Berkomunikasi dengan Aman

Bekerja di jaringan besar berarti terjadi pengiriman data. Berhati-hatilah dan gunakan protokol yang aman atau data pribadi Anda menjadi konsumsi publik.

Perkembangan suatu teknologi untuk kebaikan selalu disertai dengan perkembangan teknologi tersebut untuk kejahatan. Hal tersebut lumrah adanya. Menolak perkembangan jelas tidak mungkin. Mengharapkan teknologi yang semata-mata untuk kebaikan saja juga jelas tidak mungkin.

Komputer terhubung ke Internet dan data kemudian dicuri. Komputer dapat digunakan untuk memodifikasi gambar dan gambar baik-baik kemudian dimodifikasi untuk tujuan pencemaran nama baik. Komputer semakin mudah digunakan dan virus pun dikembangkan oleh berbagai kalangan.

Bagi Anda yang setiap harinya bekerja mengirimkan data lewat jaringan, data Anda memiliki risiko untuk disadap. Anda membuka *webmail* dan kemudian mengisikan *password*. Anda *login* ke server untuk melakukan administrasi sederhana dan berbagai contoh lainnya.

Cara terbaik untuk kompromi adalah dengan mencegah. Tentunya bukan mencegah perkembangan suatu teknologi atau mencegah penggunaan. Namun, usahakan untuk menggunakan sesuatu yang saat ini terbukti aman.

Apabila Anda selalu menggunakan telnet, segeralah ganti. Apabila masih menggunakan ftp, gunakan protokol lain. Kami akan tunjukkan kepada Anda betapa beberapa protokol sangat rentan untuk disadap. Dan proses penyadapan pun dapat dilakukan oleh siapa saja, karena program untuk itu telah tersedia. Bukan *cracker* saja yang bisa menyadap informasi yang Anda kirimkan lewat telnet. Asalkan bisa mengoperasikan tool untuk menyadap, siapa saja bisa melakukan penyadapan tersebut. Ini bukan basa basi.

Sadap! Sadap! Sadap!

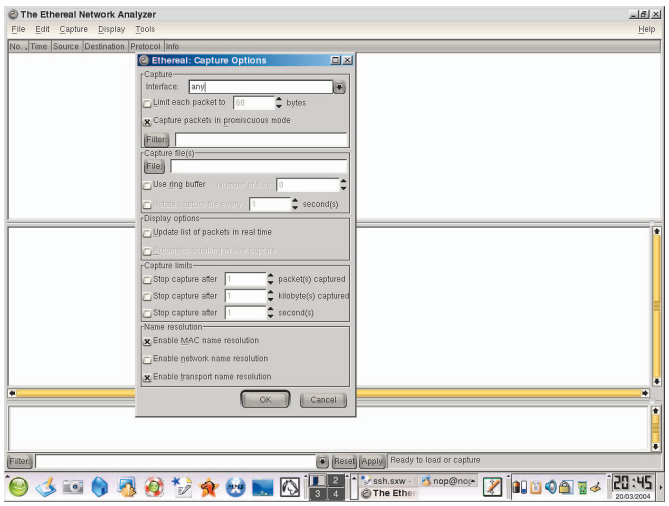
Berikut ini kita akan melihat betapa penyadapan informasi sangatlah mudah dilakukan. Untuk mengujinya, jalankanlah telnet server di komputer Anda. Telnet adalah protokol yang sangat rentan, karena semua informasi ditransmisikan dalam bentuk *clear text*.

Untuk melakukan penyadapan, kita akan menggunakan program Ethereal, yang dapat di-*download* di *http://www.ethereal.com*. Namun, cobalah cek terlebih dahulu paket-paket distro Anda, karena Ethereal termasuk program yang sangat umum dipaketkan bersama suatu distro. Ethereal berbasis GUI dan sangat mudah digunakan. Fiturnya pun sangat lengkap.

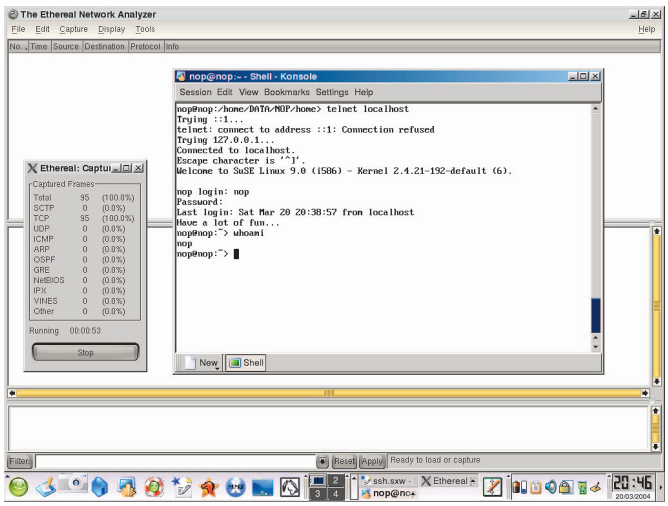
Jalankan telnet server. Telnet server umumnya dijalankan oleh inetd atau xinetd. Sebagai root, jalankan pula ethereal, dan segeralah akses menu *Capture*|*Start*. Sebuah dialog akan ditampilkan dan pastikan pada field interface, Anda memilih *any*. Klik OK untuk segera memulai penyadapan. Sebuah dialog statistik akan ditampilkan.

