NAME

tcptrack − Monitor TCP connections on the network

SYNOPSIS

tcptrack [**-dfhvp**] [**-r** *seconds*] **-i** *interface*
[*filter expression*]

DESCRIPTION

tcptrack displays the status of TCP connections that it sees on a given network interface. tcptrack monitors their state and displays information such as state, source/destination addresses and bandwidth usage in a sorted, updated list very much like the top(1) command.

The filter expression is a standard pcap filter expression (identical to the expressions used by tcpdump(8)) which can be used to filter down the characteristics of TCP connections that tcptrack will see. See tcpdump(8) for more information about the syntax of this expression.

OPTIONS

−d Only track connections that were started after tcptrack was started. Do not try to detect existing connections.

−f Enable fast average recalculation. TCPTrack will calculate the average speeds of connections by using a running average. TCPTrack will use more memory and CPU time, but averages will seem closer to real time and will be updated more than once per second and may be more accurate under heavy load. The number of times per second that averages will be recalculated in fast mode is a compile-time setting that defaults to 10 times per second.

−h Display command line help

−i [interface]
Sniff packets from the specified network interface.

−p Do not put the interface being sniffed into promiscuous mode.

−r [seconds]
Wait this many seconds before removing a closed connection from the display. Defaults to 2 seconds. See also the pause interactive command (below).

−v Display tcptrack version

INTERACTIVE COMMANDS

The following keys may be pressed while tcptrack is running to change runtime options:

p - Pause/unpause display. No new connections will be added to the display, and all currently displayed connections will remain in the display.

q - Quit tcptrack.

s - Enable/disable sorting.

The options for pausing and toggling sorting are useful if you’re watching a very busy network and want to look at the display without connections jumping around (due to sorting and new connections being added) and disappearing (due to being closed for a certain time).

When paused (via the p command) no new connections will be displayed, however tcptrack will still monitor and track all connections it sees as usual. This option affects the display only, not internals. When you unpause, the display will be updated with all current information that tcptrack has been gathering all along.

EXAMPLES

tcptrack requires only one parameter to run: the -i flag followed by an interface name that you want tcptrack to monitor. This is the most basic way to run tcptrack:

 # tcptrack -i eth0

tcptrack can also take a pcap filter expression as an argument. The format of this filter expression is the same as that of tcpdump(8) and other libpcap-based sniffers. The following example will only show connections from host 10.45.165.2:

 # tcptrack -i eth0 src or dst 10.45.165.2

The next example will only show web traffic (ie, traffic on port 80):

 # tcptrack -i eth0 port 80

SEE ALSO

tcpdump(8), pcap(3), http://www.rhythm.cx/~steve/devel/tcptrack

BUGS

When picking up a connection that was already running before tcptrack was started, there is no way tcptrack can know for sure which end of the connection is the client (ie, which peer started the connection) and which is the server (ie, which peer was listening). tcptrack makes a crude guess at which is which by looking at the port numbers; whichever end has the lower port number is considered the server side. This isn't always accurate of course, but future versions may have better heuristics to figure out which end is which.

Currently the interface is not very flexible. Display timing settings (such as the refresh interval) can only be changed by editing the source code (defs.h in particular). See the TODO file included with the source distribution for further bugs.