URAIAN MATERI (REMOTE SERVER)

1. Pengertian *Remote Server*

   Remote access merupakan salah satu teknologi yang digunakan untuk mengakses suatu sistem melalui jaringan sehingga seorang *user* dapat mengkonfigurasi suatu sistem dimana saja asalkan terkoneksi ke internet atau jaringan tersebut. Tentunya *remote server* memiliki banyak manfaat seperti dari melakukan kontrol ke *server* dari jarak jauh, memodifikasi pengaturan *server* dari jarak jauh.

   Salah satu *remote access* yang aman adalah menggunakan SSH (*Secure Shell*). Seperti namanya, SSH menyediakan koneksi untuk melakukan remote dengan aman dengan *interface command line* meskipun dengan jaringan yang tidak aman. Aplikasi dari SSH ini biasanya digunakan untuk *login* sistem UNIX, untuk menggantikan sistem *remote* seperti telnet yang mengirim informasi *password* dengan tulisan biasa tanpa enkripsi.

2. SSH (Secure Shell)

   SSH (*Secure Shell*) adalah sebuah protokol jaringan yang digunakan untuk mengamankan komunikasi antara dua perangkat, seperti komputer dan *server*, melalui jaringan yang tidak aman. Protokol ini memberikan cara untuk mengakses dan mengendalikan perangkat jarak jauh secara aman. SSH menyediakan enkripsi data dan otentikasi pengguna, sehingga data yang dikirim antara perangkat terlindungi dari akses yang tidak sah. Secara *default*, SSH *server* berjalan di atas port 22. Port ini bisa dirubah sesuai kebutuhan dan biasanya dirubah untuk kamuflase yang membuat orang mengira tidak ada SSH server di *server* tersebut.

3. SSH Linux Debian 10

   Paket aplikasi SSH *server* dalam sistem operasi linux debian 10 tidak berjalan secara otomatis, tetapi harus melalui proses instalasi dan konfigurasi. Untuk konfigurasi SSH server di debian 10 panduan lengkapnya ada pada *jobsheet* 2 mengenai cara instalasi hingga uji coba *remote server* menggunakan SSH.

JOBSHEET 2

Konfigurasi Remote Server (SSH) di Debian 10

Konfigurasi pada lembar kerja ini menggunakan topologi seperti dibawah ini. Untuk langkah pengerjaan konfigurasi *remote server* menggunakan SSH di debian 10 dapat mengikuti tahapan dibawah ini.