Bukalah emulasi terminal dan lakukan koneksi ke telnet server. Anda akan menjumpai tampilan khas *prompt login*, dan lakukanlah otentikasi. Setelah itu, berikanlah beberapa perintah seperti:

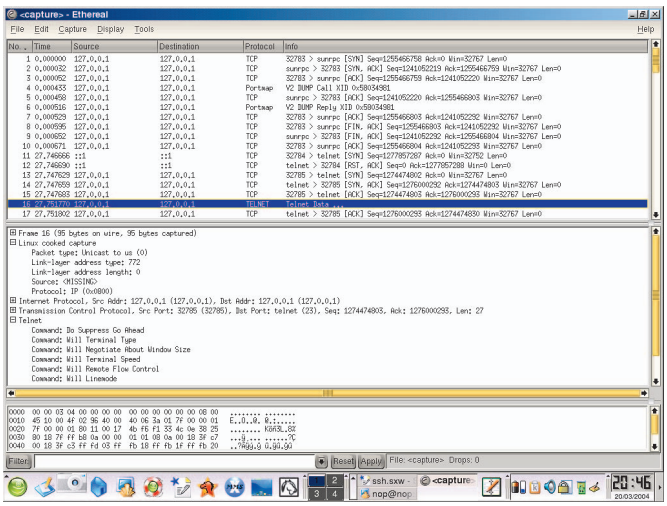
- ls
- whoami
- logout



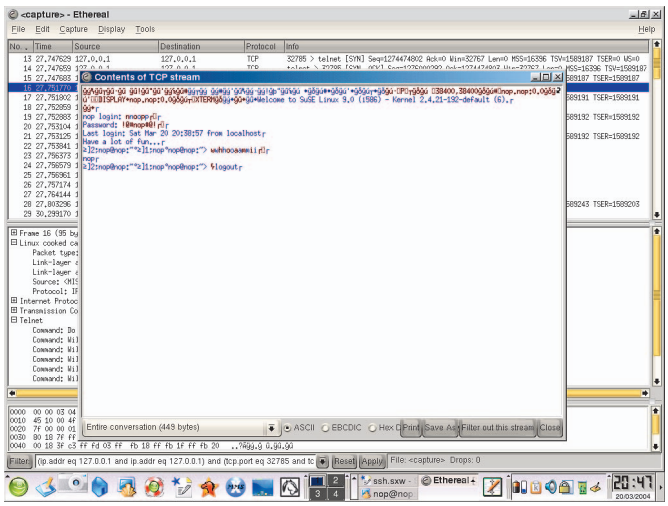
Opsi capture Ethereal.



Sesi telnet sedang di-capture Ethereal.



Hasil capture ditampilkan terstruktur.



Hasil capture sesi telnet.

Amatilah layar statistik penyadapan. Pastilah di bagian TCP akan menunjukkan angka lebih besar dari nol, yang menunjukkan paket yang tertangkap.

Tutup emulasi terminal Anda dan telnet server boleh dinonaktifkan. Klik pula tombol Stop di dialog statistik Ethereal karena penyadapan telah selesai. Di layar utama Ethereal Anda, akan tampil berbagai teks yang menunjukkan hasil penyadapan.

Seperti yang kita janjikan bahwa penyadapan dapat dilakukan dengan mudah, lupakanlah teks-teks dan angka-angka tersebut. Klik kananlah pada salah satu entri, dan pilihlah *Follow TCP Stream*.

Sebuah window baru akan terbuka dan seperti melihat sejarah, Anda akan melihat keseluruhan sesi telnet Anda sebelumnya, termasuk *password*-nya. Jelas. Siap dicuri. Siap disalah gunakan.

Hal ini menunjukkan bahwa menggunakan sesuatu yang tidak aman sangatlah berisiko. Jangan pernah lagi menggunakan telnet. Kalau Anda terpaksa harus melakukan *remote shell connection*, gunakanlah ssh. Lakukan penyadapan yang sama pada ssh dan Anda hanya akan melihat karakter-karakter tak berarti ketika Anda melakukan Follow TCP Stream.

Berikut ini, kita akan membahas beberapa tool pengganti untuk tool-tool yang tidak aman. Tool-tool yang akan kita bahas tersebut tentu saja tidak menjanjikan keamanan 100%, namun, untuk saat ini, lebih aman untuk digunakan.

