

PRAKTIKUM 7

SECURE SHELL (SSH)

I. Tujuan :

- Mahasiswa dapat memahami penggunaan service secure shell dan secure ftp pada sistem operasi unix/linux
- Mahasiswa mampu melakukan instalasi dan konfigurasi ssh untuk meningkatkan keamanan data
- Mahasiswa memahami kelebihan penggunaan secure shell dibanding service telnet, ftp dan perintah remote lainnya

II. Peralatan yang dibutuhkan

1. Beberapa PC yang terhubung ke sistem jaringan
2. Program yang digunakan adalah :
 - openssh-server-xxx.rpm
 - openssh-clients-xxx.rpm
 - openssh-xxx.rpm

III. Dasar Teori

Secure Shell

Secure Shell (ssh) adalah suatu protokol yang memfasilitasi sistem komunikasi yang aman diantara dua sistem yang menggunakan arsitektur client/server, serta memungkinkan seorang user untuk login ke server secara remote. Berbeda dengan telnet dan ftp yang menggunakan plain text, SSH meng-enkripsi data selama proses komunikasi sehingga menyulitkan intruder yang mencoba mendapatkan password yang tidak dienkripsi. Fungsi utama aplikasi ini adalah untuk mengakses mesin secara remote. Bentuk akses remote yang bisa diperoleh adalah akses pada mode teks maupun mode grafis/X apabila konfigurasinya mengijinkan

SSH dirancang untuk menggantikan service-service di sistem unix/linux yang menggunakan sistem plain-text seperti telnet, ftp, rlogin, rsh, rcp, dll). Untuk menggantikan fungsi ftp dapat digunakan sftp (secure ftp), sedangkan untuk menggantikan rcp (remote copy) dapat digunakan scp (secure copy).

Dengan SSH, semua percakapan antara server dan klien di-enkripsi. Artinya, apabila percakapan tersebut disadap, penyadap tidak mungkin memahami isinya. Bayangkan

seandainya Anda sedang melakukan maintenance server dari jauh, tentunya dengan account yang punya hak khusus, tanpa setahu Anda, account dan password tersebut disadap orang lain, kemudian server Anda dirusak setelahnya.

Implementasi SSH yang banyak dipakai saat ini adalah OpenSSH, aplikasi ini telah dimasukkan kedalam berbagai macam distribusi linux. Redhat Linux versi 9 sudah menyediakan program tersebut dalam format RPM.

Fitur-fitur SSH

Protokol SSH menyediakan layanan sbb.:

- Pada saat awal terjadinya koneksi, client melakukan pengecekan apakah host yang dihubungi sudah terdaftar pada client atau tidak
- Client mengirimkan proses autentifikasi ke server menggunakan teknik enkripsi 128 bit
- Semua data yang dikirimkan dan diterima menggunakan teknik enkripsi 128 bit sehingga sangat sulit untuk dibaca tanpa mengetahui kode enkripsinya
- Client dapat memforward aplikasi Xwindows / X11 ke server, layanan ini disebut

IV. Tugas Pendahuluan

1. Apa kelebihan secure shell dibanding perintah telnet, ftp dan perintah remote lainnya
2. Sistem enkripsi apa yang digunakan oleh program ssh pada Redhat Linux 9
3. Jelaskan bagaimana program ssh bekerja pada sistem jaringan client/server

V. Langkah percobaan :

1. Login ke sistem Linux sebagai root
2. Cek apakah konfigurasi alamat IP untuk host.
 - a. Jalankan perintah **ifconfig**, tulis konfigurasi IP host anda.
Interface : _____
IP Address : _____
Subnet mask : _____
 - b. Jalankan perintah netstat -r, tuliskan default gateway host anda.
Default Gateway :

3. Untuk menjalankan service ssh pada server diperlukan paket program yang bernama `openssh-server-xxx.rpm`, sedangkan pada PC client diperlukan program `openssh-clients-xxx.rpm`.

Cek apakah program kedua program tersebut sudah terinstall atau belum. Jika sudah, langsung kerjakan langkah nomer 8.

- a. Jalankan perintah **`rpm -qa | grep openssh`**, tulis hasilnya
- b. Ada berapa banyak program openssh yang terinstall di PC anda ?
- c. Apakah sudah ada program `openssh-server` ?

