Secure Shell, Secure Copy dan Secure FTP

Oleh :

Idris Winarno

JURUSAN TEKNOLOGI INFORMASI
POLITEKNIK ELEKTRONIKA NEGERI SURABAYA
INSTITUT TEKNOLOGI SEPULUH NOPEMBER
SURABAYA
2008

Praktikum 3

Secure Shell, Secure Copy dan Secure FTP

I. Tujuan:

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

II. Alat–alat:

1.PC yang terhubung ke sisitem jaringan minimal 2 buah

2.Program yang digunakak adalah:

- Openssh-server-xxx.rpm
- Openssh-clients-xxx.rpm
- Openssh-xxx.rpm

III. Dasar teori

Secure Shell dan Secure FTP

Secure Shell (ssh) adalah suatu protokol yang memfasilitasi system komunikasi yang aman diantara dua system yang menggunakan aristektur client/server serta kemungkinan 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 untama aplikasi ini adalah untuk mengakses mesin seca remote. Bentuk akses remote yang bias diperoleh adalah akses pada mode teks maupun mode grafis/X apabila konfigurasinya mengijinkan.

SSH dirancang untuk mengantikan service-service di system unix/linux yang menggunakan system plain text (seperti telnet, ftp, flogin, 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 sever dank lien 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 secer anda dirusak setelahnya.

Impelmentasi 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 sehingga sangat sulit untuk dibaca tanpa mengetahui kode enkripsinya.
- Client dapat memfoward aplikasi Xwindos/X11 ke server.

IV. Langkah percobaan:

1. Login ke sistem Linux sebagai root

2. Mengaktifkan service ssh server

```
[root@WSC204-02 root]# /etc/init.d/sshd start
Starting sshd:                                [  OK  ]
[root@WSC204-02 root]# /etc/init.d/sshd stop
Stopping sshd:                                [  OK  ]
[root@WSC204-02 root]# /etc/init.d/sshd restart
Stopping sshd:                                [FAILED]
Starting sshd:                                [  OK  ]
```

Untuk menjalankan ssh server digunakan perintah **# /etc/init.d/sshd start**
Untuk memeatikan ssh server digunakan perintah **# /etc/init.d/sshd stop**
Untuk menjalankan ulang ssh server digunakan perintah **# /etc/init.d/sshd restart**

3. Memeriksa proses sshd

Setelah program sshd (ssh daemon) dijalankan, periksalah apakah sshd sudah aktif dimemory?

```
[root@WSC204-02 root]# ps -aux|grep sshd
root      1996  0.0  0.0  3508  240 ?        S    10:05   0:00 /usr/sbin/sshd
root      2016  0.0  0.1  3504  444 pts/0    D    10:10   0:00 grep sshd

[root@WSC204-02 root]# netstat -a|grep ssh
tcp        0      0 *:ssh                   *:*                     LISTEN
unix  2      [ ACC ]     STREAM     LISTENING     2353   /tmp/ssh-
XXTQq2DA/agent.1199
```

Sshd berjalan pada nomor proses 1996. Sedang protokol yang digunakan adalah potokol **tcp**

4. Catatlah berapa nomor port yang digunakan oleh service ssh

```
[root@WSC204-02 root]# cat /etc/services|grep ssh
ssh             22/tcp                          # SSH Remote Login Protocol
ssh             22/udp                          # SSH Remote Login Protocol
x11-ssh-offset  6010/tcp                        # SSH X11 forwarding offset
```

Nomor port yang digunakan ssh adalah **port 22**

5. Menghapus rule firewall.

Redhad Linux versi 8 atau yang lebih baru, akan mengaktifkan firewall secara default sehingga semua akses dari luar akan ditolak. Untuk kepnetingan percobaan ini, ada baiknya sementara semua rule firewall dihapus.

```
[root@WSC204-02 root]# iptables -F
```

6. Ujicoba dari localhost.

```
[root@WSC204-02 root]# ssh localhost
root@localhost's password:

[root@WSC204-02 root]# /etc/rc.d/init.d/sshd stop
Stopping sshd:                                             [  OK  ]
[root@WSC204-02 root]# ssh localhost
ssh: connect to host localhost port 22: Connection refused
```

