# Setting Telnet dan SSH

Oleh : Ripto Mukti Wibowo
rip.wibowo@gmail.com

## I. PENDAHULUAN

Layanan remote login adalah layanan yang mengacu pada program atau protokol yang menyediakan fungsi yang memungkinkan seorang pengguna internet untuk mengakses (login) ke sebuah terminal (remote host) dalam lingkungan jaringan internet. Dengan memanfaatkan remote login, seorang pengguna internet dapat mengoperasikan sebuah host dari jarak jauh tanpa harus secara fisik berhadapan dengan host bersangkutan. Dari sana ia dapat melakukan pemeliharaan (maintenance), menjalankan sebuah program atau malahan menginstall program baru di remote host.

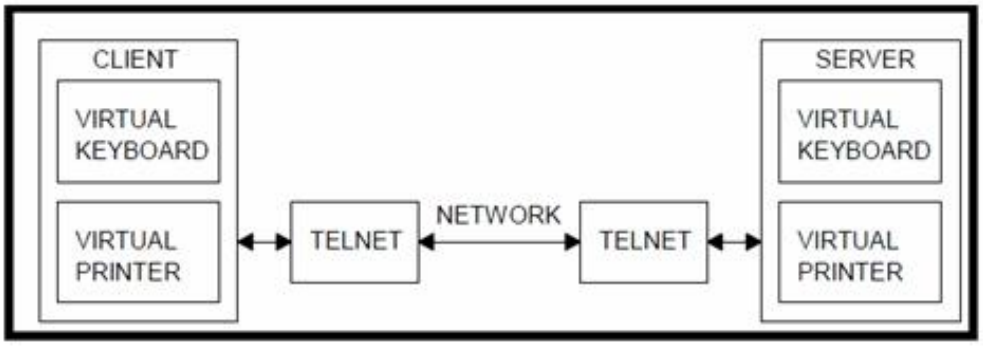
Protokol yang umum digunakan untuk keperluan remote login adalah Telnet. Namun demikian, penggunaan remote login Telnet, sebenarnya mengandung resiko, terutama dari tangan-tangan jahil yang banyak berkeliaran di internet. Untuk memperkecil resiko ini, maka telah dikembangkan protokol SSH (secure shell) untuk menggantikan Telnet dalam melakukan remote login.

## II. TELNET

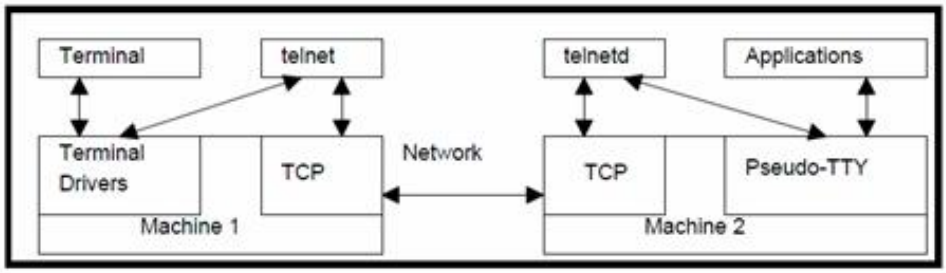
### *A. Pengertian Telnet*

Telnet adalah aplikasi *remote login Internet*. Telnet digunakan untuk login ke komputer lain di Internet dan mengakses berbagai macam pelayanan umum, termasuk katalog perpustakaan dan berbagai macam database. Telnet memungkinkan pengguna untuk duduk didepan komputer yang terkoneksi ke internet dan mengakses komputer lain yang juga terkoneksi ke internet. Dengan kata lain koneksi dapat terjadi ke mesin lain di satu ruangan, satu kampus, bahkan setiap komputer di seluruh dunia. Setelah terkoneksi, input yang diberikan pada keyboard akan mengontrol langsung ke remote computer tadi. Akan dapat diakses pelayanan apapun yang disediakan oleh *remote machine* dan hasilnya ditampilkan pada terminal lokal. Dapat dijalankan session interaktif normal (login, eksekusi command), atau dapat diakses berbagai service seperti: melihat catalog dari sebuah perpustakaan, akses ke teks dari *USA today*, dan masih banyak lagi service yang disediakan oleh masing-masing host pada di network.

Telnet menggunakan 2 program, yang satu adalah client (*telnet)* dan server *(telnetd*). Yang terjadi adalah ada dua program yang berjalan, yaitu software *client* yang dijalankan pada komputer yang meminta pelayanan tersebut dan software server yang dijalankan oleh computer yang menghasilkan pelayanan tadi.




