

# **Arsitektur & Organisasi Komputer**

## **“SSH”**



**Dosen Pembimbing :**

Adi Hermansyah, S.Kom., M.T.

**Disusun Oleh :**

Prita Salma (09030582226036)

**Fakultas Ilmu Komputer**

**Program Studi Teknik Komputer**

**UNIVERSITAS SRIWIJAYA 2022/2023**

# MENJALANKAN SSH

## 1.1 TUJUAN

1. Memberikan pemahaman mendalam mengenai penggunaan SSH (Secure Shell) pada sistem Ubuntu Server.
2. Menjelaskan tujuan dari implementasi SSH
3. Memberikan panduan praktis mengenai cara menjalankan SSH pada Ubuntu Server dan cara mengaksesnya menggunakan alamat IP.
4. Diharapkan pembaca dapat memahami pentingnya keamanan dalam mengakses dan mengelola sistem jarak jauh serta memiliki keterampilan praktis dalam mengimplementasikan SSH pada Ubuntu Server.

## 1.2 ALAT

Dalam pratikum ini kita menggunakan :

1. Ubuntu Server
2. Putty
3. Windows + R > CMD

## 1.3 DASAR TEORI

SSH adalah singkatan dari Secure Shell. Ini adalah protokol jaringan yang memungkinkan pengguna untuk mengakses dan mengelola sistem jarak jauh secara aman melalui koneksi jaringan yang terenkripsi. Dengan menggunakan SSH, informasi yang dikirim antara perangkat pengguna dan server dienkripsi, sehingga menjaga keamanan dan privasi data selama proses komunikasi.

Penggunaan utama SSH adalah untuk mengakses dan mengelola sistem atau server jarak jauh tanpa harus berada di lokasi fisik. Hal ini sangat berguna dalam pengelolaan server, pemeliharaan, dan pemecahan masalah dari jarak jauh. Selain itu, SSH juga memungkinkan untuk melakukan transfer file secara aman antara dua perangkat, membuat tunneling untuk mengamankan koneksi jaringan, dan menyediakan berbagai mekanisme otentikasi untuk memverifikasi identitas pengguna yang mencoba mengakses sistem.

Menjalankan SSH (Secure Shell) pada Ubuntu Server memungkinkan pengguna untuk mengakses dan mengelola sistem secara aman melalui koneksi jaringan. SSH adalah protokol yang memungkinkan pertukaran data yang terenkripsi antara dua perangkat, sehingga memastikan keamanan komunikasi. Untuk menjalankan SSH pada Ubuntu Server, pertama-tama pastikan bahwa paket OpenSSH sudah terinstal di sistem Anda. OpenSSH adalah implementasi dari protokol SSH yang paling umum digunakan pada sistem Linux.

Untuk memulai, buka terminal pada Ubuntu Server dan pastikan Anda telah masuk sebagai pengguna dengan hak administratif atau memiliki izin untuk menjalankan perintah sebagai sudo. Jika OpenSSH belum terinstal, Anda dapat menginstalnya dengan perintah:

```
sudo apt-get install openssh-server
```

Setelah instalasi selesai, SSH akan secara otomatis mulai berjalan. Anda dapat memeriksa statusnya dengan perintah:

```
sudo systemctl status ssh
```

Untuk mengakses Ubuntu Server melalui SSH menggunakan alamat IP, Anda perlu tahu alamat IP dari server tersebut. Alamat IP ini dapat berupa alamat IP lokal di jaringan lokal Anda atau alamat IP publik yang dapat diakses melalui internet. Untuk terhubung ke server menggunakan SSH, gunakan perintah berikut:

```
ssh username@alamat_ip
```

Gantilah "username" dengan nama pengguna Anda di Ubuntu Server dan "alamat\_ip" dengan alamat IP dari server tersebut. Setelah itu, Anda akan diminta untuk memasukkan kata sandi pengguna. Setelah berhasil, Anda akan masuk ke shell pada server melalui koneksi SSH yang aman.