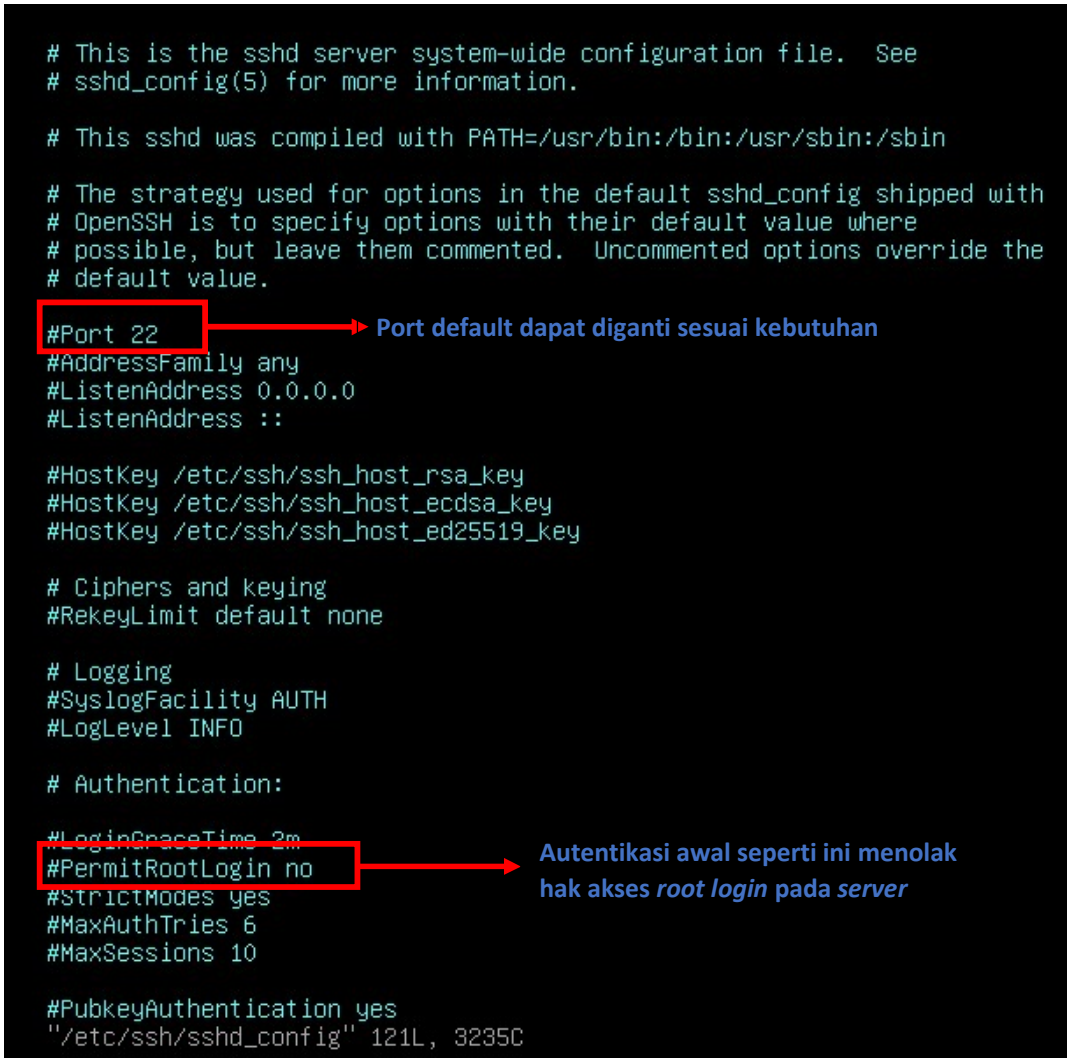
1. *Install* paket *remote server* dengan perintah **apt install openssh-server** untuk melanjutkan install masukkan **y** kemudian enter.

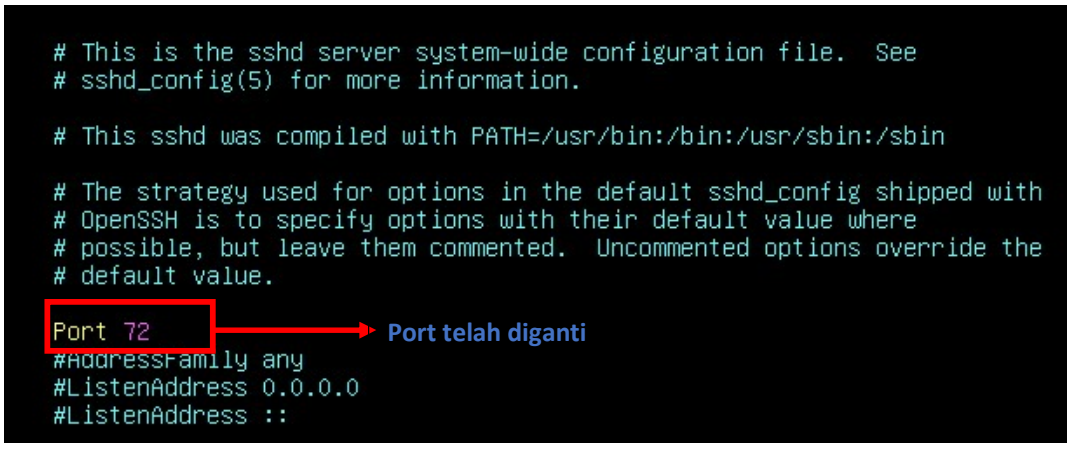
```
root@debian:~# apt install openssh-server
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
  libwrap0 openssh-sftp-server
Suggested packages:
  molly-guard monkeysphere rssh ssh-askpass ufw
The following NEW packages will be installed:
  libwrap0 openssh-server openssh-sftp-server
0 upgraded, 3 newly installed, 0 to remove and 0 not upgraded.
Need to get 0 B/455 kB of archives.
After this operation, 1,719 kB of additional disk space will be used.
Do you want to continue? [Y/n] y_
```

