por Mario M. Knopf (homepage)

Sobre el autor:

A Mario le divierte estar entretenido con Linux,con las redes y otros asuntos relacionados con la seguridad.

darkstat – Un analizador de tráfico de red

Resumen:

En este artículo se presenta el analizador de tráfico de red "*darkstat*" y dando una visión general de su instalación, puesta en marcha y uso.

Traducido al español por:
Alberto Pardo
<apardoyo(at)yahoo.es>

Introducción

"*darkstat*" [1] es una herramienta para monitorizar una red, el cual analiza el tráfico de la red y en base a los datos obtenidos genera un informe estadístico en formato HTML. Este informe se puede ver con cualquier navegador. Para este proposito, el autor del programa, Emil Mikulic, ha estado usando el programa "*ntop*" [2] durante bastante tiempo. Pero no esta contento con su estabilidad y su mal uso de la memoria. Por esta razón ha desarrollado "*darkstat*". Entre las observaciones que realiza el programa , permite: realizar la estadística de direcciones que se generan en la comunicación entre hosts,el tráfico que se produce y los diferentes números de puerto usados por los diversos protocolos. Adicionalmente , el programa permite obtener un breve resumen y gráficos por periodos de tiempo de los paquetes analizados desde que se empieza a ejecutar el programa.

Instalación

Las fuentes del programa "darkstat" puede encontrarse directamente en [3]. Como alternativa , pudes visitar los siguientes mirrors [4] y [5]. Si alguien quiere , puede mirar los paquetes Debian en [6].

"*darkstat*" tambien depende,como otras herramientas de monitorización de red, del fichero "*libpcap*" [7]. Es una libreria utilizada por los sniffers y les proporciona un interface para capturar y analizar paquetes desde los dispositivos de la red.Para instalar "*darkstat*" necesitarás esta libreria.

Tendrás que compilarla de la siguiente manera:"*./configure && make && make install*". Es importate, que almenos la última instrución la ejecutes con los privilegios de "root".

Empezando

"*darkstat*" ofrece algunos parámetros, que pueden activarse al empezar el programa. De cualquier forma, la primera prueba se puede realizar sin activar ninguna opción. Para poder ejecutar correctamente el programa, se ha de inicializar como "root" o con los privulegios "*sudo*"−privileges [8]:

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

Confiamos que tengas una lectura normal desde el Administrador del Systema local.
Es importante que tengas en cuenta estas dos cosas:

#1) Respeta la privacidad de los demas.
#2) Piensa antes de escribir.

Password:
```

Después de que el usuario autorizado haya introducido su password, "*darkstat*" obtiene e presenta varios mensajes 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.
```

Tras el test y con la descripción de las salidas, podemos mirar los parámetros iniciales.

Opciones de arranque

Tal como se mencionó previamente,z"*darkstat*" hay varias opciones, que se puede proporcionar al inicio. Estos parámetros son:

Con la opción "−*i*" se puede especificar el interface a monotorizar.

darkstat −i eth1

Si "*darkstat*" se ejecuta sin parámetros iniciales, el programa abre automaticamente el puerto 666. Se puede cambiar este puerto mediante el parámetro "−*p*":

darkstat −p 8080

Para ocultar un puerto especifico para un dispositivo concreto, puedes usar la opción "−*b*". En el siguiente ejemplo , ocultamos la dirección local de "loopback":

darkstat −b 127.0.0.1

Con el parámetro "*−n*" se puede prevenir el uso de la resolución DNS. Esta opción es útil para gente sin una red de tasa de flujo constante o linea dedicada .

darkstat −n

La opción "*−P*" previene que "*darkstat*" tenga el interface en "*promiscuous mode*". De todos modos, esto no es recomendable , ya que "*darkstat*" sólo captura los paquetes que son direccionados con la dirección MAC del interface de red que esta siendo monotorizado. El resto de paquetes son rechazados.

darkstat −P

El parametro "*−l*" activa correctamente "*SNAT*"− en la red local. "*SNAT*" simboliza "*Source Network Address Translation*" y significa que tu router enmascara la dirección IP local con su dirección pública. Des esta manera el programa envia sus requerimientos , en lugar de los requerimientos originales del cliente.