## 1.4 PRATIKUM

### Langkah-langkah untuk Menjalankan SSH pada Ubuntu Server

- 1) Login terlebih dahulu, login menggunakan Hostname dan Password yang telah kita buat sebelumnya

```
prita login: prita
Password:
Welcome to Ubuntu 20.04.5 LTS (GNU/Linux 5.4.0-139-generic x86_64)
```

- 2) Jangan lupa untuk selalu mengupdate

```
prita@prita:~$ sudo apt update
```

- 3) Ketik **ifconfig** untuk melihat Alamat ip kita

```
prita@prita:~$ ifconfig
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 10.1.9.106 netmask 255.255.252.0 broadcast 10.1.11.255
    inet6 fe80::a00:27ff:fef3:d661 prefixlen 64 scopeid 0x20<link>
    ether 08:00:27:f3:d6:61 txqueuelen 1000 (Ethernet)
    RX packets 373 bytes 41301 (41.3 KB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 40 bytes 4644 (4.6 KB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 88 bytes 6784 (6.7 KB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 88 bytes 6784 (6.7 KB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

```
prita@prita:~$ curl ifconfig.me
103.208.137.90prita@prita:~$
```

- 4) Memastikan OpenSSH Terinstal: Pastikan paket OpenSSH telah terinstal di Ubuntu Server. Jika belum, instal dengan perintah:

```
sudo apt-get install openssh-server
```

- 5) Memulai Layanan SSH: Setelah instalasi, SSH akan mulai berjalan secara otomatis. Namun, jika belum, gunakan perintah:

```
sudo systemctl start ssh
```

- 6) Untuk Memeriksa Status SSH: Kita dapat memeriksa status SSH dengan perintah:

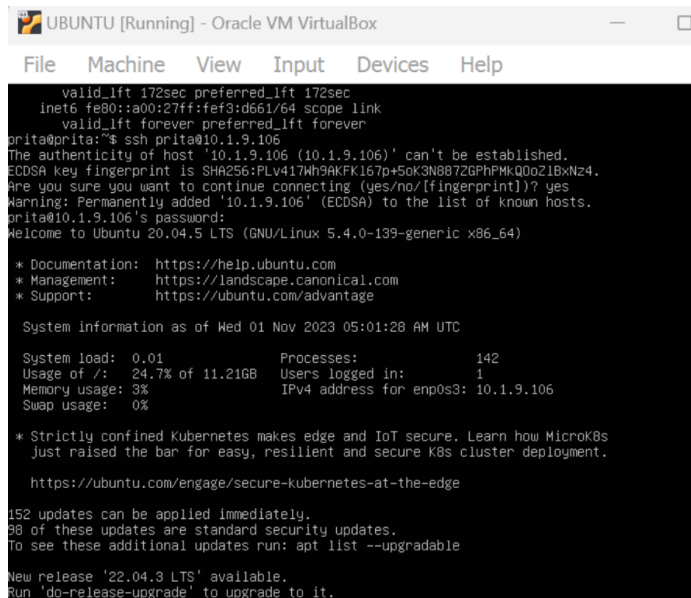
```
sudo systemctl status ssh
```

```
prita@prita:~$ sudo systemctl status ssh
• ssh.service - OpenBSD Secure Shell server
   Loaded: loaded (/lib/systemd/system/ssh.service; enabled; vendor preset: enabled)
   Active: active (running) since Wed 2023-11-01 04:10:06 UTC; 47min ago
     Docs: man:sshd(8)
           man:sshd_config(5)
  Main PID: 768 (sshd)
    Tasks: 1 (limit: 8270)
   Memory: 3.7M
    CGroup: /system.slice/ssh.service
            └─768 sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups

Nov 01 04:10:05 prita systemd[1]: Starting OpenBSD Secure Shell server...
Nov 01 04:10:06 prita sshd[768]: Server listening on 0.0.0.0 port 22.
Nov 01 04:10:06 prita systemd[1]: Started OpenBSD Secure Shell server.
Nov 01 04:10:06 prita sshd[768]: Server listening on :: port 22.
```

- 7) Jika muncul tulisan active di atas berarti ssh telah berhasil aktif dan bisa juga kita jalani melalui Windows + R > CMD maupun Putty sebagai berikut ini

➤ Ubuntu Server



```
UBUNTU [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help

valid_lft 172sec preferred_lft 172sec
inet6 fe80::a00:27ff:fe3:d661/64 scope link
valid_lft forever preferred_lft forever
prita@prita:~$ ssh prita@10.1.9.106
The authenticity of host '10.1.9.106 (10.1.9.106)' can't be established.
ECDSA key fingerprint is SHA256:PLv417Wh9AKFK167p+5oK3N8072GPhPMKQ0o21BxNz4.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.1.9.106' (ECDSA) to the list of known hosts.
prita@10.1.9.106's password:
Welcome to Ubuntu 20.04.5 LTS (GNU/Linux 5.4.0-139-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