2. Jika paket sudah terinstall lanjut untuk konfigurasi *port* SSH, konfigurasi opsional dan sesuai kebutuhan. Hal ini untuk mengganti *port default* SSH yaitu 22 yang bisa diganti dengan perintah **vim /etc/ssh/sshd_config**

```
root@debian:~# vim /etc/ssh/sshd_config _
```

3. Lanjutkan cari port lalu aktifkan dengan menghapus tanda # **(pagar)** dan anda dapat mengubah 22 sebagai *default port* menjadi port berbeda misalnya 72, 111, 68 dan lainnya. Dan bisa di simpan dengan menekan tombol **shift** dan **z** dua kali secara persamaan atau menggunakan perintah **:wq** lalu enter.





4. Selain *port* ada juga tentang autentikasi *login* menggunakan root yang dapat di aktifkan pada konfigurasi di folder **/etc/ssh/sshd_config**. Jika semua konfigurasi telah selesai simpan konfigurasi

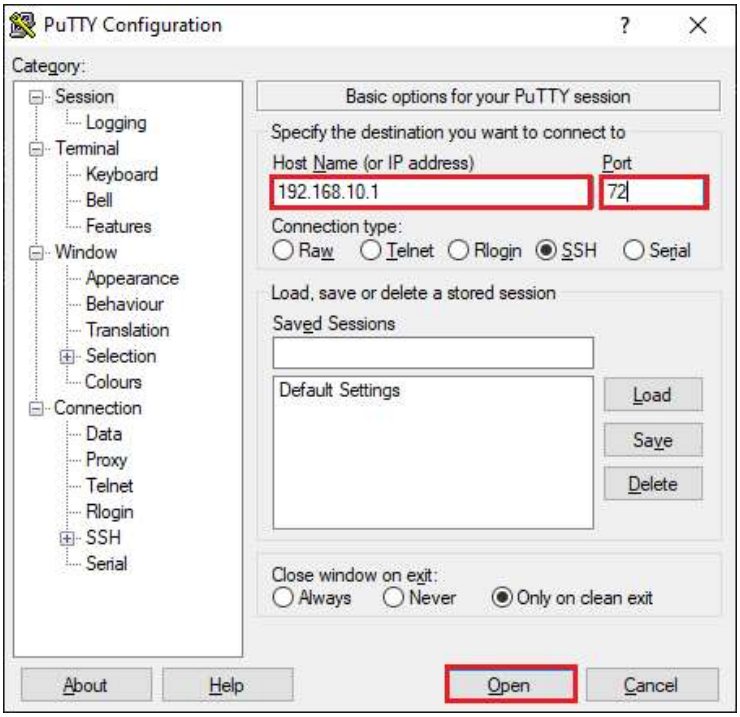
```
# Authentication:

#LoginGraceTime 2m
PermitRootLogin yes
#StrictModes yes
#MaxAuthTries 6
#MaxSessions 10
```

