

Menampilkan Informasi Koneksi TCP dengan tcptrack

Inginkan mengamati secara mendetail dan *realtime* koneksi TCP pada *interface* jaringan Anda? Tcptrack adalah salah satu tool yang sangat berguna untuk tugas-tugas tersebut. Sebagai program yang bekerja cukup *low level*, tcptrack sangatlah mudah digunakan.

Secara umum, tcptrack merupakan program *sniffer* yang akan menampilkan informasi koneksi TCP yang diamati pada suatu *interface* jaringan yang dimiliki. Tcptrack secara pasif akan mengamati koneksi-koneksi yang ada, kemudian menampilkan informasi yang berhasil didapatkannya dalam user interface yang sederhana dan mudah dipahami.

Walaupun tcptrack berjalan pada modus teks, *user interface* yang ditawarkan sangatlah menarik, mirip dengan program top.

Berikut ini adalah berbagai informasi yang ditampilkan dalam tampilan utama program ini:

- *Source address* dan *port* yang digunakan.
- *Destination address* dan *port* yang digunakan.
- Status koneksi.
- Waktu *idle*.
- *Bandwidth* yang digunakan.

Salah satu fitur lain yang sangat berguna adalah kemampuan filtering yang disediakan. Filter yang digunakan juga merupakan filter standar pcap (identik dengan yang digunakan pada tcpdump).

Tcptrack telah dipaketkan ke dalam berbagai distribusi Linux populer. Bagi Anda yang ingin men-download *source code* tcptrack terbaru, kunjungi website tcptrack di <http://www.rhythm.cx/~steve/devel/tcp-track/>. Pada saat tulisan ini dibuat, versi terbaru tcptrack adalah 1.1.5, yang dirilis pada 12 Maret 2005 lalu.

Tulisan ini dibuat di atas sistem Debian GNU/Linux 3.1, namun seharusnya bisa diterapkan pada sistem lainnya tanpa masalah.

Instalasi tcptrack

Carilah tcptrack di dalam *repository* distro yang Anda gunakan. Apabila tidak tersedia, carilah di *website* tcptrack. Di *website* tersebut, binary untuk berbagai distro juga turut disertakan. Apabila paket untuk distro Anda tidak juga bisa ditemukan atau Anda senang melakukan kompilasi sendiri, *download*-lah *source code* tcptrack dan lakukanlah kompilasi sendiri, sesuai dengan petunjuk di dalam *tree source code*-nya.

Di sistem Debian GNU/Linux, instalasi tcptrack dapat dilakukan dengan perintah:

```
# apt-get install tcptrack
```

Apabila instalasi telah dilakukan, maka tcptrack dapat dijalankan dengan perintah berikut:

```
$ tcptrack
```

Menjalankan tcptrack

Cara termudah dalam menjalankan tcptrack adalah:

- *Login*-lah sebagai root (atau dengan su atau sudo).
- Berikan opsi *-i* untuk argumen berupa *interface* jaringan yang ingin diamati. Sebagai contoh:
tcptrack -i eth1

Perintah tersebut bisa dimaksudkan sebagai perintah untuk menjalankan tcptrack dan untuk selanjutnya, tcptrack akan mengamati *interface* eth1. Gantilah eth1 sesuai dengan konfigurasi sistem Anda. *Interface* jaringan pertama pada sistem Linux umumnya diberi nama eth0.

Setelah tcptrack dijalankan, sebuah tampilan mirip dengan program top akan ditampilkan. Di tampilan tersebut, kita dapat melihat informasi-informasi seperti disebutkan sebelumnya pada awal tulisan. Di bagian bawah, kita bisa melihat informasi lain seperti jumlah koneksi

Ketika terjadi koneksi pada *interface* yang diamati, maka sejumlah informasi akan ditampilkan.

Sebagai contoh:

- Penulis mengamati eth1, dengan IP address 192.168.0.101.
- Melakukan koneksi ke Squid proxy dengan IP address 192.168.0.1, port 8080.
- Dan mengunjungi website <http://www.infolinux.web.id>.
- Pada saat koneksi sedang dilakukan, beberapa baris contoh seperti pada gambar 1 akan ditampilkan. Di sistem Anda, keluaran program bisa jauh berbeda.
- Di gambar 1 tersebut, bisa dilihat dengan jelas bahwa:
 - Koneksi dilakukan dari IP 192.168.0.101.
 - Koneksi ditujukan ke IP 192.168.0.1 port 8080.
 - Banyak koneksi dilakukan sekaligus.

Client	Server	State	Idle	A	Speed
192.168.0.101:43516	192.168.0.1:8080	CLOSED	0s	1	KB/s
192.168.0.101:43524	192.168.0.1:8080	CLOSING	0s	601	B/s
192.168.0.101:43523	192.168.0.1:8080	CLOSED	0s	252	B/s
192.168.0.101:43522	192.168.0.1:8080	CLOSED	0s	252	B/s
192.168.0.101:43521	192.168.0.1:8080	CLOSED	0s	252	B/s
192.168.0.101:43520	192.168.0.1:8080	CLOSED	0s	252	B/s
192.168.0.101:43519	192.168.0.1:8080	CLOSED	0s	252	B/s
192.168.0.101:43518	192.168.0.1:8080	CLOSED	0s	251	B/s
192.168.0.101:43532	192.168.0.1:8080	SYN_SENT	0s	0	B/s
192.168.0.101:43531	192.168.0.1:8080	ESTABLISHED	0s	0	B/s
192.168.0.101:43530	192.168.0.1:8080	ESTABLISHED	0s	0	B/s
192.168.0.101:43529	192.168.0.1:8080	ESTABLISHED	0s	0	B/s
192.168.0.101:43528	192.168.0.1:8080	ESTABLISHED	0s	0	B/s
192.168.0.101:43527	192.168.0.1:8080	ESTABLISHED	0s	0	B/s
192.168.0.101:43526	192.168.0.1:8080	ESTABLISHED	0s	0	B/s
192.168.0.101:43525	192.168.0.1:8080	CLOSING	0s	0	B/s
192.168.0.101:43517	192.168.0.1:8080	CLOSED	1s	0	B/s
		LUKEU	1s	0	B/s