System information as of Wed 01 Nov 2023 05:01:28 AM UTC

System load:  0.01               Processes:    142
Usage of /:   24.7% of 11.21GB   Users logged in: 1
Memory usage: 3%                IPv4 address for enp0s3: 10.1.9.106
Swap usage:  0%

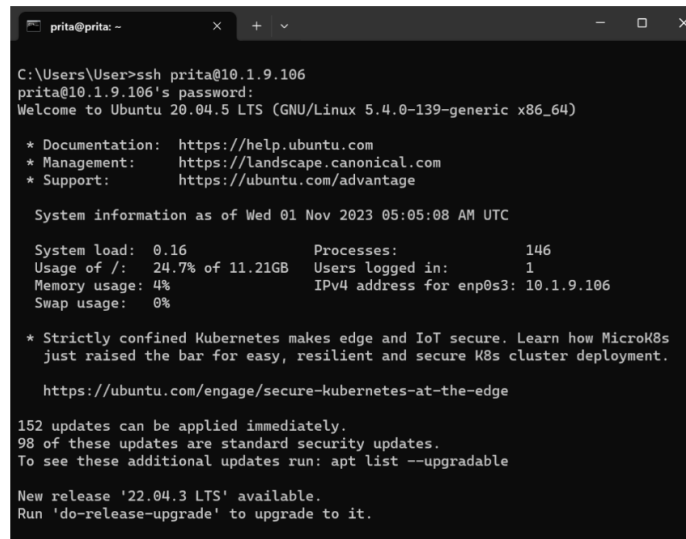
 * Strictly confined Kubernetes makes edge and IoT secure. Learn how MicroK8s
   just raised the bar for easy, resilient and secure K8s cluster deployment.

   https://ubuntu.com/engage/secure-kubernetes-at-the-edge

152 updates can be applied immediately.
98 of these updates are standard security updates.
To see these additional updates run: apt list --upgradable

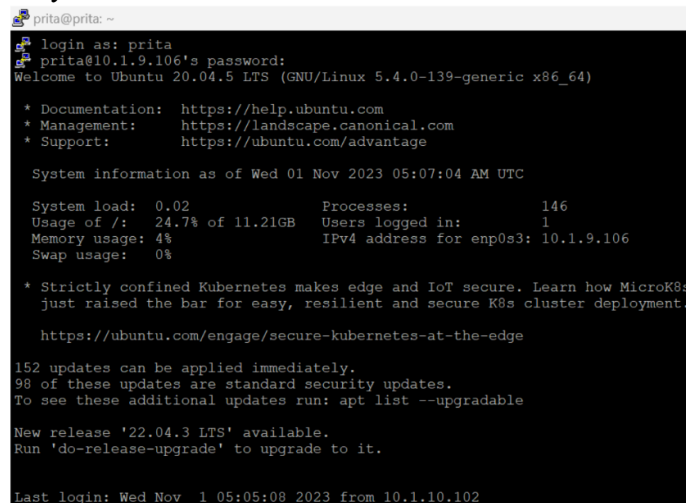
New release '22.04.3 LTS' available.
Run 'do-release-upgrade' to upgrade to it.
```

➤ Windows + R > CMD



```
prita@prita: ~  
C:\Users\User>ssh prita@10.1.9.106  
prita@10.1.9.106's password:  
Welcome to Ubuntu 20.04.5 LTS (GNU/Linux 5.4.0-139-generic x86_64)  
  
* Documentation:  https://help.ubuntu.com  
* Management:    https://landscape.canonical.com  
* Support:        https://ubuntu.com/advantage  
  
System information as of Wed 01 Nov 2023 05:05:08 AM UTC  
  
System load:  0.16          Processes:            146  
Usage of /:   24.7% of 11.21GB Users logged in:           1  
Memory usage: 4%          IPv4 address for enp0s3: 10.1.9.106  
Swap usage:   0%  
  
* Strictly confined Kubernetes makes edge and IoT secure. Learn how MicroK8s  
  just raised the bar for easy, resilient and secure K8s cluster deployment.  
  
https://ubuntu.com/engage/secure-kubernetes-at-the-edge  
  
152 updates can be applied immediately.  
98 of these updates are standard security updates.  
To see these additional updates run: apt list --upgradable  
  
New release '22.04.3 LTS' available.  
Run 'do-release-upgrade' to upgrade to it.
```

➤ Putty



