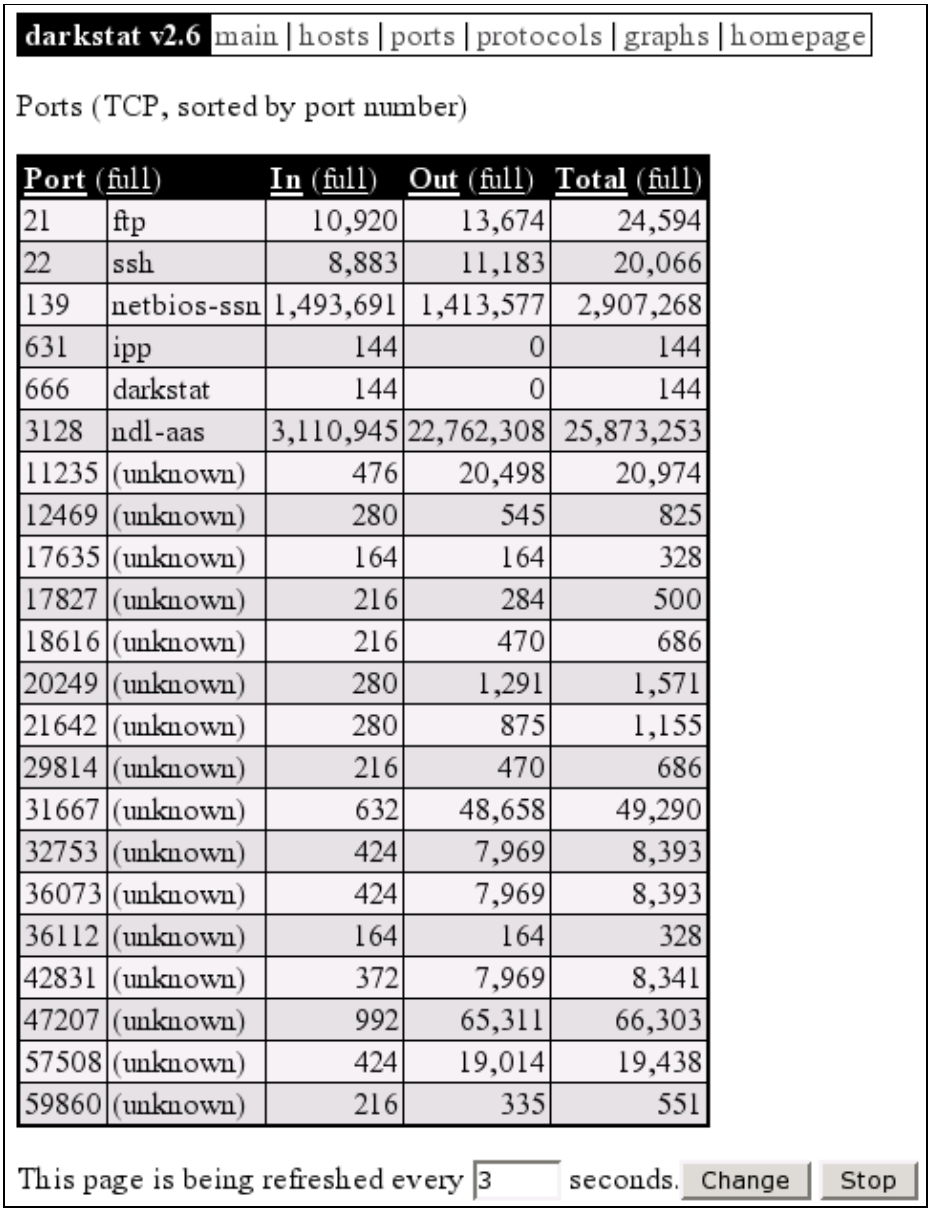
Hosts (sorted by IP, top 25)