Telnet dan ssh

Pada bagian sebelumnya, kita telah belajar menyadap suatu sesi telnet. Dengan Ethereal, penyadapan tersebut dapat dilakukan dengan sangat mudah. Telnet sendiri telah digunakan sejak awal-awal jaman unix. Fleksibilitasnya diakui memang pantas diberikan acungan jempol.

Namun, Anda melihat sendiri betapa mudahnya melakukan penyadapan terhadap sesi telnet. Apabila masih menggunakan telnet, segeralah hentikan dan berpindahlah ke ssh. Apabila administrator jaringan Anda masih menerapkan telnet server, segeralah meminta untuk mengaktifkan ssh daemon. Fungsionalitasnya sama dan ssh jelas jauh lebih aman. Berikut ini adalah beberapa hal seputar penggunaan ssh:

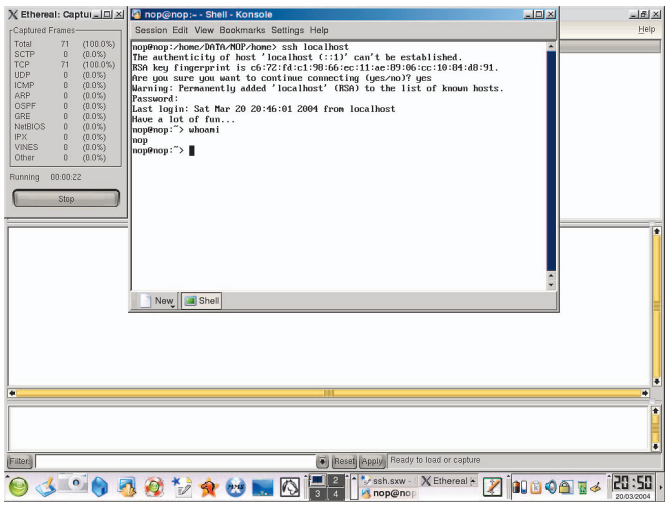
- **Pertama.** Jangan kaget apabila pertama kali ssh menanyakan soal *fingerprint* RSA dan lain sebagainya. *Host key verification* seperti ini hanya dilakukan sekali dan selanjutnya, benar-benar akan menyerupai sesi telnet.
- Tersedia beberapa *front end* untuk ssh. Apabila Anda mengunakan KDE, cobalah KSSH. Tidak terlalu bagus memang, namun paling tidak, Anda tidak perlu mengingat berbagai opsi ssh karena sebagian opsi ssh dapat dipilih di KSSH.
- Ada dua protokol SSH. Apabila memiliki waktu luang, bacalah manual ssh, di mana Anda akan mendapatkan penjelasan panjang lebar mengenai kedua protokol ini.
- SSH dapat menampilkan berbagai hal dalam bentuk yang rinci. Berikan saja opsi -v, dan Anda akan menjumpai tampilan verbose. Semakin banyak opsi -v yang diberikan, semakin rinci informasi yang Anda peroleh.
- Kompresi didukung untuk memperkecil ukuran data yang ditransfer. Dengan demikian, apabila Anda melakukan remote shell ke Internet dan koneksinya cukup lambat, diharapkan dengan mengaktifkan kompresi, transfer data dapat dilakukan lebih cepat.

Secure copy: scp

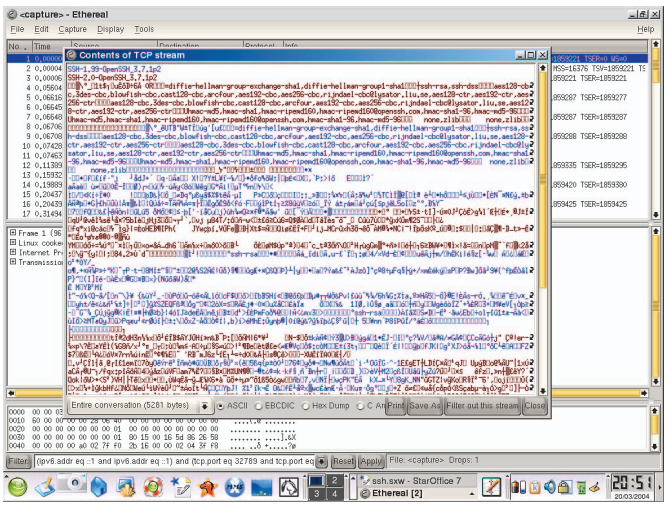
Anda ingin meng-*copy* suatu file dari komputer lain di dalam jaringan Anda. Kebetulan, komputer tidak mengaktifkan file sharing apapun juga. FTP server juga tidak diaktifkan. Yang diaktifkan hanyalah ssh daemon.