```
prita@prita: ~  
login as: prita  
prita@10.1.9.106's password:  
Welcome to Ubuntu 20.04.5 LTS (GNU/Linux 5.4.0-139-generic x86_64)  
  
* Documentation:  https://help.ubuntu.com  
* Management:    https://landscape.canonical.com  
* Support:        https://ubuntu.com/advantage  
  
System information as of Wed 01 Nov 2023 05:07:04 AM UTC  
  
System load:  0.02          Processes:            146  
Usage of /:   24.7% of 11.21GB Users logged in:           1  
Memory usage: 4%          IPv4 address for enp0s3: 10.1.9.106  
Swap usage:   0%  
  
* Strictly confined Kubernetes makes edge and IoT secure. Learn how MicroK8s  
  just raised the bar for easy, resilient and secure K8s cluster deployment.  
  
https://ubuntu.com/engage/secure-kubernetes-at-the-edge  
  
152 updates can be applied immediately.  
98 of these updates are standard security updates.  
To see these additional updates run: apt list --upgradable  
  
New release '22.04.3 LTS' available.  
Run 'do-release-upgrade' to upgrade to it.  
  
Last login: Wed Nov  1 05:05:08 2023 from 10.1.10.102
```

## 1.5 ANALISIS

Implementasi SSH pada Ubuntu Server merupakan langkah kunci dalam memastikan keamanan dan keterjangkauan sistem dari jarak jauh. SSH mengamankan koneksi dengan enkripsi, melindungi dari ancaman keamanan. Memungkinkan manajemen server tanpa kehadiran fisik, menghemat waktu dan biaya. Penting untuk memastikan instalasi OpenSSH dan konfigurasi server yang benar. Akses melalui alamat IP memungkinkan koneksi dari mana saja dengan koneksi internet. Dengan pemahaman ini, pengguna dapat mengakses dan mengelola server Ubuntu dengan efektif dan aman.

Pada bab ini, akan dilakukan analisis lebih mendalam terkait implementasi dan penggunaan SSH pada Ubuntu Server. Selain itu, akan dibahas juga mengenai dua metode pengaksesan SSH, yaitu melalui aplikasi PuTTY dan melalui command prompt pada sistem operasi Windows menggunakan kombinasi tombol Windows+R dan CMD.

Penggunaan PuTTY merupakan salah satu pilihan yang umum digunakan untuk mengakses server melalui SSH pada sistem operasi Windows. Aplikasi ini menyediakan antarmuka yang intuitif dan user-friendly untuk melakukan koneksi ke server jarak jauh dengan aman.

Selain itu, akan dibahas juga cara akses melalui command prompt pada Windows dengan menggunakan kombinasi tombol Windows+R dan CMD. Metode ini memungkinkan pengguna untuk melakukan koneksi SSH dengan menggunakan antarmuka command-line, yang seringkali menjadi pilihan bagi pengguna yang lebih terbiasa dengan penggunaan terminal.

Melalui analisis ini, diharapkan pembaca dapat memahami berbagai opsi akses SSH yang tersedia dan memilih metode yang sesuai dengan preferensi dan kebutuhan mereka. Selain itu, pembaca juga akan memperoleh keterampilan praktis dalam penggunaan aplikasi PuTTY dan akses melalui command prompt pada sistem operasi Windows.

## **1.6 KESIMPULAN**

Melalui pembahasan materi ini, dapat disimpulkan bahwa penggunaan SSH (Secure Shell) pada Ubuntu Server adalah suatu langkah penting untuk memastikan keamanan dan keterjangkauan sistem dari jarak jauh. SSH memberikan lapisan keamanan tambahan dengan menggunakan enkripsi data, melindungi dari potensi ancaman keamanan. Langkah-langkah praktis telah dijabarkan untuk menjalankan SSH pada Ubuntu Server, termasuk instalasi OpenSSH dan konfigurasi server. Kemudian, penggunaan alamat IP memungkinkan akses dari mana saja dengan koneksi internet. Metode akses SSH juga telah dianalisis, termasuk penggunaan aplikasi PuTTY dan command prompt pada Windows. Kedua metode ini memberikan opsi yang fleksibel bagi pengguna untuk mengelola server dengan preferensi masing-masing. Dengan pemahaman ini, pembaca diharapkan dapat mengimplementasikan SSH dengan efektif, memastikan keamanan akses jarak jauh, dan meminimalkan risiko potensial. Dengan demikian, pengelolaan dan manajemen sistem Ubuntu Server akan menjadi lebih efisien dan aman.