Jika koneksi ssh ke localhost berhasil maka akan tampil pesan permintaan password **root@localhost's password:**

Sedang jika koneksi ssh ke localhost gagal maka akan tampil pesan **Connection refused**

7. Percobaan kelompok

a. Membuat account

```
[root@WSC204-02 root]# useradd windi -g friend
[root@WSC204-02 root]# passwd windi
Changing password for user windi.
New password:
Retype new password:
passwd: all authentication tokens updated successfully.

[root@WSC204-02 root]# useradd idris -g friend
[root@WSC204-02 root]# passwd idris
Changing password for user idris
New password:
Retype new password:
passwd: all authentication tokens updated successfully.
```

b. Membackup dan mengedit file /etc/hosts

```
[root@WSC204-02 /]# cp /etc/hosts /etc/hosts.asli
[root@WSC204-02 /]# vi /etc/hosts
127.0.0.1  localhost.localdomain localhost
10.252.105.101 server
10.252.105.102 wsc204-02 idris
10.252.105.103 wsc204-03 windi
10.252.105.104 wsc204-04
10.252.105.105  wsc204-05
10.252.105.106  wsc204-06
10.252.105.107  wsc204-07
.....
.....
.....
10.252.105.132  wsc204-print
10.252.105.133  wsc204-33
```

c. Pengecekan konektifitas

```
[root@WSC204-02 /]# ping windi
PING windi (10.252.105.103) 56(84) bytes of data.
64 bytes from wsc204-03 (10.252.105.103): icmp_seq=1 ttl=64 time=0.295 ms
64 bytes from wsc204-03 (10.252.105.103): icmp_seq=2 ttl=64 time=0.160 ms
64 bytes from wsc204-03 (10.252.105.103): icmp_seq=3 ttl=64 time=0.154 ms
64 bytes from wsc204-03 (10.252.105.103): icmp_seq=4 ttl=64 time=0.158 ms

--- windi ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 2997ms
rtt min/avg/max/mdev = 0.154/0.191/0.295/0.062 ms

[root@WSC204-02 /]# ping idris
PING windi (10.252.105.102) 56(84) bytes of data.
64 bytes from wsc204-02 (10.252.105.102): icmp_seq=1 ttl=64 time=0.295 ms
64 bytes from wsc204-02 (10.252.105.102): icmp_seq=2 ttl=64 time=0.160 ms
64 bytes from wsc204-02 (10.252.105.102): icmp_seq=3 ttl=64 time=0.154 ms
64 bytes from wsc204-02 (10.252.105.102): icmp_seq=4 ttl=64 time=0.158 ms

--- windi ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 2997ms
rtt min/avg/max/mdev = 0.154/0.191/0.295/0.062 ms
```

8. Mencoba ssh server

```
[root@WSC204-02 /]# hostname
WSC204-02

[root@WSC204-02 /]# ssh windi -l idris
The authenticity of host 'windi (10.252.105.103)' can't be established.
RSA key fingerprint is ce:f1:82:37:77:29:47:1a:30:a9:1f:17:16:c2:cb:30.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added 'windi' (RSA) to the list of known hosts.
idris@windi's password:
[idris@WSC204-03 idris]$ whoami
```

```
idris
[idris@WSC204-03 idris]$ finger
Login     Name       Tty      Idle  Login Time   Office     Office Phone
idris                pts/1          Aug  4 10:35 (wsc204-02)
root      root       *:0              Aug  4 09:00
root      root        pts/0       1  Aug  4 09:53 (:0.0)

[idris@WSC204-03 idris]$ hostname
WSC204-03
[idris@WSC204-03 idris]$ pwd
/home/idris
[idris@WSC204-03 idris]$ exit
[root@WSC204-02 /]# hostname
WSC204-02
[root@WSC204-02 /]# hostname
WSC204-02
```

Hostname sebelum digunakan ssh adalah **WSC204-02**, namun setelah dilakukan ssh hostname berubah menjadi **WSC204-03** (hostname dari Komputer yang dituju).
Sedang jumlah user yang login dikomputer **WSC204-03** (saat dilakukan ssh) ada 2 yaitu **root** dan **idris**.
Saat dilakukan ssh direktori aktifnya adalah **/home/idris** (direktori dari user)