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

Ilustração 2: darkstat hosts

Na Ilustração 3 pode ver os números dos portos que são usados pelas aplicações clientes e servidoras. Pode reconhecer imediatamente o número das portas usados pelos seguintes demónios: *21 (FTP)*, *22 (SSH)*, *139 (Samba)*, *631 (CUPS)*, *666 (darkstat)*, *3128 (Squid)*. Contudo, os dois serviços "*dhcpd*" e o "*dnsmasq*" não são visíveis, porque estes serviços comunicam via "*UDP*". Todos os outros portos superiores a 1024 são não priveligiados e foram usados pelas aplicações clientes para a comunicação. O servidor proxy "*squid*" representa a excepção, porque usa o porto 3128 por omissão. Pode ver uma lista de todos os portos atrivuídos na IANA [9], a qual é responsável por eles. Em alternativa pode dar uma vista de olhos no ficheiro "*/etc/services*".



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

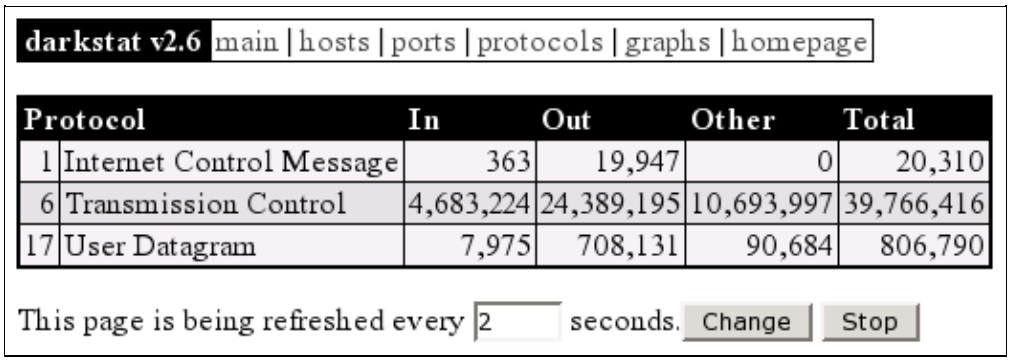
Ports (TCP, sorted by port number)

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

Ilustração 3: darkstat ports

Na figura seguinte podem ver os protocolos "*ICMP*", "*TCP*" e "*UDP*" envolvidos na transmissão de ficheiros. Se alguém estiver interessado nestes protocolos, encontrará boas instruções nos seguintes RFCs [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

Ilustração 4: darkstat protocols

O último ecrã mostra um resumo dos tempos de recolha comos gráficos:

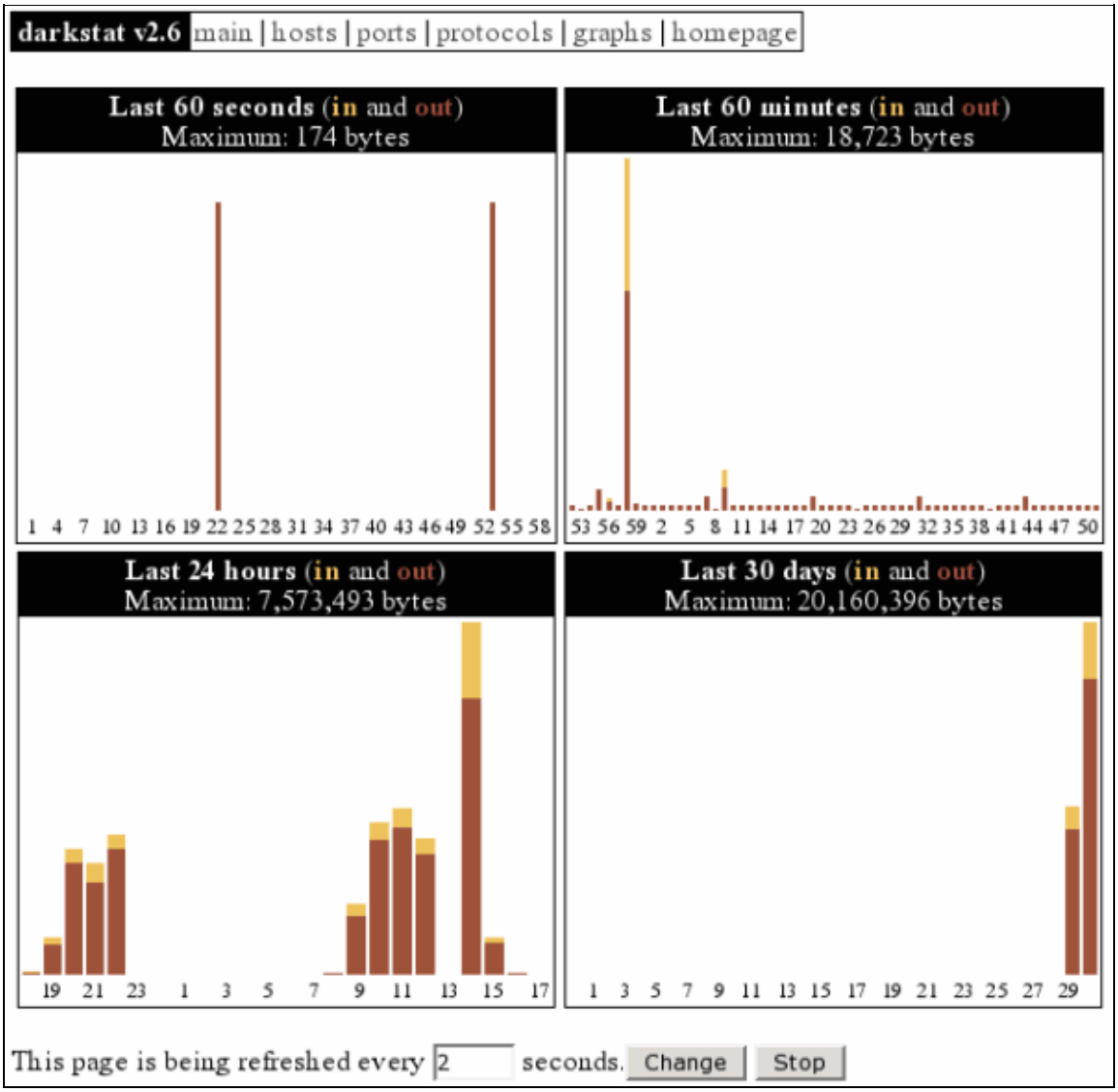


Ilustração 5: darkstat graphs

Aspectos Futuros

A versão 2.6 do "*darkstat*" que disctutimos aqui, infelizmente é dependente dos "*pthreads*". O que causa problemas noutras plataformas (exemplo: NetBSD). Por esta razão o autor do programa Emil Mikulic decidiu não desenvolver mais a versão actual e começou a trabalhar na versão 3.x.

Na nova versão estão a ser implementadas coisas como a captura simultânea em várias interfaces, um ficheiro de configuração, um output melhorado para os diagramas (algo comparativo ao RDDtool [13]), um ficheiro personalizado CSS, um login para o administrador e a edição da base de dados através da interface web.

Conclusão

O "*darkstat*" é muito estável e é um utilitário de monitorização de rede bastante rápido servindo exclusivamente o propósito para que foi desenhado – analisar tráfego. Para além disto, trabalha sem problemas e encontra–se em constante desenvolvimento e terá muitas novas e interessantes características na nova versão. Despeço–me desejando sucesso na pesquisa dos "pecadores de tráfego" na sua rede local.

Links

[1] http://purl.org/net/darkstat [Página oficial do darkstat]
[2] http://www.ntop.org/ [Página oficial do 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/ [Página oficial da libpcap]
[8] http://www.courtesan.com/sudo/ [Página oficial do sudo]
[9] http://www.iana.org/assignments/port–numbers [IANA Números dos portos]
[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/ [Página oficial do RRDtool]

Translation information:
de −−> −− : Mario M. Knopf (homepage)
de −−> en: Mario M. Knopf (homepage)
en −−> pt: Bruno Sousa <bruno/at/linuxfocus.org>

2005−01−10, generated by lfparser_pdf version 2.51