

# LAPORAN JARINGAN KOMPUTER II

SSH



Disusun Oleh :

Adham Hayukalbu | IK-2B | 3.34.12.1.01

Jurusan Elektro

Teknik Informatika

**Politeknik Negeri Semarang**

**2012/2014**

## I. Tujuan

Setelah menyelesaikan praktek ini, mahasiswa dapat :

- a. menjelaskan Konsep SSH sederhana
- b. mengkonfigurasi SSH pada Mesin Linux

## II. Dasar Teori

Program sshd (SSH Daemon) adalah daemon untuk program SSH (secure shell). Program SSH digunakan untuk login dalam suatu mesin (komputer) dari jauh (secara remote) dan mengeksekusi perintah pada mesin tersebut. Program ssh ini mirip dengan telnet, tetapi punya pengendalian terhadap keamanan. Program ssh menyediakan komunikasi aman terenkripsi antara dua host yang tidak saling kenal melalui jaringan yang umumnya tidak aman. Dengan alasan keamanan, fungsi program telnet sudah mulai ketinggalan diganti dengan ssh.

Program sshd adalah daemon yang menunggu koneksi dari klien pada port22. Program ini akan membuat cabang daemon baru untuk tiap koneksi yang datang. Masing-masing daemon menangani secara mandiri pertukaran kunci, enkripsi, autentikasi, eksekusi perintah dan pertukaran data. Penerapan program sshd mendukung protokol SSH versi1 dan versi2 secara serentak.

## III. Peralatan yang Digunakan

- |   |                   |
|---|-------------------|
| 1) PC Komputer sebagai Server             | 1 unit            |
| 2) PC Komputer sebagai Client/workstation | 8 unit atau lebih |
| 3) Alat penghubung Switch/hub             | 1 unit            |
| 4) Kabel UTP                              | secukupnya        |
| 5) Port RJ45                              | secukupnya        |
| 6) Crippling tools                        |                   |
| 7) Tester kabel                           |                   |

## IV. Langkah dan Lembar Kerja

1. Pertama, install server SSH terlebih dahulu menggunakan user root.
2. Login pada root terlebih dahulu,

```
root@ubuntu: /home/sojoyenjoy
root@ubuntu:/home/sojoyenjoy# apt-get install openssh-server
```

3. kemudian ketikkan perintah berikut

**# apt-get install openssh-server**

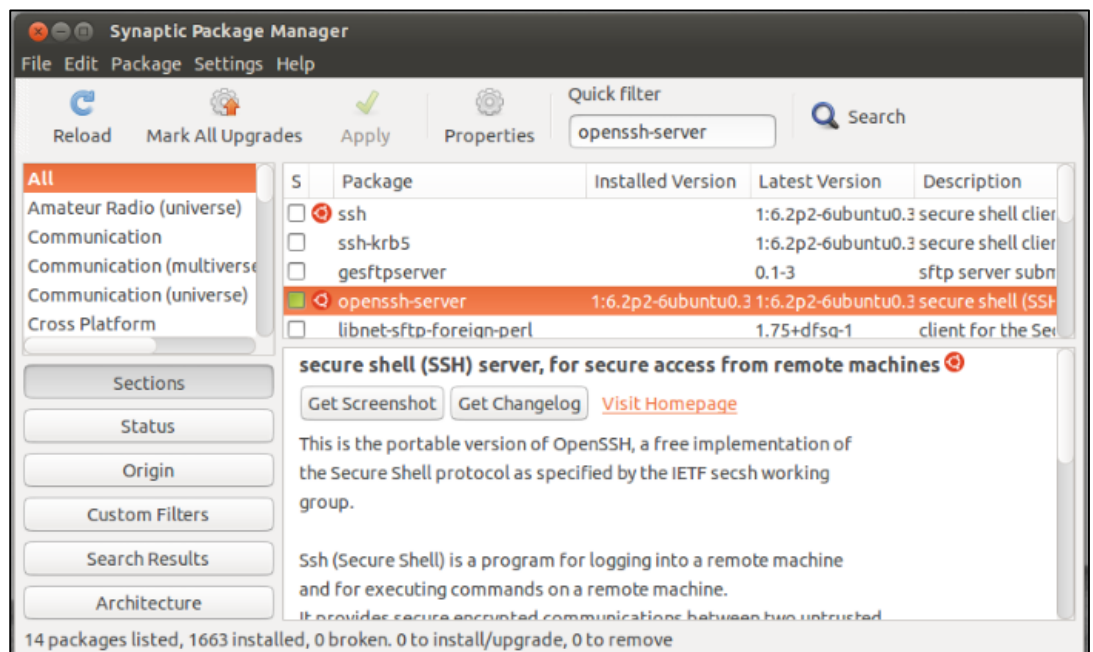
```
root@ubuntu: /home/sojoyenjoy
root@ubuntu:/home/sojoyenjoy# apt-get install openssh-server
```