9. Mencoba service sftp

```
[root@WSC204-02 /]# hostname
WSC204-02
[root@WSC204-02 /]# su -l idris
[idris@WSC204-02 idris]$ pwd
/home/idris
[idris@WSC204-02 idris]$ whoami
idris
[idris@WSC204-02 idris]$ sftp windi
Connecting to windi...
The authenticity of host 'windi (10.252.105.103)' can't be established.
RSA key fingerprint is ce:f1:82:37:77:29:47:1a:30:a9:1f:17:16:c2:cb:30.
Are you sure you want to continue connecting (yes/no)? yes
```

```
Warning: Permanently added 'windi,10.252.105.103' (RSA) to the list of known
hosts.
idris@windi's password:
sftp> whoami
Invalid command.
sftp> finger
Invalid command.
sftp> hostname
Invalid command.
sftp> pwd
Remote working directory: /home/idris
sftp> Connection to windi closed by remote host.
[idris@WSC204-02 idris]$ hostname
WSC204-02
```

Perintah **whoami**, **finger**, dan **hostname** tidak dapat digunakan di dalam program ftp karena ftp di khususkan untuk transfer file (bukan untuk remote accsess).

10. Mencoba upload dan download file

```
[idris@WSC204-02 idris]$ cd
[idris@WSC204-02 idris]$ hostname>namapcku
[idris@WSC204-02 idris]$ whoami>loginku
[idris@WSC204-02 idris]$ echo $HOME>homedirku
[idris@WSC204-02 idris]$ mkdir dataku
[idris@WSC204-02 idris]$ cp /etc/g* /home/idris/dataku
cp: omitting directory `/etc/gconf'
cp: omitting directory `/etc/gimp'
cp: omitting directory `/etc/gnome'
cp: omitting directory `/etc/gnome-vfs-2.0'
cp: omitting directory `/etc/gnucash'
cp: cannot open `/etc/group.lock' for reading: Permission denied
cp: cannot open `/etc/grub.conf' for reading: Permission denied
cp: cannot open `/etc/gshadow' for reading: Permission denied
cp: cannot open `/etc/gshadow-' for reading: Permission denied
cp: cannot open `/etc/gshadow.lock' for reading: Permission denied
```

```
cp: omitting directory `/etc/gtk'
cp: omitting directory `/etc/gtk-2.0'
[idris@WSC204-02 idris]$ ls -l
total 20
drwxrwxr-x    2 idris    idris        4096 Aug  4 11:08 dataku
-rw-rw-r--    1 idris    idris          12 Aug  4 11:07 homedirku
-rw-rw-r--    1 idris    idris           6 Aug  4 11:07 loginku
-rw-rw-r--    1 idris    idris          10 Aug  4 11:07 namapcku
drwxr-xr-x    2 idris    idris        4096 Aug  4 10:44 public_html
[idris@WSC204-02 idris]$ sftp windi
Connecting to windi...
idris@windi's password:
sftp> ?
Available commands:
cd path                      Change remote directory to 'path'
lcd path                     Change local directory to 'path'
chgrp grp path               Change group of file 'path' to 'grp'
chmod mode path              Change permissions of file 'path' to 'mode'
chown own path               Change owner of file 'path' to 'own'
help                         Display this help text
get remote-path [local-path]  Download file
lls [ls-options [path]]      Display local directory listing
ln oldpath newpath           Symlink remote file
lmkdir path                  Create local directory
lpwd                         Print local working directory
ls [path]                    Display remote directory listing
lumask umask                 Set local umask to 'umask'
mkdir path                   Create remote directory
put local-path [remote-path]  Upload file
pwd                          Display remote working directory
exit                         Quit sftp
quit                         Quit sftp
rename oldpath newpath       Rename remote file
rmdir path                   Remove remote directory
rm path                      Delete remote file
symlink oldpath newpath      Symlink remote file
version                      Show SFTP version
!command                     Execute 'command' in local shell
```

```
!                    Escape to local shell
?                    Synonym for help
sftp> mput namapcku
Uploading namapcku to /home/idris/namapcku
sftp> lpwd
Local working directory: /home/idris
sftp> lls
dataku  homedirku  loginku  namapcku  public_html
sftp> lcd dataku
sftp> lpwd
Local working directory: /home/idris/dataku
sftp> mkdir datakuremote
sftp>cd datakuremote
sftp> mput *
Uploading gnome-vfs-mime-magic to /home/idris/datakuremote/gnome-vfs-mime-
magic
Uploading gpm-root.conf to /home/idris/datakuremote/gpm-root.conf
Uploading group to /home/idris/datakuremote/group
Uploading group- to /home/idris/datakuremote/group-
Uploading hasildownload to /home/idris/datakuremote/hasildownload
sftp> ls
.
..
gnome-vfs-mime-magic
gpm-root.conf
group
group-
hasildownload
sftp> pwd
Remote working directory: /home/idris/datakuremote
sftp> lpwd
Local working directory: /home/idris
sftp>cd /etc
sftp> ls
.
..
.aumixrc
.pwd.lock
```

