🔐 SSH — Full Step by Step Guide (Beginner Friendly) + Important Options

---

🧩 Step 1: What is SSH?

SSH (Secure Shell) *is a way to connect safely to another computer over the internet* 🌐🔒
It encrypts your data so no one can steal it.

Example use:
You sit at your laptop 💻 and control a remote server 🖥️.

🧰 Step 2: Install SSH

✅ *On Ubuntu/Linux:*

```
sudo apt update
sudo apt install openssh-server
```

Check SSH status:

```
sudo systemctl status ssh
```

🔑 Step 3: Generate SSH Key (Recommended)

```
ssh-keygen
```

*Press **Enter** for all options* ✅
This creates:

```
~/.ssh/id_rsa       (private key 🔐)
~/.ssh/id_rsa.pub   (public key 🔓)
```

📤 Step 4: Copy Key to Server

```
ssh-copy-id user@server_ip
```

Now passwordless login will work 🔑✅

🔌 Step 5: Connect Using SSH

Basic command:

```
ssh user@server_ip
```

Example:

```
ssh ubuntu@192.168.1.10
```

⭐ Step 5.1: IMPORTANT SSH OPTIONS (For Tests & Real Use)

- **`-p` → Custom Port 🔢**

```
ssh -p 2222 user@server_ip
```

- **`-i` → Use Private Key 🔑**

```
ssh -i ~/.ssh/id_rsa user@server_ip
```

🔸 ***-v → Debug Mode*** 👁️

```
ssh -v user@server_ip
```

🔸 ***-X → GUI Forwarding*** 🖥️

```
ssh -X user@server_ip
```

🔸 ***-L → Local Port Forwarding*** 🔁

```
ssh -L 8080:localhost:80 user@server_ip
```

🔸 ***-R → Remote Port Forwarding*** 🌐

```
ssh -R 9090:localhost:22 user@server_ip
```

⚙️ Step 6: Change SSH Port (Optional)

Edit config:

```
sudo nano /etc/ssh/sshd_config
```

Find:

```
#Port 22
```

Change to:

```
Port 2222
```

Save the file ✅

Restart SSH:

```
sudo systemctl restart ssh
```

Check port:

```
Netstat -plunt | grep 2222
```

📁 Step 7: Create SSH Client Config File

🧩 What is config ?

An SSH config file is a file that stores connection settings (like hostname, username, port, and key file) so you can connect to servers easily without typing long commands every time.

Create:

```
vim ~/.ssh/config
```

Add:

```
Host myserver
    HostName 192.168.1.10
    User ubuntu
    Port 2222
    IdentityFile ~/.ssh/id_rsa
```

Now connect:

```
ssh myserver
```

🧪 Step 8: Troubleshooting Commands

```
sudo systemctl status ssh
sudo sshd -t
ssh -v user@server_ip
```

🧠 *Easy Summary (Remember This)*

✅ *SSH = Secure remote login* 🔐
✅ *Default port = 22* 🔢
✅ `sshd_config` *controls server* ⚙️
✅ `~/.ssh/config` *controls client* 💻
✅ *SSH encrypts data* 🛡️

📌 *One Line Definition (Exam)*

SSH is a secure protocol used to remotely access and control computers over encrypted connections.