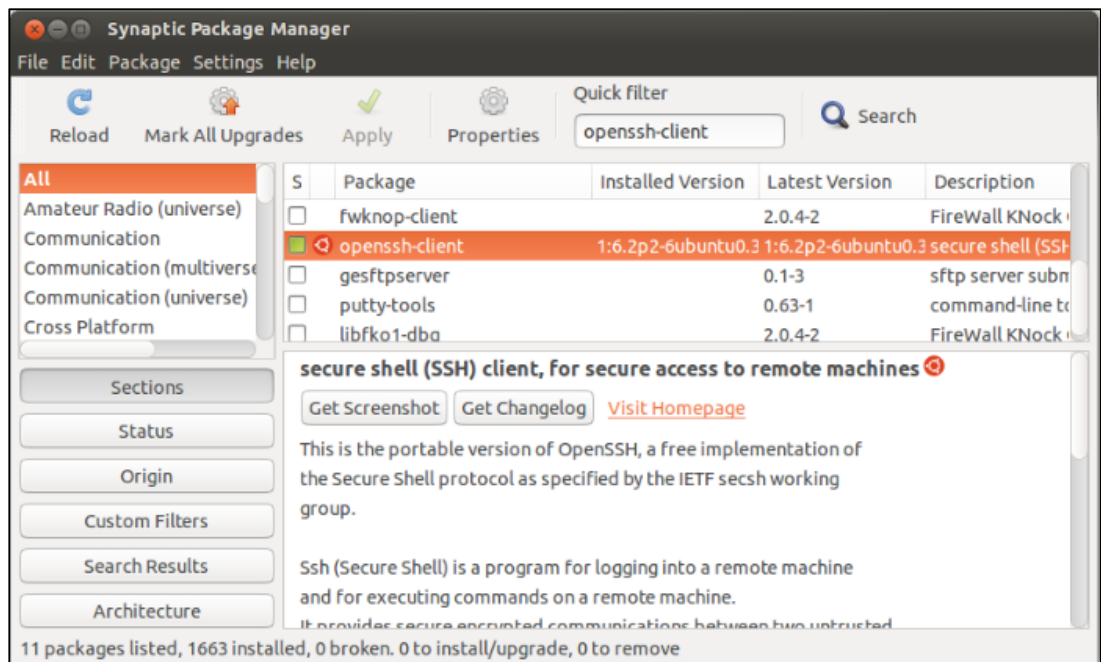
4. Ketikkan Y untuk melanjutkan proses instalasi SSH.

```
root@ubuntu: /home/sojoyenjoy
root@ubuntu:/home/sojoyenjoy# apt-get install openssh-server
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following extra packages will be installed:
  libck-connector0 ncurses-term openssh-client python-requests python-urllib3
  ssh-import-id
Suggested packages:
  libpam-ssh keychain monkeysphere openssh-blacklist openssh-blacklist-extra
  rssh molly-guard
The following NEW packages will be installed:
  libck-connector0 ncurses-term openssh-server python-requests python-urllib3
  ssh-import-id
The following packages will be upgraded:
  openssh-client
1 upgraded, 6 newly installed, 0 to remove and 55 not upgraded.
Need to get 789 kB/1,279 kB of archives.
After this operation, 3,507 kB of additional disk space will be used.
Do you want to continue [Y/n]?
```

```
root@ubuntu: /home/sojoyenjoy
Selecting previously unselected package ssh-import-id.
Unpacking ssh-import-id (from ../ssh-import-id_3.19-0ubuntu1_all.deb) ...
Processing triggers for man-db ...
Processing triggers for ureadahead ...
ureadahead will be reprofiled on next reboot
Processing triggers for ufw ...
Setting up libck-connector0:amd64 (0.4.5-3.1ubuntu2) ...
Setting up openssh-client (1:6.2p2-6ubuntu0.4) ...
Setting up ncurses-term (5.9+20130608-1ubuntu1) ...
Setting up openssh-server (1:6.2p2-6ubuntu0.4) ...
Creating SSH2 RSA key; this may take some time ...
Creating SSH2 DSA key; this may take some time ...
Creating SSH2 ECDSA key; this may take some time ...
ssh start/running, process 3410
Setting up python-urllib3 (1.6-2) ...
Setting up python-requests (1.2.3-1) ...
Setting up ssh-import-id (3.19-0ubuntu1) ...
Processing triggers for libc-bin ...
Processing triggers for ureadahead ...
Processing triggers for ufw ...
root@ubuntu: /home/sojoyenjoy#
```

5. Kemudian cek instalasi paket SSH pada synaptic laptop anda.  
Apabila telah berwarna hijau maka aplikasi paket SSH telah terinstall.