darkstat −l 192.168.1.0/255.255.255.0

Con el parámetro "*−e*" se puede ejecutar la expresión para filtra paquetes.

darkstat −e "port not 22"

A partir de la versión 2.5 "*darkstat*" puede funcionar separado del terminal de inicio. Así trabaja como un "daemon".

darkstat −−detach

Con el parámetro "*−d*" se le especifica el directorio donde "*darkstat*" crea su base de datos.

darkstat −d /directory

La opción "*−v*" activa "*verbose mode*":

darkstat −v

Si estas interesado en el número de versión de "*darkstat*" o en su completo uso y sintaxis, prueba con el parámetro "*−h*".

darkstat −h

Manejo

Después de haber ejecutado por primera vez "*darkstat*" se puede escribir en el navegador "*http://localhost:666/*", que la dirección web por defecto . Se podrá observar un resumen de las estadisticas y unos pocos gráficos obtenidos desde que el programa empezó a ejecutarse:

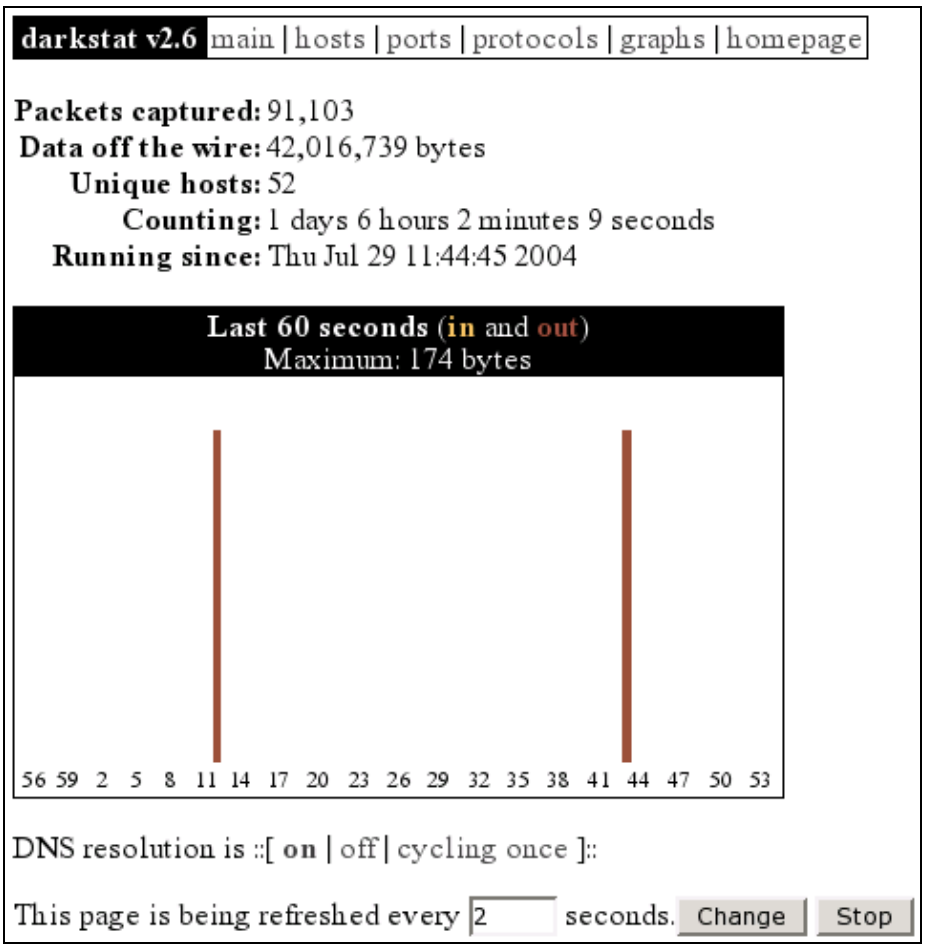
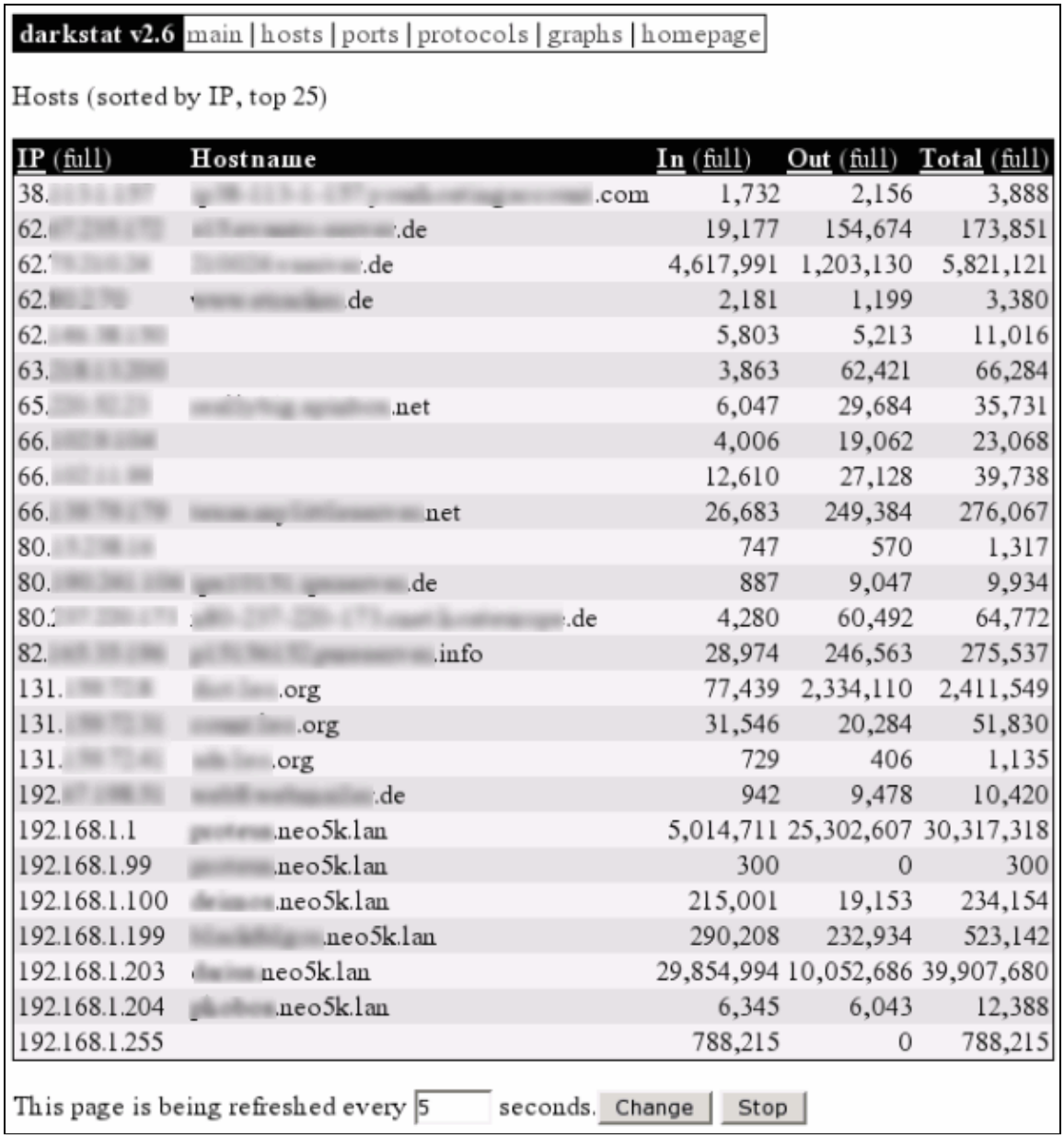


Ilustración 1: La pantalla principal de darkstat

En la posición "*hosts*" se pueden ver todas las máquinas que forman parte de las comunicaciones. Se puede organizar por tráfico o por su dirección IP particular.Con esta posibilidad, se puede detectar las maquinas que estan produciendo un mayor tráfico en la red local , de forma my rápida. De esta manera, los administradores de sistemas tiene la oportunidad de conocer la causa del problema. Por ejemplo, la siguiente pantalla corresponde a un cliente con la dirección local IP "*192.168.1.203*".