CORBA

DIR_COLORS

DIR_COLORS.xterm

FreeWnn

Muttrc

.....

.....

.....

ypserv.conf

ytalkrc

zebra

zlogin

zlogout

zprofile

zshenv

zshrc

sftp>lmkdir hasildownload

sftp>lcd hasildownload

sftp> mget passwd*

Fetching /etc/passwd to passwd

Fetching /etc/passwd- to passwd-

Fetching /etc/passwd.lock to passwd.lock

Couldn't get handle: Permission denied

sftp> mget group*

Fetching /etc/group to group

Fetching /etc/group- to group-

Fetching /etc/group.lock to group.lock

Couldn't get handle: Permission denied

sftp> mget host*

Fetching /etc/host.conf to host.conf

Fetching /etc/hosts to hosts

Fetching /etc/hosts.allow to hosts.allow

Fetching /etc/hosts.asli to hosts.asli

Fetching /etc/hosts.bak to hosts.bak

Fetching /etc/hosts.canna to hosts.canna

Fetching /etc/hosts.deny to hosts.deny

Fetching /etc/hosts.whyen to hosts.whyen

Fetching /etc/hosts~ to hosts~

```
sftp> ls
.
..
.aumixrc
.pwd.lock
CORBA
DIR_COLORS
DIR_COLORS.xterm
FreeWnn
Muttrc
X11
a2ps-site.cfg
a2ps.cfg
adjtime
aep
aep.conf
aeplog.conf
alchemist
aliases
.....
.....
.....
zlogin
zlogout
zprofile
zshenv
zshrc
sftp> lls
group  host.conf  hosts~  hosts.asli  hosts.canna  hosts.whyen  passwd-
group-  hosts  hosts.allow  hosts.bak  hosts.deny  passwd
sftp>bye
[idris@WSC204-02 idris]$ hostname
WSC204-02
```

Untuk meng-upload file digunakan perintah **mput**, sedang untuk mendownload file digunakan perintah **mget**.
Untuk melihat isi file dari computer yang dituju digunakan perintah **ls** sedang untuk melihat isi dari komputer kita, kita digunakan perintah **lls**.
Untuk pindah direktori pada komputer kita, kita gunakan perintah **lcd**.