6. Kemudian lakukan pembuatan password pada user root pada PC anda.

```

root@ubuntu: ~
root@ubuntu:/home/sojoyenjoy# passwd root
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully

```

7. Kemudian coba uji paket SSH yang telah diinstallkan dengan mengetikkan perintah berikut :

# ssh IP Address

```

root@ubuntu: ~
root@ubuntu:/home/sojoyenjoy# ssh 192.168.150.25
root@192.168.150.25's password:
Welcome to Ubuntu 13.10 (GNU/Linux 3.11.0-20-generic x86_64)

* Documentation:  https://help.ubuntu.com/

Last login: Fri May 30 08:40:40 2014 from adham-01.net
root@ubuntu:~#

```

Akan muncul pertanyaan apakah anda akan melanjutkan koneksi jika iya maka ketikkan yes kemudian enter.

8. Kemudian masukkan password root yang telah anda dibuat sebelum langkah ini.

Sojoyenjoy-pc

```
root@ubuntu: ~
root@ubuntu:/home/sojoyenjoy# ssh 192.168.150.25
root@192.168.150.25's password:
Welcome to Ubuntu 13.10 (GNU/Linux 3.11.0-20-generic x86_64)

 * Documentation:  https://help.ubuntu.com/

Last login: Fri May 30 08:40:40 2014 from adham-01.net
root@ubuntu:~#
```

9. Setelah login kedalam IP Address PC RizkaHadi maka akan dapat digunakan untuk bertukar pesan seperti berikut.

```
root@ubuntu:~#
Message from root@ubuntu on pts/18 at 09:25 ...
EOF

Message from root@ubuntu on pts/18 at 09:25 ...
hallo
█
```

10. Setelah masuk kedalam SSH maka akan terdapat tulisan selamat datang user baru selamat belajar hal tersebut berrarti anda berhasil login kedalam SSH. Maka selanjutnya anda dapat melakukan koneksi dengan user lainnya dengan cara mengetikkan perintah berikut :

# SSH IP Address

Pada percobaan kali ini saya mencoba melakukan koneksi dengan DIKA-PC dengan nomor IP 192.168.150.17

```
root@ubuntu: ~
root@ubuntu:~# ssh 192.168.150.17
root@192.168.150.17's password:
Welcome to Ubuntu 13.10 (GNU/Linux 3.11.0-19-generic x86_64)

 * Documentation:  https://help.ubuntu.com/

New release '14.04' available.
Run 'do-release-upgrade' to upgrade to it.

"Selamat Datang User, Selamat Belajar"
Last login: Fri May 30 10:28:01 2014 from ubuntu-4.local
root@ubuntu:~# █
```

Kemudian setelah saya berhasil login selanjutnya saya dapat melakukan chating atau wall kepada DIKA-PC

```
root@ubuntu: ~
root@ubuntu:~# wall
dika setya puspita hai selamat belajar

Broadcast Message from root@ubuntu
(/dev/pts/17) at 10:29 ...

dika setya puspita hai selamat belajar

Broadcast Message from root@ubuntu
(/dev/pts/17) at 10:29 ...

dika setya puspita hai selamat belajar

root@ubuntu:~# █
```

11. Kemudian ketikkan perintah write root pts/17.

```
root@ubuntu: ~
root@ubuntu:~# write root pts/17
write: write: you have write permission turned off.

dika
█
```

Maka dari DIKA-PC dapat membalas seperti berikut :

```
root@ubuntu: ~
root@ubuntu:~# write root pts/17
write: write: you have write permission turned off.

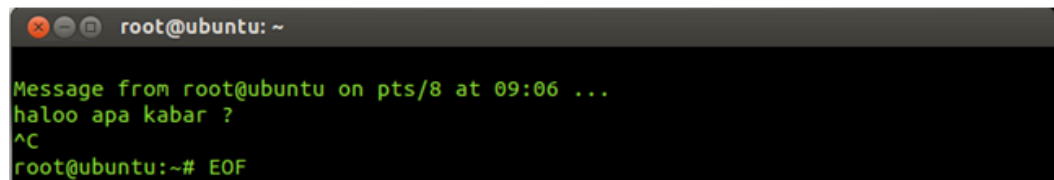
dika
hadi
hai dik, kamu lagi belajar jarkom?

Message from root@ubuntu on pts/18 at 09:31 ...
lya Hadi, kamu juga?
oke dik selamat belajar
```