Gambar 1. Interaksi TELNET (Parker, 1994:117)



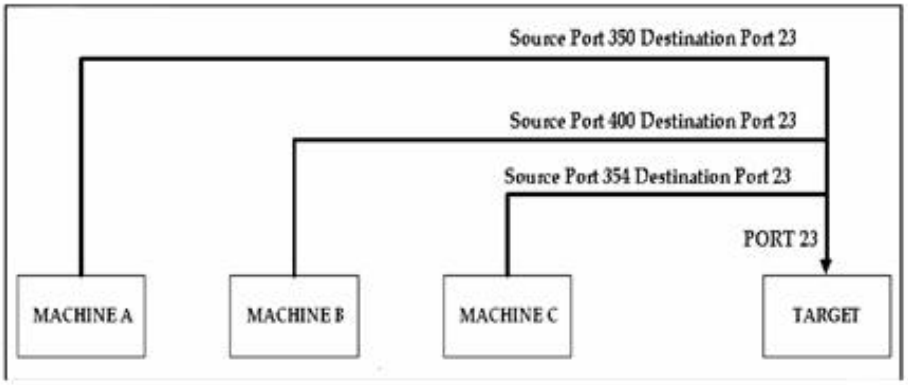

Gambar 2. Koneksi mesin ketika terjadi TELNER (Parker, 1994:118)

Tugas dari *client* adalah:

- Membuat koneksi network TCP (*Transfer Control Protocol*) dengan *server*.
- Menerima inputan dari *user*
- Menformat kembali inputan dari user kemudian mengubah dalam bentuk format standard dan dikirim ke *server*.
- Menerima output dari *server* dalam format standard.
- Mengubah format output tadi untuk ditampilkan pada layar.

Sedangkan tugas dari *server* adalah:

- Menginformasikan software jaringan bahwa komputer itu siap menerima koneksi.
- Menunggu permintaan dalam bentuk format standard.
- Melaksanakan permintaan tersebut.
- Mengirim kembali hasil ke *client* dalam bentuk format standard.
- Menunggu permintaan selanjutnya.



Gambar 3. Penggunaan Port untuk Server yang dituju oleh banyak pengguna (Parker, 1994:98)

Ketika terjadi koneksi A-B

Pada mesin A terjadi Port yang digunakan adalah
Source=350 Destination=23
Pada mesin B Port yang digunakan
Source=23 Destination=350

Ketika terjadi koneksi B-C

Pada mesin B Porty yang digunakan
Source=400 Destination=23
Pada Mesin C Port yang digunakan
Source=23 D estination=351

Ketika terjadi koneksi C-A

Pada mesin A
Source=351 Destination=23
Pada mesin B
Source=23 Destination=400

Telnet adalah program yang memungkinkan komputer host Internet anda menjadi terminal dari komputer host lain di Internet. Dengan ftp anda dapat membuka koneksi hanya untuk mentransfer file. Telnet memungkinkan anda untuk login sebagai pemakai pada komputer jarak jauh dan menjalankan program layanan Internet yang disediakan oleh komputer tersebut.

B. *Akses Telnet*

Telnet menyediakan akses langsung ke beragam layanan di Internet. Komputer host anda memang menyediakan beragam layanan, namun jika layanan tersebut tidak ada, anda bisa menggunakannya melalui Telnet. Misalnya ketika masyarakat Internet menulis interface untuk membantu pengguna lain, Telnet memungkinkan anda mengakses host mereka dan menggunakan interface yang mereka buat. Demikian juga ketika seorang membuat layanan yang bermanfaat, Telnet memungkinkan anda mengakses sumber daya informasi yang berharga ini.Maintaining the Integrity of the Specifications

## III. SSH (SECURE SHELL)

### A. *Pengertian SSH*

Pada awalnya SSH dikembangkan oleh Tatu Yl nen di Helsinki University of Technology. SSH memberikan alternatif yang secure terhadap remote session tradisional dan file transfer protocol seperti telnet dan relogin.Protokol SSH mendukung otentikasi terhadap remote host, yang dengan demikian meminimalkan ancaman pemalsuan identitas client lewat IP address spoofing maupun manipulasi DNS. Selain itu SSH mendukung beberapa protocol enkripsi secret key untuk membantu memastikan privacy dari keseluruhan komunikasi, yang dimulai dengan username/password awal.

Algoritma enkripsi yang didukung oleh SSH di antaranya TripleDES(Pengembangan dari DES oleh IBM), *BlowFish* (BRUCE SCHNEIER), *IDEA (The International Data Encryption Algorithm)*, dan *RSA (The Rivest-Shamir-Adelman)*. Dengan berbagai metode enkripsi yang didukung oleh SSH, Algoritma yang digunakan dapat diganti secara cepat jika salah satu algoritma yang diterapkan mengalami gangguan. SSH menyediakan suatu virtual private connection pada application layer, mencakup interactive logon protocol (ssh dan sshd) serta fasilitas untuk secure transfer file (scd). Setelah meng-instal SSH, sangat dianjurkan untuk mendisable telnet dan rlogin. Implementasi SSH pada linux diantaranya adalah OpenSSH. SSH merupakan paket program yang digunakan sebagai pengganti yang aman untuk rlogin, rsh dan rcp.