Dalam skenario tersebut, Anda dapat menggunakan scp untuk meng-copy suatu file dari komputer lain selama Anda memiliki hak atau *account* dan mengetahui lokasi filenya. Apabila Anda memiliki account, maka lokasi file tentu saja dapat dilihat ketika Anda membuka sesi ssh ke komputer tersebut.

Dengan menggunakan scp, Anda dapat melakukan peng-copy-an baik satu file ataupun direktori secara rekursif. Dengan demikian, Anda tidak perlu repot-repot mengaktifkan file sharing ataupun



Sesi ssh sedang di-capture Ethereal.



Hasil capture sesi ssh.

membuka sesi FTP. Selain itu, dengan scp, Anda dapat meng-copy file dari suatu komputer ataupun meng-copy-kan file ke suatu komputer.

Sebagian besar opsi scp mirip dengan opsi program cp. Bedanya, dengan scp, peng-copy-an dapat dilakukan secara aman melewati jaringan. Sebagai bonus, scp pun menampilkan *progress bar* yang menarik sehingga lebih informatif karena pengopian melewati Internet, misalnya, dapat memakan waktu yang cukup lama.

Berikut ini adalah beberapa contoh penggunaan scp:

```
$ scp a nop@192.168.1.2:~/a_copy
```

➔ Perintah ini akan meng-copy-kan file a ke home directory nop di komputer 192.168.1.2. File a tersebut akan dikopikan menjadi file a_copy.

```
$ scp a* nop@192.168.1.2:/tmp
```

➔ Perintah ini akan meng-copy-kan file-file yang namanya diawali dengan karakter a ke direktori /tmp di komputer 192.168.1.2.

```
$ scp -r lagu nop@192.168.1.2:/tmp
```

➔ Perintah ini akan mengopikan directory lagu secara rekursif ke direktori /tmp di komputer 192.168.1.2.

```
$ scp nop@192.168.1.2:/boot/vmlinuz-
2.4.21-192-default ~/
```

➔ Perintah ini akan meng-copy file /boot/vmlinuz-2.4.21-192-default dari komputer 192.168.1.2 ke home directory user aktif.

Berikut ini adalah beberapa hal seputar penggunaan scp:

- Tidak seperti saudara sepupunya, rcp, yang sama-sama melakukan kopi meng-copy file, scp akan meminta password apabila diperlukan.
- Scp menggunakan ssh untuk transfer data dan menggunakan kemampuan yang sama untuk menjamin keamanan data.
- Pada saat kita sedang berada di komputer A, kita dapat meng-copy-kan file dari komputer B ke komputer C. Jadi, pengopian di antara dua *remote host* dimungkinkan. Luar biasa sekali. Apa yang Anda perlukan hanyalah informasi *login* dan file.
- Scp ternyata cukup memahami keterbatasan *bandwidth*. Oleh karena itu, Anda juga dapat membatasi bandwidth yang digunakan oleh scp dalam satuan Kbit/s.
- Sama seperti ssh, scp juga mendukung kompresi. Dalam peng-copy-an file, kompresi dapat meningkatkan kecepatan transfer, walaupun Anda akan mengorbankan waktu untuk melakukan kompresi/dekompresi.

FTP dan SFTP

Pada bagian sebelumnya, kita telah melihat penggunaan ssh dan scp, masing-masing untuk remote shell dan peng-copy-an file antar-host. Dengan kedua tools tersebut, Anda dapat melakukan aksi administratif sekaligus melakukan transfer file.

Bagi Anda yang sering bekerja dalam dunia kirim mengirim file dan terbiasa dengan FTP, Anda masih dapat menggunakan tool serupa, namun dalam cara yang lebih aman. Gunakan SFTP! Perintah-perintahnya mirip!

Berikut ini adalah beberapa hal seputar penggunaan sftp:

- Sama seperti scp, sftp juga dapat memanfaatkan kemampuan ssh seperti enkripsi dan kompresi.
- Sftp memungkinkan proses batching, sehingga perintah dapat diberikan dalam suatu file batch, alih-alih mengetikkan berbagai perintah secara manual. Fitur ini sangat berguna.

Untuk kebutuhan *remote shell connection* dan file transfer, mulai saat ini, bagi Anda yang masih menggunakan telnet dan ftp, segeralah lupakan kedua tool tersebut. Mulailah gunakan ssh, scp, ataupun sftp. Pengaturan server untuk semua tool tersebut pun sangatlah sederhana. Anda hanya membutuhkan ssh daemon.

Keamanan data adalah isu yang sangat penting. Jangan pernah sesekali meremehkan hal sekecil apapun dalam keamanan data. Karena, banyak pihak di luar sana yang siap untuk menyalahgunakan data yang didapatnya. Sesekali bertindak paranoid, bolehlah.

Noprianto *(noprianto@infolinux.co.id)*