12. Setelah melihat pada finger kemudian pilih pts yang telah masuk pada SSH PC anda maka anda dapat melakukan wall dengan user lain, dengan mengetikkan perintah berikut :

# Wall

Kemudian enter setelah itu tekan ctrl + d maka anda akan dapat mengirim pesan seperti berikut :



```
root@ubuntu: ~  
Message from root@ubuntu on pts/8 at 09:06 ...  
haloo apa kabar ?  
^C  
root@ubuntu:~# EOF
```

## V. Pertanyaan

1. Jelaskan dalam user apa, instruksi ssh dilaksanakan dan apa alasannya?

Jawab :

Paket SSH sendiri berfungsi untuk kebutuhan akses ke console server secara aman. Pada instruksi atau cara menggunakan paket instalasi SSH hanya dapat diakses oleh user ROOT saja, mengapa demikian karena pada konfigurasi settingan awal yang diperbolehkan mengakses instruksi SSH adalah user ROOT sehingga user lain tidak dapat mengakses instruksi SSH akan tetapi sebenarnya user lain dapat mengakses instruksi SSH dengan cara menambahkan user lain untuk dapat mengakses instruksi SSH. Akan tetapi kembali lagi pada fungsi dasar SSH untuk kebutuhan komunikasi akses dengan console server sehingga agar aman lebih baik hanya user root saja yang dapat mengakses instruksi SSH.

2. Terangkan langkah-langkah yang dilakukan agar instruksi ssh tak dapat dilaksanakan pada PC yang sedang anda jalankan?

Jawab :

Terdapat 2 cara untuk memutus koneksi pada PC yang sedang dijalankan :

- a. Buka file sshd\_config

Kemudian atur PermitRootLogin menjadi NO hal tersebut bertujuan agar user tersebut tidak dapat mengakses instruksi SSH.

<pre>#Authentication: LoginGraceTime 130 PermitRootLogin NO</pre>
---

- b. Kemudian juga dapat dengan cara lain yaitu mengubah port pada instalasi paket SSH



```
# What ports, Ips and  
PORT 2  
# use these options t
```

3. Terangkan caranya dengan menggunakan instruksi ssh digunakan untuk mendapatkan data dari pasangan PC yang terkoneksi/terhubung?

Jawab :

- Cara mendapatkan data dari pasangan PC yang telah terkoneksi dengan mengetikkan instruksi #SSH IP Address – p
- Atau dengan cara kedua dengan mengetikkan perintah #scp [nama login @ alamat ip]: [/path/namafile namafilebaru]

## VI. Kesimpulan

1. SSH adalah aplikasi pengganti remote login seperti telnet, rsh, dan rlogin, yang jauh lebih aman.
2. Hal yang dapat diimplementasikan dalam instruksi SSH antara lain :
  - untuk login ke shell pada remote host (menggantikan Telnet dan rlogin)
  - untuk mengeksekusi satu perintah pada remote host (menggantikan rsh)
  - untuk menyalin file dari server lokal ke remote host. Lihat SCP, sebagai alternatif untuk rcp
3. Untuk mengkonfigurasi paket default dari aplikasi OpenSSH server, sshd, dengan mengedit file `/etc/ssh/sshd_config`
4. fungsi utamanya adalah untuk menjamin keamanan dalam melakukan transmisi data pada suatu jaringan. SSH banyak dimanfaatkan oleh berbagai network admin di berbagai belahan dunia untuk mengontrol web dan jenis jaringan lainnya seperti WAN.

Fungsi SSH ini sebenarnya adalah dibuat untuk menggantikan protokol sebelumnya yang dianggap sangat rentan terhadap pencurian data melalui malware berbahaya. Protokol tersebut antara lain adalah rlogin, TELNET dan protokol rsh.

### Fungsi SSH

1. Melakukan enkripsi terhadap data yang dikirim
2. Protokol untuk pertukaran data dalam suatu jaringan
3. Otentifikasi, mekanisme untuk memastikan pengirim dan penerima adalah benar dan aman.
4. Kerahasiaan, memastikan kerahasiaan data yang dikirim agar hanya diketahui oleh penerima dan pengirim.