### B. *Kegunaan SSH*

SSH dirancang untuk menggantikan protokol telnet dan FTP. SSH merupakan produk serbaguna yang dirancang untuk melakukan banyak hal, yang kebanyakan berupa penciptaan tunnel antar host. Dua hal penting SSH adalah console login (menggantikan telnet) dan secure filetransfer (menggantikan FTP), tetapi dengan SSH anda juga memperoleh kemampuan membentuk source tunnel untuk melewatkan HTTP,FTP,POP3, dan apapun lainnya melalui SSH tunel.

### C. *Public Key Cryptografi (Kriptografi Kunci Publik)*

SSH menggunakan metode public-key cryptography untuk mengenkripsi komunikasi antara dua host, demikian pula untuk autentikasi pemakai. Dengan metode ini, kita akan memerlukan 2 buah kunci berbeda yang digunakan baik untuk melakukan enkripsi dan dekripsi. Dua buah kunci tersebut masing-masing disebut public key (dipublikasikan ke publik/orang lain) dan private key (dirahasiakan/hanya pemiliknya yang tahu). Masing-masing kunci di atas dapat digunakan untuk melakukan enkripsi dan dekripsi.

SSH dapat digunakan untuk login secara aman ke remote host atau menyalin data antar host, sementara mencegah man-in-themiddle attacks (pembajakan sesi) dan DNS spoofing atau dapat dikatakan Secure Shell adalah program yang melakukan loging terhadap komputer lain dalam jaringan, mengeksekusi perintah lewat mesin secara remote, dan memindahkan file dari satu mesin ke mesin lainnya. SSH merupakan produk serbaguna yang dirancang untuk melakukan banyak hal, yang kebanyakan berupa penciptaan tunnel antar host.

### D. *Cara Kerja SSH*

Saat suatu client mencoba mengakses suatu linux server melalui SSH. SH daemon yang berjalan baik pada linux server maupun SSH client telah mempunyai pasangan

public/private key yang masing-masing menjadi identitas SSH bagi keduanya. Langkah-langkah koneksinya adalah sebagai berikut :

*Langkah 1*

Client bind pada local port nomor besar dan melakukan koneksi ke port 22 pada server.

*Langkah 2*

Client dan server setuju untuk menggunakan sesi SSH tertentu. Hal ini penting karena SSH v.1 dan v.2 tidak kompatibel.

*Langkah 3*

Client meminta public key dan host key milik server.

*Langkah 4*

Client dan server menyetujui algoritma enkripsi yang akan dipakai (misalnya TripleDES atau IDEA).

*Langkah 5*

Client membentuk suatu session key yang didapat dari client dan mengenkripsinya menggunakan public key milik server.

*Langkah 6*

Server men-decrypt session ky yang didapat dari client, meng-re-encrypt-nya dengan public key milik client, dan mengirimkannya kembali ke client untuk verifikasi.

*Langkah 7*

Pemakai mengotentikasi dirinya ke server di dalam aliran data terenkripsi dalam session key tersebut. Sampai disini koneksi telah terbentuk, dan client dapat selanjutnya bekerja secara interaktif pada server atau mentransfer file ke atau dari server. Langkah ketujuh diatas dapat dilaksanakan dengan berbagai cara (username/password, kerberos, RSA dan lain-lain).

## IV. PERBEDAAN TELNET DAN SSH


Gambar 4. Cara kerja TELNET dan SSH

Disini dapat kita lihat SSH memberikan alternatif yang secure terhadap remote session tradisional dan file transfer protocol seperti telnet dan relogin.Protokol SSH mendukung otentikasi terhadap remote host, yang dengan demikian meminimalkan ancaman pemalsuan identitas client lewat IP address spoofing maupun manipulasi DNS. Aplikasi seperti Telnet tidak menggunakan enkripsi sedangkan SSH dilengkapi dengan enkripsi.

Sebab itulah SSH (Secure Shell) dapat memberi keamanan yang lebih daripada Telnet atau rlogin. Banyak orang menggunakan Telnet sebagai aplikasi jaringan mereka. Sebenarnya hal tersebut kurang

begitu aman sebab dalam proses mengirim atau menerima data memungkinkan sesion kita terlihat dalam bentuk text. Sehingga orang yang jahil yang masuk ke network kita dapat mengetahui username, password, atau perintah-perintah yang kita baca

## REFERENCES


[1] http://www.telnet.org/

[2] http://www.scribd.com/doc/14682116/Belajar-Ssh?autodown=pdf

[3] http://72.14.235.132/search?q=cache:Mla5Wf7wEIUJ:idkf.bogor.net/linux-heboh/September%25202001/internet-3-telnet-remote-login.pdf+remote+login+filetype:pdf&cd=1&hl=id&ct=clnk&gl=id

[4] http://www.ssh.com/

[5] http://www.te.ugm.ac.id/~risanuri/distributed/TELNET.pdf

[6] http://www.ssh.com/support/downloads/secureshellwks/non-commercial.html