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

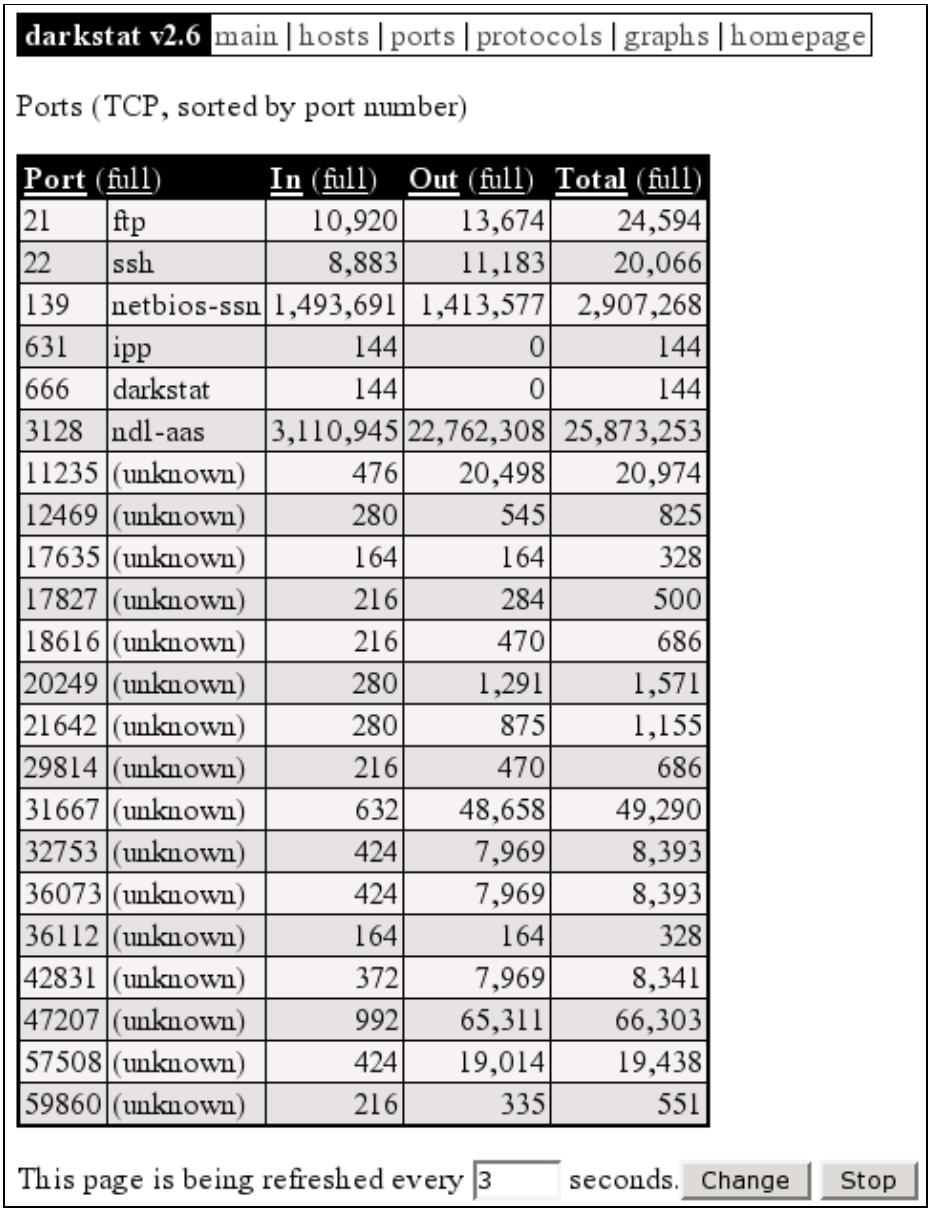
Hosts (sorted by IP, top 25)

