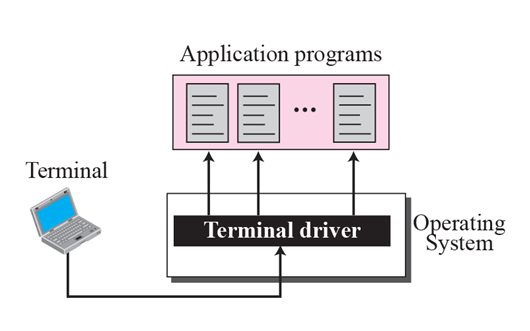
Laporan Pendahuluan Praktikum Keamanan Data : Telnet & SSH

oleh Dimas Rizky H.P. – 2110141011 – 3 D4 IT A

1. Telnet

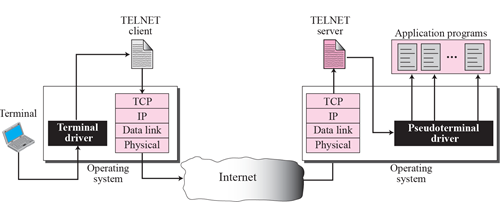
Telnet merupakan kepanjangan dari *Telecommunications Network Protocol*. Telnet adalah salah satu dari aplikasi internet yang memungkinkan user terhubung ke “terminal” komputer lain (*host remote*) yang berada di luar jaringan.

Pada masa ARPANET, sebulm adanya *workstation grafis*, setiap user yang menggunakan terminal pasti terhubung dengan *mainframe* melalui koneksi serial. Setiap terminal memiliki *keyboard* dan *monitor* masing masing namun tanpa ada CPU, karena setiap proses akan dilakukan di *mainframe*



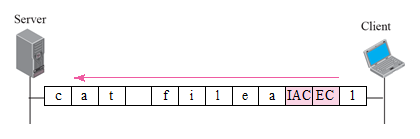
*Gambar 1.1 Alur data Telnet*

Telnet, biasanya digunakan untuk “*remote login”* dari PC ke PC lain dalam jaringan, sehingga memungkinkan user untuk menjalankan aplikasi yang berada di sistem *remote. Remote login* yang dilakukan menggunakan *text onnly* *connection*, sehingga setiap kali telnet terhubung, dan setiap kali huruf di ketik-kan, data per character akan dikirimkan ke *remote host* dalam bentuk *plain text* melalui protocol TCP/IP.

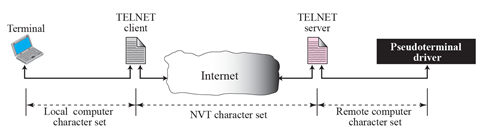


Gambar 1.2. Pengiriman data telnet melalui Internet menggunakan protocol TCP/IP

Telnet merupakan aplikasi *client/server*. *Client* mengambil karakter yang dimasukan dari *keyboard*, mengirimkannya ke *server* dan mencetak *output* yang dikirim oleh *server*. Kemudian, *server* akan melewatkan karakter input dari *client*, merepresentasikannya sebagai perintah, membaca output dan mengirimnya kembali ke *client* untuk dicetak ke layar. Pengiriman perintah/informasi *login* dikirimkan sebagai *plain text*, sehingga jika packetnya dapat diambil akan terbaca apa saja yang diketikan oleh *client.*



Hal ini erat kaitannya dengan pengkonversian local computer character set ke NVT character set pada saat data karakter dikirimkan melalui internet. Pada saat data sampai ke server, NVT charset tersebut akan dirubah lagi menjadi charset local *remote computer* yang dituju.

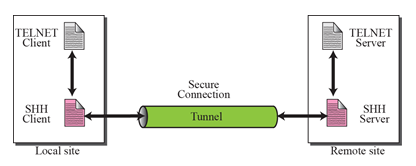


*Gambar 1.3. Alur charset yang digunakan.*

1. SSH

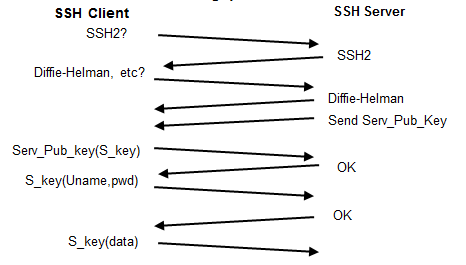
SSH (Secure Shell) merupakan suatu protokol yang memfasilitasi sistem komunikasi yang aman diantara dua sistem yang menggunakan arsitektur client/server. SSH memungkinkan user untuk login ke server secara remote layaknya telnet namun berbeda. Bedanya adalah pada saat pengiriman data. Pada telnet, data dikirimkan dalam bentuk *plain text*, sehingga jika packet data dianalisa, akan terlihat character apa yang diketikan oleh client. Pada SSH data dikirimkan dalam bentuk enkripsi, sehingga menyulitkan penyusup yang mencoba mendapatkan *password* yang tidak dienkripsi.

SSH memang dirancang untuk menggantikan *servicei* pada sistem *unix/linux*  yang masih menggunakan plain-text dalam pengiriman datanya. Dengan SSH, semua percakapan antara server dan klien di-enkripsi. Pada saat data karakter dikirimkan, SSH akan membuat semacam *tunnel* atau terowongan data, sehingga seolah olah, data mengalir di dalam sebuah *terowongan* dan user diluar *terowongan* itu tidak ada yang dapat melihat isi datanya. *Tunnel* ini sebenarnya adalah enkripsi yang dilakukan antara *client/server* sebelum melakukan pengiriman data.



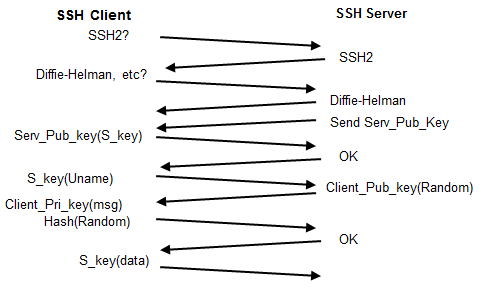
*Gambar 2.1 Proses pengiriman data melalui tunnel*

Komunikasi SSH bekerja mulai pada saat *client* mengontak *server*. Pertama kali akan ditanyakan tentang versi SSH yang digunakan, jika versi yang digunakan sama, maka akan berlanjut *client* akan menanyakan metode enkripsi seperti apa yang akan digunakan. Setelah itu, *server* akan mengirimkan *server public key* ke client sebagai tanda dimulainya proses *tunneling.* Client akan menerima server public key dana lalu mengirimkan key milik client ke server. Setelah metode enkripsi dan pertukaran key selesai, terjadilah proses autentifikasi, dimasukannya username dan password untuk login, setelah login dilakukan, maka pertukaran data dengan SSH bisa dilakukan.



*Gambar 2.2 Proses pengiriman data mulai enkripsi sampai autentifikasi.*

Terdapat beberapa permasalah dalam autentifikasi menggunakan password, yaitu password dapat ditebak, SSH secara default membolehkan multiple attempt pada saat autentitfikasi, jika ingin menebak user dan password hanya diperlukan satu account, sehingga ada metode lain yatu menggunakan *public key*.



*Gambar 2.3 Proses komunikasi data menggunakan public key.*

Adapun pendekatan lainnya adalah menggunakan passwordless login. Metodenya adalah dengan membuat key pair di client, lalu menyimpannya di direktori .ssh dan dicopy kan ke direktori .ssh/authorized\_keys pada komputer server. Dengan cara ini, setiap kali melakukan koneksi SSH ke server, proses autentifikasi tidak lagi memerlukan username dan password.