Autentikasi diubah seperti ini memberi izin hak akses *root login* pada *server*

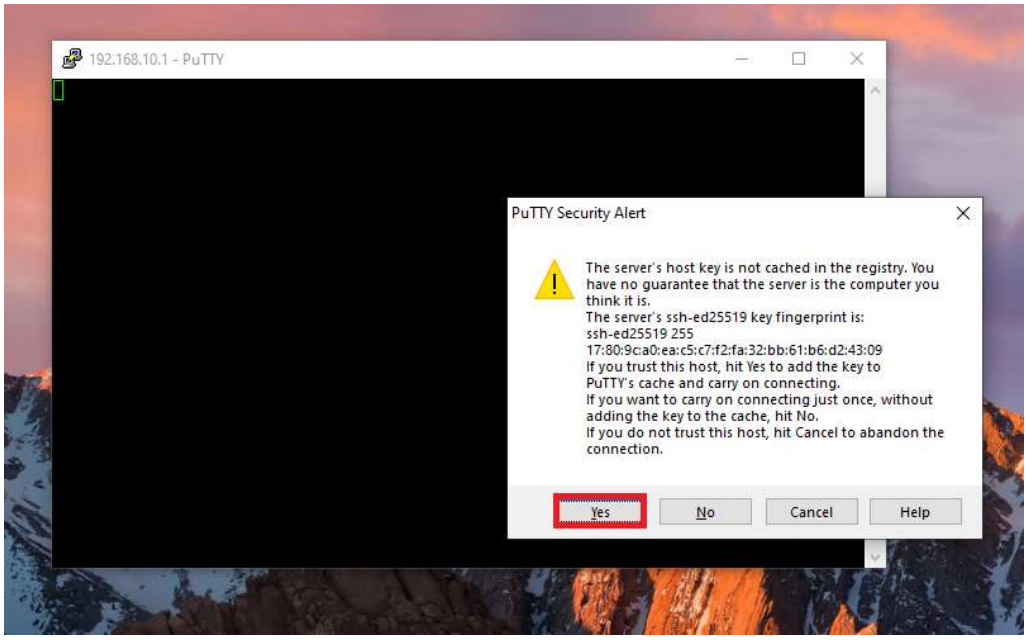
5. Selanjutnya lakukan *restart* untuk mengaktifkan semua konfigurasi yang telah diubah dengan perintah **/etc/init.d/ssh restart.** Jika sudah ada *feedback* keterangan **ok** artinya tidak ada kesalahan dan konfigurasi berhasil.

```
root@debian:~# /etc/init.d/ssh restart
[ ok ] Restarting ssh (via systemctl): ssh.service.
root@debian:~# _
```

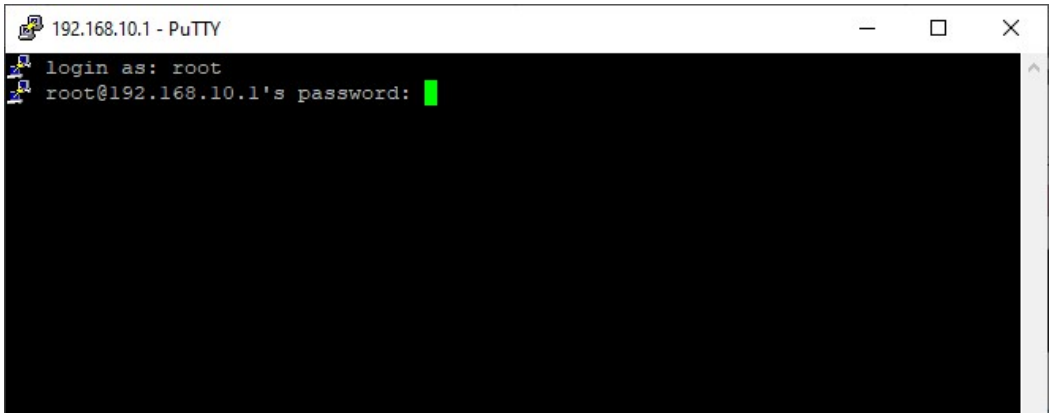
6. Berikutnya adalah uji coba konfigurasi melalui aplikasi **PuTTY**. Namun perlu di ingat sebelumnya bahwa untuk uji coba *server* debian yang anda telah konfigurasi harus memiliki IP *Address*, misal disini IP *Address server* yang digunakan yaitu 192.168.10.1 dan lakukan juga pengaturan jaringan sesuai dengan jaringan *server* yang digunakan. Untuk uji coba ini digunakan jaringan **host-only adapter.** Saat *login* sesuaikan *port* dan IP *Address* yang digunakan.



7. Selanjutnya jika muncul pesan *Putty Security Alert* silakan pilih **Yes** untuk melanjutkan



8. Lalu masukkan *login as* **root** dan masukkan *password server* yang digunakan



9. Jika berhasil maka akan *login* dan anda dapat mengakses *server* anda.