Jalankan perintah **`rpm -qa | grep openssh-server`** , tulis hasilnya

4. Jika program `openssh-server` dan `openssh-client` belum ada, installah dengan cara sbb. Masukkan CD Rom Redhat dan ketiklah perintah berikut ini.

```
# mount /dev/cdrom /mnt/cdrom
# cd /mnt/cdrom
# ls -l
# cd RedHat
# ls -l
# cd RPMS
# ls -l openssh*
```

5. Jika tidak ditemukan `openssh-server-xxxx.rpm` atau `openssh-client.rpm` (xxx = nomer versi) gantilah dengan CD yang lain. Jika anda tidak membawa CD Redhat Linux, anda bisa mendownloadnya di ftp server.

```
# cd -- ke home direktori
# ping 10.252.105.101 -- cek konektivitas
# ftp 10.252.105.101
Connected to host8.
220 (vsFTPD 1.1.3)
530 Please login with USER and PASS.
KRB5 V4 rejected as an authentication type
Name (localhost:root): anonymous
331 Please specify the password.
Password:
230 Login successful. Have fun.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
ftp> cd pub
```

```
ftp> ls -- lihat isi direktori pub
ftp> bin -- mode binary file
ftp> mget openssh* -- ketik yes untuk download
ftp> bye -- keluar dari ftp server
#
```

6. Instalasi program ssh

```
# rpm -ivh openssh-server*.rpm
# rpm -ivh openssh-clients*.rpm
```

7. Catatlah di direktori mana saja program openssh server diinstall.

```
# rpm -ql openssh-server
```

- Dimana binary/executeble file program ssh berada ?
- Dimana file konfigurasi ssh berada ?
- Bacalah manual dari program ssh server

```
# man sshd
```

- Bacalah semua informasi yang ada di file konfigurasi ssh server

```
# more /etc/ssh/sshd_config
# man sshd_config
```

8. Catatlah di direktori mana saja program openssh-clients diinstall.

```
# rpm -ql openssh-clients
```

- Catatlah semua binary/executable file yang terinstall
- Dimana file konfigurasi ssh client berada ?
- Baca dan pahami manual dari program-program ssh client berikut ini

```
# man ssh
# man scp
# man sftp
# man slogin
```

Jelaskan apa fungsi atau kegunaan dari masing-masing service ssh, scp, sftp dan slogin

- d. Bacalah semua informasi yang ada di file konfigurasi ssh client

```
# more /etc/ssh/ssh_config
# man ssh_config
```

9. Mengaktifkan service sshserver

Untuk menjalankan service ssh service gunakan perintah

```
# /etc/rc.d/init.d/sshd start
```

Untuk mematikan services gunakan perintah :

```
# /etc/rc.d/init.d/sshd stop
```

Untuk menjalankan ulang services gunakan perintah :

```
# /etc/rc.d/init.d/sshd restart
```

10. Memeriksa proses sshd

Setelah program sshd (ssh daemon) dijalankan, periksalah apakah sshd sudah aktif di memory.

```
# ps -aux | grep sshd
```

Catatlah, berapa nomer proses sshd di pc anda.

```
# netstat -a | grep ssh
```

Protokol apa yang digunakan oleh program ssh ?

11. Catatlah berapa nomer port yang digunakan oleh service ssh

```
# cat /etc/services | grep ssh
```

Berapa nomer port yang digunakan oleh service ssh ?

12. Menghapus rule firewall

Redhat Linux versi 8 atau yang lebih baru, akan mengaktifkan firewall secara default sehingga semua akses dari luar akan ditolak. Untuk kepentingan percobaan ini, ada baiknya untuk sementara semua rule firewall dihapus. Gunakan perintah :

```
# iptables -F
```

13. Uji coba dari localhost

Untuk menguji coba apakah ssh server sudah berfungsi dengan baik gunakan perintah :

```
# ssh localhost
The authenticity of host 'localhost (127.0.0.1)' can't
be established.
RSA key fingerprint is
82:0a:7f:f3:f3:5c:cf:87:db:a0:4d:b6:ce:20:26:1c.
Are you sure you want to continue connecting (yes/no)?
yes
Warning: Permanently added 'localhost' (RSA) to the list
of known hosts.
root@localhost's password: *****
Last login: Wed May  5 08:46:13 2004
#
```

Jika anda ssh ke localhost dan terdapat pesan seperti diatas, maka ssh server sudah dapat berfungsi dengan baik.

Misalkan sshd sedang dalam keadaan tidak aktif, maka jika ada permintaan service ssh akan ditolak oleh server.

```
# /etc/rc.d/init.d/sshd stop          -- mematikan service
Stopping sshd:  OK  ]
# ssh localhost
ssh: connect to host localhost port 22: Connection
refused          -- koneksi ssh ditolak
#
# /etc/rc.d/init.d/sshd start
```

14. Percobaan kelompok

Percobaan-percobaan yang ada dibawah ini dilakukan secara berpasangan (2 orang). Sebelum memulai percobaan, buatlah user baru sbb. :

```
# useradd userkiri
# passwd userkiri
# useradd userkanan
# passwd userkanan
```

Keterangan : userkiri digunakan untuk user yang duduk di sebelah kiri, dan userkanan untuk user yang duduk di sebelah kanan. Jangan lupa beritahu pasangan anda password yang sudah anda tentukan.