11. Mencoba service scp

```
[idris@WSC204-02 idris]$ cd
[idris@WSC204-02 idris]$ touch kiri1 kiri2 kiri3
[idris@WSC204-02 idris]$ ls
dataku  hasildownload  kiri1  kiri3   namapcku
hasil   homedirku      kiri2  loginku  public_html
[idris@WSC204-02 idris]$ scp kiri* idris@windi:/home/idris
idris@windi's password:
kiri1              100% |*****************************|     0       00:00
kiri2              100% |*****************************|     0       00:00
kiri3              100% |*****************************|     0       00:00
[idris@WSC204-02 idris]$ cp /etc/g* dirbaru
cp: omitting directory `/etc/gconf'
cp: omitting directory `/etc/gimp'
cp: omitting directory `/etc/gnome'
cp: omitting directory `/etc/gnome-vfs-2.0'
cp: omitting directory `/etc/gnucash'
cp: cannot open `/etc/group.lock' for reading: Permission denied
cp: cannot open `/etc/grub.conf' for reading: Permission denied
cp: cannot open `/etc/gshadow' for reading: Permission denied
cp: cannot open `/etc/gshadow-' for reading: Permission denied
cp: cannot open `/etc/gshadow.lock' for reading: Permission denied
cp: omitting directory `/etc/gtk'
cp: omitting directory `/etc/gtk-2.0'
[idris@WSC204-02 idris]$ ls -l
total 32
drwxrwxr-x    3 idris    idris        4096 Aug  4 11:15 dataku
drwxrwxr-x    2 idris    idris        4096 Aug  4 11:27 dirbaru
drwxrwxr-x    2 idris    idris        4096 Aug  4 11:22 hasil
drwxrwxr-x    2 idris    idris        4096 Aug  4 11:23 hasildownload
-rw-rw-r--    1 idris    idris          12 Aug  4 11:07 homedirku
-rw-rw-r--    1 idris    idris           0 Aug  4 11:25 kiri1
```

```
-rw-rw-r--    1 idris    idris          0 Aug  4 11:25 kiri2
-rw-rw-r--    1 idris    idris          0 Aug  4 11:25 kiri3
-rw-rw-r--    1 idris    idris          6 Aug  4 11:07 loginku
-rw-rw-r--    1 idris    idris         10 Aug  4 11:07 namapcku
drwxr-xr-x    2 idris    idris       4096 Aug  4 10:44 public_html
[idris@WSC204-02 idris]$ scp -r dirbaru idris@windi:/home/idris
idris@windi's password:
gnome-vfs-mime-magic 100% |*****************************|  9167
00:00
gpm-root.conf       100% |*****************************|  1756       00:00
group               100% |*****************************|   934       00:00
group-              100% |*****************************|   921       00:00
[idris@WSC204-02 idris]$ ls
dataku   hasil          homedirku  kiri2  loginku   public_html
dirbaru  hasildownload  kiri1     kiri3  namapcku
[idris@WSC204-02 idris]$ scp -r idris@windi:/home/idris /etc
cp: cannot stat `idris@windi:/etc': No such file or directory
```

Pada saat ingin melakukan copy ke remote komputer pada directory **/etc** tidak dapat dilakukan karena akses ke **/etc** hanya diperbolehkan untuk **root** saja.

12. Ethereal 1

- Lakukan TCP dump menggunakan ethereal
- Buat routing untuk menghubunkan komputer remote ke client
- Lakukan TCP dump untuk login Telnet
- Lakukan TCP dump untuk SSH

13. Tunneling menggunakan ssh

```
[root@WSC204-01 root]# ssh –L 0.0.0.0:80:10.252.105.102:80 10.252.105.102 –l
idris
idris@10.252.105.102 password:
[idris@WSC204-02 root]$
```

Setelah berhasil melakukan login ke komputer tujuan maka klien akan membuat port untuk melakukan binding ke komputer klient

14. Tes tunneling

- Buka web browser
- Akses http://10.252.105.101/
- Akses http://localhost/

15. Ethereal 2

- Lakukan TCP dump menggunakan ethereal
- Buat routing untuk menghubunkan komputer remote ke client
- Lakukan TCP dump pada routing untuk http://10.252.105.101 pada client
- Lakukan TCP dump pada routing untuk http://localhost pada client

16. Password-less SSH

- $ ssh-keygen –t rsa

  Generating public/private rsa key pair.

  Enter file in which to save the key (/home/idris/.ssh/id_rsa):

  Enter passphrase (empty for no passphrase):

  Enter same passphrase again:

  Your identification has been saved in /home/idris/.ssh/id_rsa.

  Your public key has been saved in /home/idris/.ssh/id_rsa.pub.

  The key fingerprint is:

  55:19:fb:37:55:91:a3:b6:cd:52:0e:32:09:32:08:aa idris@n4n0
- Copy-kan file /home/idris/.ssh/id_rsa.pub ke computer tujuan pada directory /home/xxx/.ssh/`authorized_keys (gunakan sftp)`
- Lakukan login ke komputer client