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

Ilustración 2: Los hosts en darkstat

En la ilustración 3 se pueden ver el número de los ports que son usados por el server y las aplicaciones cliente. Se reconoce rápidamente los ports que están siendo utilizados por los siguientes "daemons": *21 (FTP)*, *22 (SSH)*, *139 (Samba)*, *631 (CUPS)*, *666 (darkstat)*, *3128 (Squid)*. Sin embargo, hay dos servicios , "*dhcpd*" y "*dnsmasq*" que no son visibles. Esto es debido a que estos dos servicios se comunican via "*UDP*".Todos lo puertos mayores 1024 no son privilegiados y son utilizados por aplicaciones cliente para comunicaciones. El proxy server "*squid*" representa la excepción, por que usa por defecto el puerto 3128. Se Puede ver una lista actualizada de los números de los puertos que es IANA [9], la cual es responsable de esta lista. Artenativamente se puede mirar en el fichero "*/etc/services*".



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

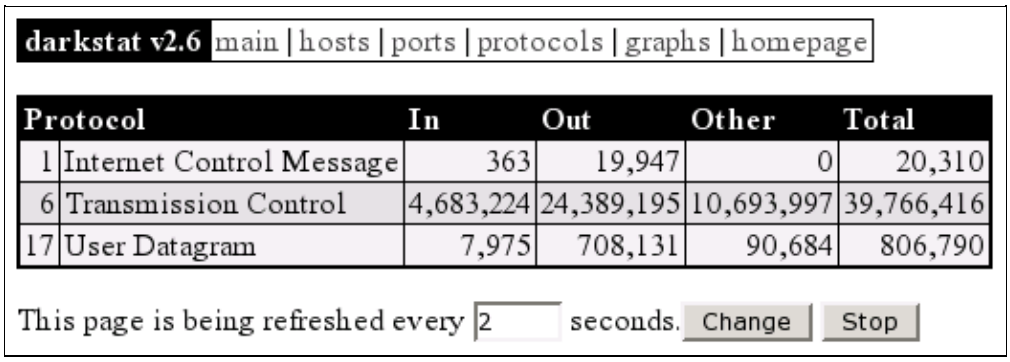
Ports (TCP, sorted by port number)

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

Ilustración 3: Los puertos en darkstat

En la siguiente figura se puede observar los protocolos "*ICMP*", "*TCP*" y "*UDP*"para la transmisión de ficheros, que forman parte del proceso de comunicación. Si alguien se interesa en estos protocoles,puede encotrar buenas referencias en: el las RFCs odesde [10], [11] hasra [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

Ilustración 4: Los protocolos en darkstat

La última pantalla muestra un resumen de gráficos por periodos de tiempos:

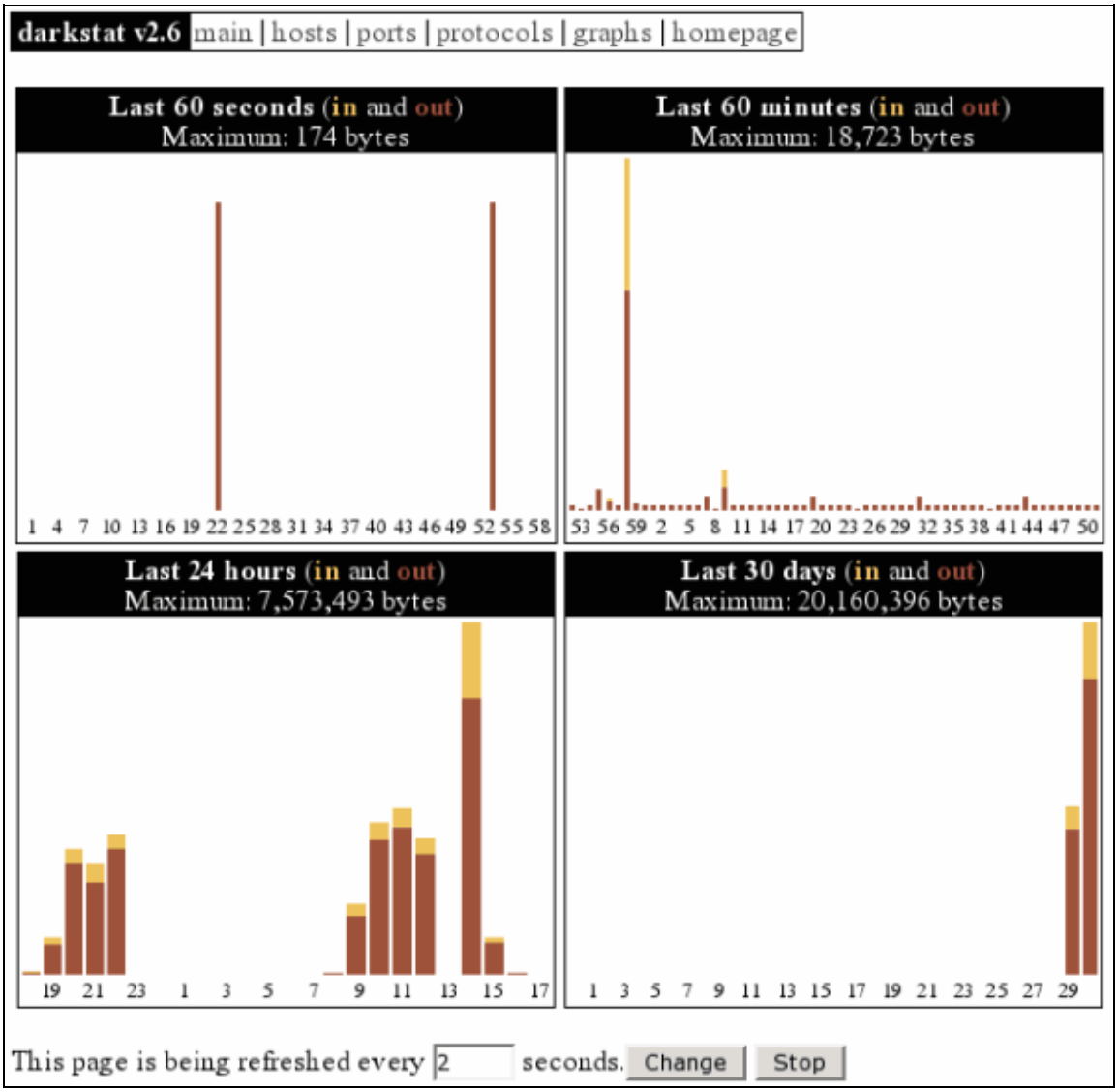


Ilustración 5: Las gráficas en darkstat

Prespectica de futuro

La versión 2.6 de "*darkstat*", de la que hemos hablado aquí, por degracia depende de "*pthreads*". Con lo que tiene problemas en otras plataformas (ejemplo : netBSD) Por esta razón su autor Emil Mikulic decidio no desarrollar ninguna nueva versión 2.x y centrar su trabajo en la 3.x.

La nueva versión implementará nuevas cosas como: captura de paquetes desde varios interfaces simultaneamente,un fichero de configuración del programa analizador, mejora en la presentación gráfica de los diagramas (comparable con RRDtool [13]),mejoras en el fichero CSS, administración del login y edición de la base de datos atraves de un interface web, etc..

Conclusiones

"*darkstat*" es una herramienta de monitorización lo suficientemente estable y rápida que cumple su función de analizar el tráfico. Funciona sin problemas, está en constante desarrollo y tendrá nuevas e interesantes caráteristicas en las siguientes versiones. Deseo que tengais muchos exitos en la busqueda de "tráfico pecaminoso" en vuestras redes locales.

Enlaces

[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 [Descarga]
[4] http://yallara.cs.rmit.edu.au/~emikulic/_/darkstat−2.6.tar.gz [Mirror #1 de descarga]
[5] http://neo5k.de/downloads/files/darkstat−2.6.tar.gz [Mirror #2 de descarga]
[6] http://ftp.debian.org/debian/pool/main/d/darkstat/ [Paquetes Debian]
[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]

Contactar con el equipo de LinuFocus © Mario M. Knopf "some rights reserved" see linuxfocus.org/license/ http://www.LinuxFocus.org	Información sobre la traducción: de −−> −− : Mario M. Knopf (homepage) de −−> en: Mario M. Knopf (homepage) en −−> es: Alberto Pardo <apardoyo(at)yahoo.es>

2005−02−01, generated by lfparser_pdf version 2.51