Setelah itu editlah file /etc/hosts sbb. :

```
# cp /etc/hosts /etc/hosts.asli      -- backup file
# vi /etc/hosts                      -- edit file
----- tambahkan di baris paling akhir

127.0.0.1        localhost.localdomain  localhost
ip_pc_anda       nama_pc_anda
ip_pc_sebelah    nama_pc_sebelah
```

Contoh : Misalkan ip anda 10.252.105.111 dan anda duduk dikiri maka anda dapat mengisi file /etc/hosts sbb. :

```
# vi /etc/hosts                      -- edit file
----- tambahkan di baris paling akhir
127.0.0.1        localhost.localdomain  localhost
10.252.105.111   pckiri
10.252.105.112   pckanan
```

Setelah itu lakukan pengecekan konektivitas

```
# ping 10.252.105.111  ---- cek konektivitas
# ping pckiri
# ping 10.252.105.112  ---- cek konektivitas
# ping pckanan
```

15. Mencoba ssh server

Jika anda duduk di kiri, ketiklah perintah berikut ini. Jika anda duduk sebelah kanan, sesuaikan dengan perintah sejenis.

```
# hostname                        -- catat nama hostnya
# ssh pckanan -l userkiri
The authenticity of host 'localhost (127.0.0.1)' can't
be established.
RSA key fingerprint is
82:0a:7f:f3:f3:5c:cf:87:db:a0:4d:b6:ce:20:26:1c.
Are you sure you want to continue connecting (yes/no)?
yes
```

```
Warning: Permanently added 'localhost' (RSA) to the list
of known hosts.
userkiri@pckanan's password: *****
Last login: Wed May  5 08:46:13 2004
$ whoami
$ finger          -- ada berapa orang yang login ?
$ hostname        -- skr anda ada dimana ?
$ pwd             -- dimana home direktory anda ?
$ exit
# hostname        -- kembali ke pc asal
```

Setiap anda melakukan ssh ke remote PC, dimanakah home direktori anda ?

Apakah anda dapat berpindah atau masuk ke direktori /etc, /var, /bin, /usr, /home ?

Direktori apa saja yang tidak dapat anda masuki ?

16. Mencoba service sftp

Perintah-perintah berikut ini akan berhubungan dengan service sftp. Jika anda duduk di kiri, ketiklah perintah berikut ini. Jika anda duduk sebelah kanan, sesuaikan dengan perintah sejenis.

```
# hostname        -- catat nama hostnya
# su -l userkiri   -- mengganti user
$ pwd             -- home dir. userkiri
$ whoami
# sftp pckanan
  userkiri@pckanan's password: *****
  Last login: Wed May  5 08:46:13 2004
sftp> whoami
sftp> finger      -- ada berapa orang yang login ?
sftp> hostname    -- skr anda ada dimana ?
sftp> pwd         -- dimana home direktory anda ?
sftp> exit
$ hostname        -- kembali ke pc asal
```

17. Mencoba upload dan download file

Pertama buatlah beberapa file di pc anda, lalu upload ke pc sebelah menggunakan perintah sftp.


```

$ cd
$ hostname >namapcku
$ whoami > loginku
$ echo $HOME > homedirku
$ mkdir dataku
$ cp /etc/g* /home/dataku
$ ls -l
# sftp pckanan
  userkiri@pckanan's password: *****
sftp> ?          -- baca & pelajari helpnya
sftp> mput *      -- upload file
sftp> lpwd       -- local dir.
sftp> ll         -- local ls
sftp> lcd dataku -- cd dataku di local pc
sftp> lpwd       -- local pwd
sftp> mkdir datakuremote -- buar dir baru di remote pc
sftp> cd datakuremote
sftp> mput *      --upload semua file di dataku (local pc)
                  --ke datakuremote (remote pc)
sftp> ls         -- ls di remote pc
sftp> pwd        -- pwd di remote pc
sftp> ll         -- ls di local pc
sftp> lpwd       -- pwd local pc
sftp> cd /etc
sftp> ls
sftp> lmkdir hasildownload
sftp> lcd hasildownload
sftp> mget passwd* -- download file
sftp> mget group*
sftp> mget host*
sftp> ls
sftp> ll
sftp> bye
$ hostname      -- kembali ke pc asal

```

18. Catat semua hasil percobaan yang anda lakukan.

VI. Laporan Resmi .

FORMAT LAPORAN RESMI

Nama dan NRP mahasiswa

Judul Percobaan : Secure Shell (SSH)

Dasar Teori :

Tugas Pendahuluan :

Hasil percobaan :

Daftar Pertanyaan

1. Berikan kesimpulan hasil praktikum yang anda lakukan.
2. Berikan perbandingan antara telnet dengan ssh
3. Berikan perbandingan antara ftp dan sftp