TOTAL Connections 1-18 of 18 Unpaused Sorted 3 KB/s

Client	Server	State	Idle	A	Speed
192.168.0.101:45215	192.168.0.2:22	ESTABLISHED	26s	0	B/s
192.168.0.101:34740	192.168.0.1:22	ESTABLISHED	29s	0	B/s

TOTAL Connections 1-2 of 2 Unpaused Sorted 0 B/s

Informasi koneksi 1.

- Beberapa koneksi berada dalam status CLOSED, beberapa CLOSING, beberapa pada SYN_SENT, dan beberapa ESTABLISHED.
- Dari informasi tersebut, kita juga bisa melihat *idle time* koneksi.

Sebagai catatan, koneksi yang telah di-CLOSED akan ditampilkan selama 2 detik, sebelum dihapus dari daftar.

Untuk keluar dari tcptrack, berikanlah perintah q.

Perintah interaktif lain

Selama mengamati informasi yang ditampilkan oleh tcptrack, berikut ini adalah dua perintah lain yang bisa diberikan (selain q untuk keluar):

- p: untuk pause/unpause (toggle). Pada saat pause dilakukan, maka tidak ada koneksi baru yang akan ditampilkan. Namun demikian, tcptrack akan tetap memonitor dan melacak semua koneksi seperti biasanya.
- S: untuk meng-*enable*/men-*disable* pengurutan (toggle).

Opsi menjalankan tcptrack

Berikut ini adalah beberapa opsi yang disediakan, yang dapat diberikan pada saat menjalankan tcptrack:

- -d: apabila opsi ini diberikan, maka tcptrack hanya melacak koneksi yang dimulai setelah tcptrack dijalankan.
- -f: melakukan rekalkulasi rata-rata dengan cepat.
- -h: menampilkan bantuan.
- -i <interface>: meminta tcptrack untuk

Informasi koneksi 2: filter hanya port 22.

mengamati interface jaringan tertentu.

- -p: tidak menjadikan interface yang diamati dalam mode promiscuous.
- -r <sec>: menunggu selama sekian detik tertentu sebelum menghapus koneksi yang telah diclose dari tampilan. Nilai default adalah 2 detik.
- -v: menampilkan versi tcptrack.

Salah satu opsi yang mungkin berguna adalah opsi -r. Contoh perintah berikut ini akan menyebabkan tcptrack menunggu selama 10 detik sebelum menghapus koneksi yang telah di-close dari tampilan.

```
# tcptrack -i eth1 -r 10
```

Contoh filtering sederhana

Seperti telah disebutkan sebelumnya, tcptrack juga mendukung filtering dengan ekspresi filter pcap. Fitur ini akan sangat berguna.

Misal kita ingin melihat koneksi yang dilakukan ke port 22 saja. Maka, perintah yang bisa diberikan adalah:

```
# tcptrack -i eth1 port 22
```

Untuk informasi selengkapnya, bacalah manual pcap (3) dan tcpdump (8). Selamat mencoba. ☺

Noprianto [noprianto@infolinux.co.id]

Client	Server	State	Idle	A	Speed
192.168.0.101:48375	192.168.0.1:8080	CLOSED	1s	4	KB/s
192.168.0.101:48376	192.168.0.1:8080	CLOSED	0s	3	KB/s
192.168.0.101:48377	192.168.0.1:8080	CLOSING	0s	2	KB/s
192.168.0.101:48379	192.168.0.1:8080	CLOSED	1s	526	B/s
192.168.0.101:48380	192.168.0.1:8080	CLOSED	1s	526	B/s
192.168.0.101:48383	192.168.0.1:8080	ESTABLISHED	0s	493	B/s
192.168.0.101:48382	192.168.0.1:8080	ESTABLISHED	0s	485	B/s
192.168.0.101:48381	192.168.0.1:8080	CLOSING	0s	479	B/s
192.168.0.101:48378	192.168.0.1:8080	CLOSED	0s	433	B/s
192.168.0.101:48378	192.168.0.1:8080	CLOSED	1s	274	B/s
192.168.0.101:48388	192.168.0.1:8080	ESTABLISHED	0s	0	B/s
192.168.0.101:48389	192.168.0.1:8080	SYN_SENT	0s	0	B/s
192.168.0.101:48390	192.168.0.1:8080	SYN_SENT	0s	0	B/s
192.168.0.101:48387	192.168.0.1:8080	SYN_SENT	0s	0	B/s
192.168.0.101:48334	192.168.0.1:8080	ESTABLISHED	0s	0	B/s
192.168.0.101:48374	192.168.0.1:8080	CLOSED	1s	0	B/s
192.168.0.101:48386	192.168.0.1:8080	ESTABLISHED	1s	0	B/s

TOTAL Connections 1-23 of 23 Unpaused Sorted 14 KB/s

Informasi koneksi 3: filter hanya port 8080.